



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN  
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

**TRABAJO DE TITULACIÓN 1, PREVIO A LA  
OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GERENCIA  
DE SISTEMAS**

**TEMA: ANÁLISIS DE LA SITUACIÓN ACTUAL DE LOS  
PROCESOS DEL ÁREA DE SERVIDORES DE LA  
EMPRESA ACMECARD E IMPLEMENTACIÓN DE  
MEJORAS PARA EL CORRECTO FUNCIONAMIENTO  
OPERATIVO DEL ÁREA**

**AUTOR: SOCASI GUALOTUÑA PAULO CÉSAR**

**DIRECTOR: Msc. SANCHO ARIAS JOSÉ ALBERTO**

**SANGOLQUÍ**

**2015**



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN  
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA  
MAGÍSTER EN GERENCIA DE SISTEMAS**

**CERTIFICADO**

Certificó que el trabajo de titulación, “ANÁLISIS DE LA SITUACIÓN ACTUAL DE LOS PROCESOS DEL ÁREA DE INFRAESTRUCTURA Y NETWORKING DE LA EMPRESA ACMECARD Y PLANTEAMIENTO DE LAS MEJORAS PARA EL CORRECTO FUNCIONAMIENTO DEL ÁREA” realizado por el señor **SOCASI GUALOTUÑA PAULO CÉSAR**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditar y autorizar al señor Ing. **SOCASI GUALOTUÑA PAULO CÉSAR** para que lo sustente públicamente.

Sangolqui, 15 de agosto de 2015

MSC. SANCHO ARIAS JOSÉ ALBERTO  
DIRECTOR



**VICERRECTORADO DE INVESTIGACIÓN  
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

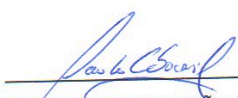
**MAGÍSTER EN GERENCIA DE SISTEMAS**

**AUTORÍA DE RESPONSABILIDAD**

Yo, **SOCASI GUALOTUÑA PAULO CÉSAR**, con cédula de identidad No. 1711972065, declaro que este trabajo de titulación **“ANÁLISIS DE LA SITUACIÓN ACTUAL DE LOS PROCESOS DEL ÁREA DE INFRAESTRUCTURA Y NETWORKING DE LA EMPRESA ACMECARD Y PLANTEAMIENTO DE LAS MEJORAS PARA EL CORRECTO FUNCIONAMIENTO DEL ÁREA”** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolqui, 15 de agosto de 2015

  
\_\_\_\_\_  
**SOCASI GUALOTUÑA PAULO CÉSAR**  
C.C. 1711972065



**VICERRECTORADO DE INVESTIGACIÓN  
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

**MAGÍSTER EN GERENCIA DE SISTEMAS**

**AUTORIZACIÓN**

Yo, **SOCASI GUALOTUÑA PAULO CÉSAR**, autorizo a la Universidad de las Fuerzas Armadas ESPE a publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **“ANÁLISIS DE LA SITUACIÓN ACTUAL DE LOS PROCESOS DEL ÁREA DE INFRAESTRUCTURA Y NETWORKING DE LA EMPRESA ACMECARD Y PLANTEAMIENTO DE LAS MEJORAS PARA EL CORRECTO FUNCIONAMIENTO DEL ÁREA”** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolqui, 15 de agosto de 2015

SOCASI GUALOTUÑA PAULO CÉSAR

C.C. 1711972065

## **DEDICATORIA.**

### **A DIOS Y A MI FAMILIA**

Dedico el éxito y la satisfacción de esta investigación a Dios quien me ha regalado los dones de la sabiduría y el entendimiento, a mis padres, hermanos y mi familia quienes siempre han estado conmigo alentándome y regalándome la paciencia necesaria. Al Ing. Master José Sánchez por su gran calidad humana, apoyo incondicional, confianza, alegría y ánimos que no me dejaron desfallecer para así poder llevar a cabo la culminación de este proyecto.

## AGRADECIMIENTO

Deseo expresar de todo corazón más sinceros agradecimientos a todas las personas que me brindaron su colaboración, sus conocimientos, su ayuda incondicional y por sobre todo su amistad durante la realización de este proyecto de tesis.

A Dios, esa fuerza superior en quienes muchos solo lo recordamos en los momentos difíciles y aun así nos recuerda siempre lo grande que es y los milagros que nos concede a cambio de nuestra devoción y se respetó, a ese ser que es omnipotente, quien me regalo a mi familia, quien me regala cada nuevo amanecer y sobre todo quien me regala el entendimiento para realizar cada reto de vida.

A mis padres, quienes siempre están pendientes y me encomiendan a diario a Dios en sus oraciones al pedir por mí y toda nuestra familia, para que cada día sea una mejor persona con un alto valor de humildad y generosidad con todos.

Ing., Master José Sánchez quien con sus valiosos conocimientos, enseñanzas y aplicables asesorías, han aportado grandes beneficios para esta investigación además de su amistad que hacen de la vida un sabor especial y una experiencia enriquecedora en cada vivencia.

En todas las etapas de vida han existido personas que desinteresadamente, tienen una participación efectiva para el buen desarrollo de mi vida y de este trabajo ya sea de una u otra forma han aportaron con su granito de arena.

MUCHAS GRACIAS A TODOS!!

## ÍNDICE

DEDICATORIA.....	V
AGRADECIMIENTO .....	VI
RESUMEN.....	XIV
PALABRAS CLAVES .....	XIV
ABSTRACT.....	XV
KEYWORDS .....	XV
CAPÍTULO I.....	1
INTRODUCCIÓN .....	1
1. OBJETIVOS.....	2
1.1 OBJETIVO GENERAL .....	2
1.2 OBJETIVOS ESPECÍFICOS .....	2
CAPÍTULO II .....	3
2. MARCO TEÓRICO.....	3
2.1 BANCA Y MERCADO .....	3
2.2 DIAGRAMAS DE FLUJO (PLEGUAZUELOS, 1999) .....	4
2.2.1 PRINCIPAL SIMBOLOGÍA DE LOS DIAGRAMAS DE FLUJO.....	4
2.3 BENEFICIOS DEL DIAGRAMA DE FLUJO.....	5
2.4 ELABORACIÓN DEL DIAGRAMA DE FLUJO.....	6
2.5 MAPAS DE PROCESOS (SIPOC) .....	7
CAPITULO III.....	10
3. DESCRIPCIÓN GENERAL DE LA EMPRESA.....	10
3.1. DEPARTAMENTO DE SISTEMAS .....	10
3.2. FUNCIONES DEL ÁREA DE TI .....	10
3.3. MISIÓN DE INFRAESTRUCTURA Y NETWORKING .....	12
3.4. VISIÓN DE INFRAESTRUCTURA Y NETWORKING.....	12
3.5. ESQUEMA ORGANIZACIONAL ACTUAL DEL ÁREA DE INFRAESTRUCTURA Y NETWORKING.....	12
3.6. DESCRIPCIÓN DE LOS SERVICIOS QUE PRESTAN LOS DEPARTAMENTOS.....	13
3.7. TIPIFICACIÓN DE LOS SERVICIOS QUE MANEJAN LAS ÁREAS DE SISTEMAS .....	13
3.8. SERVICIOS QUE MANEJAN LAS ÁREAS DE SISTEMAS.....	30
CAPITULO IV.....	42
4. FUNCIONES QUE INTERACTÚAN ENTRE LAS ÁREAS .....	42
4.1. INVENTARIO DE PROCESOS OBJETIVOS .....	43
4.1.1. DEFINICIONES IMPORTANTES.....	44
4.2. DIAGRAMA DE FLUJO DE MODELO OPERATIVO DE TI .....	46

	viii
4.3. PROCESOS DETALLADOS .....	100
4.3.1. PROCESO: ADMINISTRACIÓN DE DATOS .....	100
4.3.1.1. SUBPROCESO: CICLO DE VIDA DE BASES DE DATOS .....	100
4.3.1.2. SUBPROCESO: SOPORTE A BASES DE DATOS.....	103
4.3.2. PROCESO: ADMINISTRACIÓN DE LA CONFIGURACIÓN .....	106
4.3.2.1. SUBPROCESO: CONFIGURACIÓN DE HARDWARE .....	106
4.3.2.2. SUBPROCESO: CONFIGURACIÓN DE SISTEMA OPERATIVO Y SOFTWARE .....	108
4.3.2.3. SUBPROCESO: MANTENIMIENTO DE REDES LAN.....	112
4.3.2.4. SUBPROCESO: MANTENIMIENTO DE REDES WAN .....	115
4.3.3. PROCESO: ADMINISTRACIÓN DE LA MESA DE SERVICIO Y LOS INCIDENTES .....	117
4.3.3.1. SUBPROCESO: SOPORTE A USUARIOS EN SERVICE DESK.....	117
4.3.4. PROCESO: ADMINISTRACIÓN DE OPERACIONES .....	120
4.3.4.1. SUBPROCESO: PROCESAMIENTO DE TRANSACCIONES Y DISPONIBILIDAD DE LA INFORMACIÓN .....	120
4.3.4.2. SUBPROCESO: SERVICIO DE BACK UP.....	126
4.3.4.3. SUBPROCESO: SERVICIO DE RECOVERY .....	132
4.3.4.4. SUBPROCESO: DEPURACIÓN DE ARCHIVOS .....	134
4.3.4.5. SUBPROCESO: SOPORTE A USUARIOS .....	136
4.3.5. PROCESO: ADMINISTRACIÓN DEL DESEMPEÑO Y LA CAPACIDAD .....	137
4.3.6. PROCESO: ADMINISTRACIÓN DEL AMBIENTE FÍSICO.....	139
4.3.7. PROCESO: ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA DE TI. ....	141
4.3.7.1. SUBPROCESO: MANTENIMIENTO DE HARDWARE.....	141
4.3.7.2. SUBPROCESO: MANTENIMIENTO DE SOFTWARE.....	145
4.3.8. PROCESO: EVALUACIÓN Y ADMINISTRACIÓN LOS RIESGOS DE TI.....	149
4.3.8.1. SUBPROCESO: EVALUACIÓN Y ADMINISTRACIÓN LOS RIESGOS DE TI.....	149
4.3.9. PROCESO: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS .....	153
4.3.9.1. SUBPROCESO: ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN..	153
4.3.9.2. SUBPROCESO: MONITOREO DE SEGURIDAD .....	156
4.3.9.3. SUBPROCESO: PASO A PRODUCCIÓN .....	159
4.3.9.4. SUBPROCESO: SOLICITUD DE RESPALDOS .....	163
4.3.9.5. SUBPROCESO: ROTACIÓN DE RESPALDOS .....	165
4.3.9.6. SUBPROCESO: CUSTODIA DE RESPALDOS.....	167



4.3.9.7. SUBPROCESO: SEGURIDAD Y CONTROL ADMINISTRATIVO .....	169
4.3.10. PROCESO: GESTIÓN DE ACCESOS .....	170
4.3.10.1. SUBPROCESO: MANTENIMIENTO DE USUARIOS .....	170
4.3.11. PROCESO: GESTIÓN DE EVENTOS .....	174
4.3.11.1. SUBPROCESO: GESTIÓN DE EVENTOS .....	174
4.3.11.2. PROCESO: GESTIÓN DE LA CONTINUIDAD DE TI .....	176
4.3.11.3. SUBPROCESO: CONTINGENCIA AUTORIZADOR .....	176
4.3.11.4. SUBPROCESO: CONTINGENCIA GESTOR .....	181
4.3.11.5. SUBPROCESO: CONTINGENCIA PEOPLESOFT .....	186
4.3.12. PROCESO: GESTIÓN DE LA DISPONIBILIDAD .....	189
4.3.13. SUBPROCESO: MONITOREO DE APLICACIONES .....	189
4.3.14. SUBPROCESO: MONITOREO DE SERVIDORES Y DISCOS .....	193
4.3.15. SUBPROCESO: MONITOREO DE TRANSACCIONES .....	196
4.3.16. PROCESO: GESTIÓN DE PROBLEMAS .....	197
4.4. SIPOC .....	200
4.5. LISTADO DE ANS POR PROCESO - OPERACIÓN DEL SERVICIO .....	203
4.6. LISTADO DE KPI'S POR PROCESO - OPERACIÓN DEL SERVICIO .....	204
4.7. PROPUESTA DE LA NUEVA ESTRUCTURA PARA LA GERENCIA DE OPERACIÓN DEL SERVICIO .....	206
CAPITULO V .....	207
5.1 CONCLUSIONES .....	207
5.2 RECOMENDACIONES .....	208
BIBLIOGRAFÍA .....	209

## ÍNDICE DE TABLAS

Tabla 1	Tipificaciones de Servicios. ....	<b>14</b>
Tabla 2	Servicios y áreas responsables. ....	<b>30</b>
Tabla 3	Inventarios de procesos de objetivos. ....	<b>43</b>

## ÍNDICE DE FIGURAS

Figura 1. Estructura SIPOC.....	<b>8</b>
Figura 2. Organigrama Estructural de Tecnología.....	<b>12</b>
Figura 4. Mapa de procesos Operación del Servicio .....	<b>42</b>
Figura 5. Subproceso: Ciclo de vida de Base de Datos.....	<b>46</b>
Figura 6. Subproceso: Soporte de Bases de Datos.....	<b>47</b>
Figura 7. Subproceso: Configuración de Hardware .....	<b>48</b>
Figura 8. Subproceso: Configuración de Sistemas Operativos y Software.....	<b>49</b>
Figura 9. Subproceso: Mantenimiento de Redes WAN .....	<b>50</b>
Figura 10. Subproceso: Mantenimiento de Redes LAN.....	<b>51</b>
Figura 11. Subproceso: Mantenimiento de Redes LAN.....	<b>52</b>
Figura 12. Subproceso: Soporte a Usuarios en Service Desk .....	<b>53</b>
Figura 13. Subproceso: Procesamiento de Transacciones y Disponibilidad de Información .....	<b>54</b>
Figura 14. Subproceso: Procesamiento de Transacciones y Disponibilidad de Información .....	<b>55</b>
Figura 15. Subproceso: Procesamiento de Transacciones y Disponibilidad de Información .....	<b>56</b>
Figura 16. Subproceso: Procesamiento de Transacciones y Disponibilidad de Información .....	<b>57</b>
Figura 17. Subproceso: Servicio de backup.....	<b>58</b>
Figura 18. Subproceso: Servicio de backup s .....	<b>59</b>
Figura 19. Subproceso: Servicio de backup.....	<b>60</b>

Figura 20. Subproceso: Servicio de backup.....	<b>61</b>
Figura 21. Subproceso: Servicio de backup.....	<b>62</b>
Figura 22. Subproceso: Servicio de backup.....	<b>63</b>
Figura 23. Subproceso: Servicio de backup.....	<b>64</b>
Figura 24. Subproceso: Servicio de backup.....	<b>65</b>
Figura 25. Subproceso: Servicio de recovery .....	<b>66</b>
Figura 26. Subproceso: Depuración de archivos .....	<b>67</b>
Figura 27. Subproceso: Soporte a usuarios .....	<b>68</b>
Figura 28. Subproceso: Soporte a usuarios .....	<b>69</b>
Figura 29. Subproceso: Administración del Ambiente Físico.....	<b>70</b>
Figura 30. Subproceso: Mantenimiento de hardware .....	<b>71</b>
Figura 31. Subproceso: Mantenimiento de hardware .....	<b>72</b>
Figura 32. Subproceso: Mantenimiento de software .....	<b>73</b>
Figura 33. Subproceso: Evaluar y Administrar los riesgos de TI.....	<b>74</b>
Figura 34. Subproceso: Administración de la seguridad de la información.....	<b>75</b>
Figura 35. Subproceso: Monitoreo de seguridad .....	<b>76</b>
Figura 36. Subproceso: Paso a producción.....	<b>77</b>
Figura 37. Subproceso: Paso a producción.....	<b>78</b>
Figura 38. Subproceso: Solicitud de respaldos.....	<b>79</b>
Figura 39. Subproceso: Rotación de respaldos.....	<b>80</b>
Figura 40. Subproceso: Custodia de respaldos.....	<b>81</b>
Figura 41. Subproceso: Seguridad y control administrativo .....	<b>82</b>

Figura 42. Subproceso: Mantenimiento de usuarios .....	<b>83</b>
Figura 43. Subproceso: Mantenimiento de usuarios .....	<b>84</b>
Figura 44. Proceso: Gestión de eventos .....	<b>85</b>
Figura 45. Subproceso: Contingencia Peoplesoft .....	<b>86</b>
Figura 46. Subproceso: Contingencia Gestor.....	<b>87</b>
Figura 47. Subproceso: Contingencia Gestor.....	<b>88</b>
Figura 48. Subproceso: Contingencia Autorizador .....	<b>89</b>
Figura 49. Subproceso: Contingencia Autorizador .....	<b>90</b>
Figura 50. Subproceso: Contingencia Autorizador .....	<b>91</b>
Figura 51. Subproceso: Contingencia Peoplesoft .....	<b>92</b>
Figura 52. Subproceso: Contingencia Peoplesoft .....	<b>93</b>
Figura 53. Subproceso: Monitoreo de aplicaciones .....	<b>94</b>
Figura 54. Subproceso: Monitoreo de centrales telefónicas, equipos de comunicación y enlaces .....	<b>95</b>
Figura 55. Subproceso: Monitoreo de centrales telefónicas, equipos de comunicación y enlaces .....	<b>96</b>
Figura 56. Subproceso: Monitoreo de transacciones .....	<b>97</b>
Figura 57. Subproceso: Monitoreo de servidores y discos .....	<b>98</b>
Figura 58. Subproceso Gestión de problemas .....	<b>99</b>
Figura 59. Nueva Estructura del área de productos y servicios .....	<b>206</b>

## **RESUMEN**

En el presente proyecto se realizó una recopilación exhaustiva de todas las actividades que realizan las áreas de: ServiceDesk, comunicaciones, centro de cómputo y control tecnológico, las cuales interactúan en forma directa con el área de infraestructura y networking en el día a día de trabajo para garantizar que todas las actividades que se tienen asignadas sean cumplidas de una forma eficaz y eficiente para de esta manera evitar afectaciones a las actividades diarias de la organización. Con esta recopilación de actividades se pudo realizar un levantamiento de todos los procesos y procedimientos que compartían las áreas antes mencionadas ocasionando un desgaste de recursos tanto humanos como físicos ya que se realizaban tareas repetidas en las diferentes áreas involucradas. Tras este levantamiento de las actividades se pudo clasificar los procesos en 14 grandes grupos de procesos que interactuaban entre las áreas, se realizó el diagrama de flujo de cada uno de estos procesos, así como un análisis detallado de los mismos para poder determinar las actividades y procesos que debían ser transferidos entre las áreas involucradas mediante el SIPOC en donde se menciona el nombre de los procesos planteados para el cambio así como el nombre que tienen los procesos en la actualidad. Con todas estas actividades también se logró replantear un nuevo cuadro de ANS para una mejor atención tanto de los clientes internos como externos al área, replantear los KPI's del área y plantar un nuevo modelo estructural del área de infraestructura y networking. La cual se encuentra inmersa en una nueva área denominada Operación del Servicio.

## **PALABRAS CLAVES**

- PROCESOS
- DIAGRAMAS DE FLUJO
- SIPOC
- ANS
- KPI

## **ABSTRACT**

In this project a comprehensive compilation was made. This involves all the activities carried out in the areas of Service Desk, Communication, Computer Center and Control technology, which directly interact daily with the area of networking infrastructure and to ensure that all activities are assigned, should be fulfilled in an effective and efficient manner to thereby avoid affecting the daily activities of the organization. After relieving information activities could classify processes in 14 large groups of interacting processes between areas. The flowchart of each of these processes was performed. A detailed flow chart analysis was also performed to determine the activities and processes that must be transferred between the areas involved by SIPOC, where the name of the proposed processes for the change is indicated; as well as the name that processes today have today. With all these activities it was also possible to stake out a new chart SLA to provide better service for both internal and external customers in the area. Rethink KPIs of the area and plant a new structural model of the Infrastructure and networking area. Which is immersed in a new area called Service Operation.

## **KEYWORDS**

- PROCESSES
- FLOWCHART
- SIPOC
- SLA
- KPI

## CAPÍTULO I

### Introducción

En la actualidad todas las empresas cualquiera que sea el tamaño que tengan, hoy por hoy tendrán que irse adaptando al entorno que les rodea y a los constantes cambios que se van produciendo a su alrededor. De la capacidad de adaptación que tengan dependerá el éxito o fracaso en la carrera por ir creciendo y sobreviviendo al duro mercado competitivo que las rodea.

Es por esto que se hace presente un proceso de reorganización empresarial en las diferentes áreas, implicando con esto un cambio, dicho cambio será más o menos drástico dependiendo de la capacidad de anticipación que se tenga, es decir, cuanto antes nos anticipemos al futuro y adaptemos nuestra estructura al mismo menos drásticas serán las medidas a tomar.

En la actualidad se pueden notar dos grandes problemas en la organización de las empresas, que son:

- a) Como cada persona es responsable de una parte del proceso, nadie es responsable del total y del producto del proceso.
- b) No se aprovecha todo el potencial humano.

Por lo antes expuesto, las áreas de TI actualmente se están reorganizando para tener una orientación de servicio y asesoría en innovación de cara a todos sus clientes tanto internos como externos, traduciendo los servicios ofrecidos por TI en valor para la organización.



## 1. Objetivos

### 1.1 Objetivo General

Realizar una propuesta de mejoramiento de los procesos óptimos para el buen funcionamiento del área de Infraestructura y Networking. Los cuales permitirán realizar la reestructuración del área de Infraestructura y Networking de la empresa financiera ACMECARD.

### 1.2 Objetivos Específicos

- Levantar y analizar los procesos existentes en el área de Infraestructura y Networking.
- Consolidar los procesos más relevantes para el buen funcionamiento del área de Infraestructura y Networking.
- Levantar y analizar los ANS existentes para el cumplimiento de los procesos en el área de Infraestructura y Networking.
- Plantear las mejoras encontradas de los procesos para la reestructuración del área de Infraestructura y Networking mediante el SIPOC.

## CAPÍTULO II

### 2. Marco Teórico

#### 2.1 Banca y Mercado

Son consideradas compañías emisoras y/o administradoras de tarjetas de crédito las sociedades anónimas que prestan servicios de carácter financiero, mediante la emisión, administración, financiamiento o mercadeo de tarjetas de crédito de pago y de afinidad de circulación general, en moneda nacional o extranjera; así como tarjetas de crédito o de pago de circulación restringida en moneda nacional, previa autorización de la Superintendencia de Bancos y Seguros.

Solamente las instituciones financieras y las compañías emisoras o administradoras de tarjetas de crédito pueden actuar como emisor u operador de tarjetas de crédito.

El emisor o administrador de tarjetas de crédito únicamente podrá ofrecer a sus tarjetahabientes para el pago de sus consumos, el uso de líneas de crédito rotativo o la modalidad de crédito diferido.

#### Principales características de las Compañías Emisoras de Tarjetas de Crédito.

Son consideradas emisoras de tarjetas de crédito las sociedades autorizadas que realizan, por propia emisión o por concesión de marca, las siguientes actividades:

- a) Emitir y promover la tarjeta;
- b) Calificar y aprobar las solicitudes de los tarjetahabientes y de afiliación de establecimientos;
- c) Conceder líneas de crédito, ya por utilización de la tarjeta de crédito en establecimientos comerciales o por entrega de dinero en efectivo;
- d) Efectuar cobros a los tarjetahabientes y pagos a los establecimientos;
- e) Recibir fondos de sus tarjetahabientes con la finalidad de efectuar cargos a sus futuros consumos; y,

- f) Otras actividades estrictamente relacionadas con el objeto de las compañías emisoras o administradoras de tarjetas de crédito, las que deberán ser reportadas a la Superintendencia de Bancos y Seguros, quien informará a la Junta Bancaria.

## 2.2 Diagramas de Flujo (Pleguazuelos, 1999)

Los diagramas de flujo representan la secuencia o los pasos lógicos para realizar una tarea mediante unos símbolos. Dentro de los símbolos se escriben los pasos a seguir. Un diagrama de flujo debe proporcionar una información clara, ordenada y concisa de todos los pasos a seguir, ya que a través de él se planifica la solución a un problema.

Principales características de los flujogramas:

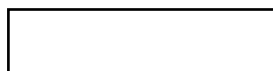
- De uso, permiten facilitar su empleo.
- De destino, permiten la correcta identificación de actividades a seguir.
- De comprensión e interpretación, permiten simplificar su comprensión.
- De interacción, permiten el acercamiento y coordinación.
- De simbología, disminuye la complejidad y accesibilidad a ellos.
- De diagramación, se elaboran con rapidez y no requieren recursos sofisticados.

### 2.2.1 Principal simbología de los diagramas de flujo

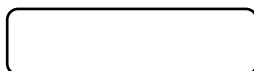
- a) Flecha: Indica el sentido y trayectoria del proceso de información o tarea.



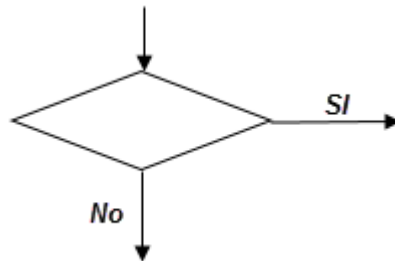
- b) Rectángulo: Se usa para representar un evento o proceso determinado.



- c) Rectángulo redondeado: Se usa para representar un evento que ocurre de forma automática y del cual generalmente se sigue una secuencia determinada, como inicio o fin del flujo.



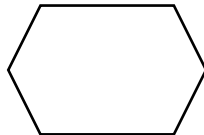
- d) Rombo: Se utiliza para representar una condición. Normalmente el flujo de información entra por arriba y sale por un lado si la condición se cumple o sale por el lado opuesto si la condición no se cumple. Lo anterior hace que a partir de éste el proceso tenga dos caminos posibles.



- e) Círculo: Representa un punto de conexión entre procesos. Se utiliza cuando es necesario dividir un diagrama de flujo en varias partes, por ejemplo por razones de espacio o simplicidad. Una referencia debe darse dentro para distinguirlo de otros. La mayoría de las veces se utilizan números en los mismos.



- f) Rombo: Expresa proceso de llamada a una subalterna.



### 2.3 Beneficios del Diagrama de Flujo.

- a) Facilitan la obtención de una visión lineal y transparente del proceso, de esta manera mejorando su comprensión. El conjunto de actividades, relaciones e incidencias de un proceso no es fácilmente discernible a priori. La diagramación hace posible aprehender ese conjunto e ir más allá, centrándose en aspectos específicos del mismo, apreciando las interrelaciones que forman parte del proceso así como las que se dan con otros procesos y subprocesos. Estas actividades de análisis y diagramación constituyen el primer paso para mejorar las prácticas organizacionales.

- b) Permiten marcar y definir los límites de un proceso. En la mayoría de los casos estos límites no son tan evidentes a simple vista, no estando definidos los distintos proveedores y clientes (internos y externos) involucrados.
- c) Facilitan la identificación de los clientes, es mucho más sencillo determinar sus necesidades y ajustar el proceso hacia la satisfacción de sus necesidades y expectativas.
- d) Estimulan el pensamiento analítico en el momento de estudiar un proceso, haciendo más factible generar alternativas útiles.
- e) Proporcionan un método de comunicación más eficaz, al introducir un lenguaje común, si bien es cierto que para ello se hace preciso la capacitación de aquellas personas que entrarán en contacto con la diagramación.
- f) Un diagrama de flujo ayuda a establecer el valor agregado de cada una de las actividades que componen los procesos y subprocesos.
- g) Igualmente, constituye una excelente referencia para establecer mecanismos de control y medición de los procesos, así como de los objetivos concretos para las distintas operaciones llevadas a cabo.
- h) Facilitan el estudio y aplicación de acciones que redunden en la mejora de las variables tiempo y costes de actividad e incidir, por consiguiente, en la mejora de la eficacia y la eficiencia.
- i) Constituyen el punto de comienzo indispensable para acciones de mejora o reingeniería.

Todas estas razones apuntan hacia el diagrama de flujo de procesos como un instrumento primordial para la correcta gestión de los procesos.

La realización de un diagrama de flujo es una actividad íntimamente ligada al hecho de modelar un proceso, que es por sí mismo un componente esencial en la gestión de procesos.

#### 2.4 Elaboración del Diagrama de Flujo

El diagrama de flujo debe ser realizado por un equipo de trabajo en el que las distintas personas aporten, en conjunto, una perspectiva completa del proceso, por lo que con frecuencia este equipo será multifuncional y multijerárquico. Para esto se debe tener presente lo siguiente:

- a) Determinar el proceso a diagramar.
- b) Definir el grado de detalle. El diagrama de flujo del proceso puede mostrar a grandes rasgos la información sobre el flujo general de actividades principales, o ser desarrollado de modo que se incluyan todas las actividades y los puntos de decisión. Un diagrama de flujo detallado dará la oportunidad de llevar a cabo un análisis más exhaustivo del proceso.
- c) Identificar la secuencia de pasos del proceso. Situándolos en el orden en que son llevados a cabo.
- d) Construir el diagrama de flujo. Para la elaboración de un diagrama de flujo, los símbolos estándar han sido normalizados, entre otros, el American National Standards Institute (ANSI).

## 2.5 Mapas de procesos (SIPOC)

La comprensión o descripción de lo que sucede en la empresa puede ser uno de los más grandes pasos para la generación de un valor agregado en los procesos de la misma.

Entre los más importantes beneficios del mapeo de procesos podemos mencionar:

- a) Ver lo que falta y agregarlo
- b) Ver donde están mal las cosas y arreglarlo
- c) Producir las mejores prácticas, si un grupo de personas está haciendo lo mismo, ver quién es el más apto para ese proceso.
- d) Concentrarse en lo que está pasando y mejorarlo.
- e) Identificar las ineficiencias existentes en los procesos para tomar las acciones necesarias para poder mejorarlas y controlar los gastos que estas presentan.
- f) Capacitar al personal puede ser más sencillo enfocándose directamente a las mejoras encontradas.

EL SIPOC se presenta como una de tantas herramientas que se usan en la actualidad para la búsqueda de áreas de mejora. Se resume como una visión a vista de pájaro de todo el proceso de una empresa bajo una perspectiva particular, la cual viene dada por el significado

de sus siglas en inglés Suppliers-Inputs-Process-Output-Customers (Proveedor-Entrada-Proceso-Salida-Cliente).

- Proveedor (Suppliers): persona que aporta recursos al proceso
- Recursos (inputs): todo lo que se requiere para llevar a cabo el proceso. Se considera recursos a la información, materiales e incluso, personas.
- Proceso (process): conjunto de actividades que transforman las entradas en salidas, dándoles un valor añadido.
- Cliente (customer): la persona que recibe el resultado del proceso. El objetivo es obtener la satisfacción de este cliente.

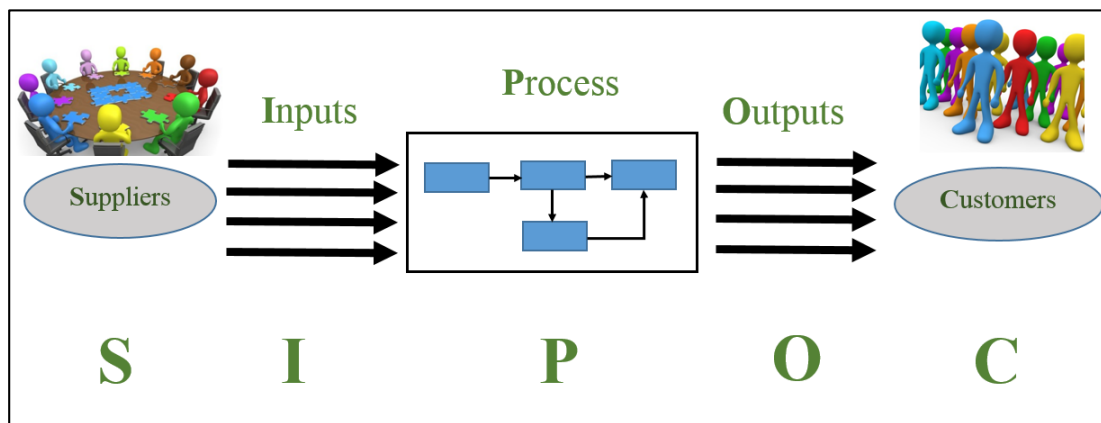


Figura 1. Estructura SIPOC

Después de que la ISO 9001, en su última actualización del año 2008, hiciera patente la importancia de la visión por procesos para poder aplicar las mejores herramientas y detectar las mayores áreas de mejora, SIPOC permite precisamente realizar eso, establecer una serie de subprocessos dentro de cada uno de los principales procesos de una empresa.

El detalle al cual se quiera llegar a través del SIPOC va a depender de múltiples factores como: complejidad organizativa, variación de tipos de procesos, complejidad técnica, etc. Por eso, lo más importante es conocer cómo funciona la herramienta SIPOC y así cada uno la podrá aplicar a su caso particular.

La forma de actuar depende mucho de cada organización, pero por lo general se recomienda realizar un mapa de procesos general de la organización (en el caso de que todavía no se tenga) y plantear una serie de reuniones con los responsables de cada uno de los procesos para entrar más en detalle sobre el funcionamiento concreto de cada uno de ellos.

De manera resumida los pasos a realizar para elaborar un Diagrama SIPOC pueden ser:

- a) Identificar los procesos de gestión
- b) Establecer las entradas del proceso, los recursos necesarios
- c) Establecer los proveedores de estas entradas al proceso
- d) Definir las salidas del proceso
- e) Establecer quién es el cliente de cada una de las salidas obtenidas

Cabe recalcar que esta herramienta no va a solucionar ningún problema estratégico de la empresa, simplemente sirve para ver el funcionamiento de la misma de una forma global teniendo en cuenta aspectos más detallados.



## CAPITULO III

### 3. Descripción General De La Empresa

La operación de las oficinas de la empresa financiera se inicia el 21 de febrero de 1968, constituida como compañía de responsabilidad limitada.

A fines de 1968 el número de tarjeta habientes había llegado a 507, la afiliación de establecimientos fue de 210.

Inicialmente la compañía se orienta básicamente hacia el campo turístico. En 1974 se realiza el lanzamiento de la tarjeta de crédito internacional incrementándose de esta forma el número de socios considerablemente de 2.000 a 5.000. En este mismo año se vinculan empresarios a la compañía, definiéndose con ellos un plan agresivo de conocimiento y utilización de la tarjeta.

A inicios de 1987 se realiza la vinculación con el Banco de la localidad, unión que consolidó aún más el prestigio y solvencia de la empresa.

Hoy en día la empresa cuenta con más de 100.000 socios principales y una red de más de 15.000 establecimientos afiliados en todo el país.

#### 3.1. Departamento de Sistemas

El área de sistemas es un elemento común en las organizaciones modernas y ha venido sufriendo un cambio en el rol que representa dentro de la misma. Actualmente, el área de Sistema o de TI no sólo provee una amplia gama de servicios a la organización sino que también se involucra a nivel de cultura organizacional, plantea estrategias para el cumplimiento de los objetivos globales y busca generar ventajas competitivas dentro del entorno operativo de la organización.

#### 3.2. Funciones del área de TI

No todas las organizaciones tienen un área de TI, sin embargo cada vez son más las que apuestan por éste concepto ya que han visto la necesidad de administrar los recursos (talento

humano, hardware, software, presupuesto) de forma tal que sean utilizados eficientemente en beneficio de la organización. Es entonces la administración la principal labor de un departamento de TI y que conlleva una serie de procedimientos, políticas y estrategias para verdaderamente hacer de las TI un valor agregado y no una carga que impida la eficiencia operativa.

Desde un punto de vista algo simple, el área de TI es esencialmente un ente encargado de prestar servicios a otras áreas dentro de la organización (o fuera de ésta en algunos casos) tales como correo electrónico, control de usuarios, desarrollo, soporte, instalación y configuración de aplicaciones, mantenimiento de hardware y software, etc. Esta descripción se podría considerar como la “visión clásica” que se tiene del área de TI.

Algunas de las nuevas funciones del área de TI son:

- a) Crear la visión de TI de la organización y asegurar que ésta sea consecuente con la visión general del negocio. De ésta forma las TI serán una herramienta para la organización y no una carga.
- b) Generar una cultura de apropiación de las TI dentro de la organización.
- c) Desarrollar un plan en el cual las TI representen una ventaja competitiva.
- d) Alinear las TI con los objetivos de la organización.
- e) Administrar el talento humano relacionado con las TI incluyendo procesos como la creación de un organigrama y la delegación de funciones específicas.
- f) Definir y promover estándares para TI.
- g) Fomentar canales de comunicación claros y eficientes con los usuarios de TI.
- h) Gestionar estrategias para el mejoramiento continuo y sostenible de la calidad de los servicios de TI.
- i) Controlar los recursos de TI así como generar requerimientos de recursos nuevos.
- j) Desarrollar controles administrativos y de aplicación que permitan un uso seguro de las TI.
- k) Dar soporte a los usuarios de TI y proveerles información útil y oportuna según la soliciten.

### 3.3. Misión de Infraestructura y Networking

Proveer soluciones tecnológicas sólidas e innovadoras, que impacten de manera diferenciadora la experiencia de nuestros clientes internos y externos, garantizando velocidad, exactitud, consistencia y alta disponibilidad de la tecnología como base fundamental del desarrollo del negocio, contando para ello con recursos humanos de alta calificación y profundo conocimiento, plataformas tecnológicas de clase mundial, procesos de operación en mejora constante y garantizando un servicio de excelencia, anclados en la innovación y la mejora continua con aprendizaje.

### 3.4. Visión de Infraestructura y Networking

Apoyando el desarrollo del negocio y visionando oportunidades futuras.

### 3.5. Esquema Organizacional actual del área de Infraestructura y Networking

En la Figura 2 se puede ver el esquema organizacional actual del área de infraestructura y networking de la empresa.



Figura 2. Organigrama Estructural de Tecnología

### 3.6. Descripción de los servicios que prestan los departamentos

De acuerdo a la distribución del organigrama estructural actual de tecnología se pueden apreciar 3 bloques: Infraestructura y Networking, Redes y comunicaciones, y, Soporte a usuarios, donde:

Infraestructura y Networking.- Es la encargada de administrar, gestionar el servicio de hardware y software que garanticen la operación del negocio, mediante procedimientos definidos y personal responsable, innovador, dinámico con capacidad de optimizar el uso de la plataforma tecnológica.

Redes y comunicaciones.- Es la encargada de garantizar y diseñar los diferentes enlaces de las redes LAN y WAN de la empresa así como el garantizar el correcto funcionamiento de los sistemas de telefonía que se encuentran bajo ésta área.

Soporte a usuarios.- Esta área se encarga de gestionar, direccionar garantizar el buen funcionamiento de los equipos de computación de la organización así como de resolver los requerimientos de primer nivel en el menor tiempo posible. Para de esta manera minimizar los impactos que puedan ocasionar los desperfectos en los equipos.

### 3.7. Tipificación de los servicios que manejan las áreas de Sistemas

En la tabla 1, se presenta un listado de las tipificaciones de los servicios que prestan las áreas, las tipificaciones que están en color rojo son lo que se han identificado que deben ser entregados a otras áreas luego de la reestructuración del área de Sistemas.

**Tabla 1.**  
Tipificaciones de Servicios

Tipificación de servicios por áreas				
Área	Nivel 1	Nivel 2	Nivel 3	Nombre del servicio
Infraestructura y Networking	Hardware	Celular	BlackBerry	Configuración de equipos BlackBerry en el servidor
Service Desk	Hardware	Celular	BlackBerry	Configuración y personalización de equipos BlackBerry
Service Desk	Hardware	Celular	IPhone	Configuración de equipos IPhone 4
Service Desk	Hardware	Componente	Cambio CPU/Local	Cambio CPU-equipo nuevo
Service Desk	Hardware	Componente	Formateo CPU/Local	Formateo CPU
Service Desk	Hardware	Componente	Cambio CPU/P. Servicio	Cambio CPU-equipo nuevo
Service Desk	Hardware	Componente	Formateo CPU/P. Servicio	Formateo CPU
Service Desk	Hardware	Componente	Formateo CPU/Provincias	Formateo CPU
Service Desk	Hardware	Componente	Cambio CPU/Provincias	Cambio CPU-equipo nuevo
Service Desk	Hardware	Componente	Cambio LAPTOP/Local	Cambio LAPTOP-equipo nuevo
Service Desk	Hardware	Componente	Formateo LAPTOP/Local	Formateo LAPTOP
Service Desk	Hardware	Componente	Cambio LAPTOP/P. Servicio	Cambio LAPTOP-equipo nuevo
Service Desk	Hardware	Componente	Formateo LAPTOP/Sitio	Formateo LAPTOP
Service Desk	Hardware	Componente	Formateo LAPTOP/Provincias	Formateo LAPTOP
Service Desk	Hardware	Componente	Cambio LAPTOP/Provincias	Cambio LAPTOP-equipo nuevo
Service Desk	Hardware	Garantías	CPU	Aplicar garantía CPU
Service Desk	Hardware	Garantías	Disco duro	Aplicar garantía Disco duro
Service Desk	Hardware	Garantías	Memorias	Aplicar garantía Memorias

CONTINUA →

Service Desk	Hardware	Garantías	Monitor	Aplicar garantía Monitor
Service Desk	Hardware	Garantías	Mouse	Aplicar garantía Mouse
Service Desk	Hardware	Garantías	Partes y Piezas	Aplicar garantía Partes y Piezas
Service Desk	Hardware	Garantías	PCs Portátil	Aplicar garantía PCs Portátil
Service Desk	Hardware	Garantías	Teclado	Aplicar garantía Teclado
Service Desk	Hardware	Periféricos	Disco Duro	Interno-Formateo
Service Desk	Hardware	Periféricos	Memoria	Cambio o aumento de Memoria
Service Desk	Hardware	Periféricos	Scanner	Instalación o Configuración Scanner Genérico
Service Desk	Hardware	Periféricos	Monitor/P. Servicio	Cambio Monitor
Service Desk	Hardware	Periféricos	Mouse/Local	Cambio Mouse
Service Desk	Hardware	Periféricos	CD-ROM/Local	Cambio CD-ROM
Service Desk	Hardware	Periféricos	Teclado/Local	Cambio Teclado
Service Desk	Hardware	Periféricos	Teléfono/Analógico/P. de Servicio	Analógico
Service Desk	Hardware	Periféricos	Teléfono/IP/P. de Servicio	IP
Service Desk	Hardware	Periféricos	Monitor/Provincias	Monitor
Service Desk	Hardware	Periféricos	Mouse/P. Servicio.	Mouse
Service Desk	Hardware	Periféricos	CD-ROM/P. Servicio	CD-ROM
Service Desk	Hardware	Periféricos	Teclado/P. Servicio	Teclado
Service Desk	Hardware	Periféricos	Teléfono/Analógico/Provincias	Analógico
Service Desk	Hardware	Periféricos	Teléfono/IP/Provincias	IP
Service Desk	Hardware	Periféricos	SWITCH	SWITCH

CONTINUA →

Service Desk	Hardware	Periféricos	Hub	Hub
Service Desk	Hardware	Periféricos	Sonido	Sonido PC
Service Desk	Hardware	Periféricos	USB	USB PC
Service Desk	Hardware	Periféricos	Cable de red	Cable de red Genérico
Service Desk	Hardware	Periféricos	Cámara Fotográfica	Cámara Fotográfica Genérico
Service Desk	Hardware	Periféricos	Lector de Barras	Lector de Barras Genérico
Service Desk	Hardware	Periféricos	Monitor/Local	Monitor
Service Desk	Hardware	Periféricos	Mouse/Provincias	Mouse
Service Desk	Hardware	Periféricos	CD-ROM/Provincias	CD-ROM
Service Desk	Hardware	Periféricos	Parlantes	Parlantes Genéricos Samsung
Service Desk	Hardware	Periféricos	Retro Proyector	Soporte Infocus
Service Desk	Hardware	Periféricos	Teclado/Provincias	Teclado
Service Desk	Hardware	Periféricos	Teléfono/Analógico/Local	Instalación o re-ubicación Analógico
Service Desk	Hardware	Periféricos	Teléfono/IP/Local	Instalación o re-ubicación IP
Service Desk	Hardware	Periféricos	Video	Pc Videos Otros
Service Desk	Hardware	Periféricos	Configurar red	Configurar tarjeta de red
Service Desk	Software	Aplicaciones	Base de datos	SQL Server
Service Desk	Software	Aplicaciones	Bridge	Instalación Bridge
Service Desk	Software	Aplicaciones	Control Telefónico Call Center	Instalación Genesys
Service Desk	Software	Aplicaciones	Creación de Base Local	Creación de Base Local
Service Desk	Software	Aplicaciones	Icono de AS400 transferencia	Instalación Icono de transferencia AS400
CONTINUA →				

Service Desk	Software	Aplicaciones	Icono de AS400 transferencia	Instalación Icono de transferencia AS400
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación o Configuración Microsoft Office
Service Desk	Software	Aplicaciones	Parche	Instalación Parche AS400
Service Desk	Software	Aplicaciones	Permisos	Permisos a Carpetas Compartidas
Service Desk	Software	Aplicaciones	Permisos	Configuración Escritorio Remoto
Service Desk	Software	Aplicaciones	Programación	Instalación Crystal Xcelsius
Service Desk	Software	Aplicaciones	Programación	Instalación Plex
Service Desk	Software	Aplicaciones	Programación	Instalación Source Safe 2003
Service Desk	Software	Aplicaciones	Programación	Instalación Visual Estudio
Service Desk	Software	Aplicaciones	Sistema Operativo	Actualizaciones Parches
Service Desk	Software	Aplicaciones	Software de Fotos	Instalación Software de Fotos
Service Desk	Software	Aplicaciones	Software de Turnos	Instalación Software de Turnos
Service Desk	Software	Aplicaciones	Clear Quest	Instalación Clear Quest
Service Desk	Software	Aplicaciones	Clear Case	Instalación Clear Case
Service Desk	Software	Aplicaciones	Cristal Report	Instalación Cristal Report
Service Desk	Software	Aplicaciones	VISA Edit Package	Instalación o actualización VISA Edit Package
Service Desk	Software	Aplicaciones	Visa_Interchange	Instalación o actualización Visa_Interchange
Service Desk	Software	Aplicaciones	RespalDOS Datacard	RespalDOS Datacard
Service Desk	Software	Aplicaciones	Recuperación de RespalDOS	Recuperación de RespalDOS
Service Desk	Software	Aplicaciones	Sistema Operativo	Instalación Windows
Service Desk	Software	Aplicaciones	Envió Paquetería	Urbano Esxpress
CONTINUA →				



Service Desk	Software	Aplicaciones	Requerimientos	Remedy/Generación de Ticket
Service Desk	Software	Aplicaciones	Claves	CAO CONECTOR
Service Desk	Software	Aplicaciones	Claves	CAO GRAFICO
Service Desk	Software	Aplicaciones	Claves	Claves Banco Loja
Service Desk	Software	Aplicaciones	Claves	Claves Pc Sistel
Service Desk	Software	Aplicaciones	Claves	Reseteo de Claves/AS400 Producción y Desarrollo
Service Desk	Software	Aplicaciones	Claves	PROVEEDURÍA
Service Desk	Software	Aplicaciones	Claves	Claves Banco Pichincha
Service Desk	Software	Aplicaciones	Claves	Claves Banco Rumiñahui
Service Desk	Software	Aplicaciones	Claves	Claves Banco Machala
Service Desk	Software	Aplicaciones	Acrobat Reader	Instalación Acrobat Reader
Service Desk	Software	Aplicaciones	Antivirus	Instalación Symantec Endpoint Protección
Service Desk	Software	Aplicaciones	CAO Desarrollo	Instalación CAO Desarrollo
Service Desk	Software	Aplicaciones	CAO Producción	Instalación CAO Producción
Service Desk	Software	Aplicaciones	Captura Pantallas	Instalación Snagit
Service Desk	Software	Aplicaciones	Compresores	Instalación WinRar
Service Desk	Software	Aplicaciones	Compresores	Instalación WinZip
Service Desk	Software	Aplicaciones	Configuración Teclados	Configuración Teclados AS400
Service Desk	Software	Aplicaciones	ContraCargo	Instalación Contra Cargo (internacional)
Service Desk	Software	Aplicaciones	Flash Player	Instalación Flash Player
Service Desk	Software	Aplicaciones	FTP/SFTP	Instalación FTP/SFTP
				CONTINUA →

Service Desk	Software	Aplicaciones	Icono de AS400 desarrollo	Instalación y configuración AS400 Desarrollo
Service Desk	Software	Aplicaciones	Icono de AS400 contingencia	Instalación y configuración Icono de contingencia AS400
Service Desk	Software	Aplicaciones	Texpad	Instalación Texpad
Service Desk	Software	Aplicaciones	Java	Instalación o actualización de Java
Service Desk	Software	Aplicaciones	Multimedia	Instalación Quick Time
Service Desk	Software	Aplicaciones	PARCHES	Instalación Cubos para Información
Service Desk	Software	Aplicaciones	Proveeduría	Instalación Proveeduría
Service Desk	Software	Aplicaciones	Seguridad	Configuración Firewall Sistema Operativo
Service Desk	Software	Aplicaciones	SMS	Instalación SMS
Service Desk	Software	Aplicaciones	DLP	Instalación DLP
Service Desk	Software	Aplicaciones	Red Datacard	Red Datacard
Service Desk	Software	Aplicaciones	SAR	Instalación SAR
Service Desk	Software	Aplicaciones	Certificados Bco. Central.	Instalación Plugging Banco Central
Service Desk	Software	Aplicaciones	Content Manager OnDemand	Instalación Content Manager OnDemand
Service Desk	Software	Aplicaciones	Control Telefónico	C. Telefónico Pc Sistel
Service Desk	Software	Aplicaciones	SRI	Instalación SRI
Service Desk	Software	Aplicaciones	Mensajería	Instalación Messenger
Service Desk	Software	Aplicaciones	Riesgo Operativo	Instalación Riesgo Operativo
Service Desk	Software	Aplicaciones	RespalDOS Datacard	RespalDOS Datacard
Service Desk	Software	Aplicaciones	Soporte Cafetería	Configuración Software de Cafetería
Service Desk	Software	Aplicaciones	Pc Trader	Instalación y Configuración Pc Trader
CONTINUA →				

Service Desk	Software	Aplicaciones	Firefox	Instalación Firefox
Service Desk	Software	Aplicaciones	Bines Visa	Instalación Visa Interchange
Service Desk	Software	Aplicaciones	Card Courier	Instalación Card Courier
Service Desk	Software	Aplicaciones	Estadística	Instalación SPSS12
Service Desk	Software	Aplicaciones	Estadística	Instalación SPSS16
Service Desk	Software	Aplicaciones	File Magister	Instalación o configuración File Magister
Service Desk	Software	Aplicaciones	Framework	Instalación Framework
Service Desk	Software	Aplicaciones	HP Bridge	Instalación Plugging Diners
Service Desk	Software	Aplicaciones	IDEA	Instalación IDEA
Service Desk	Software	Aplicaciones	Internet Explorer 6	Instalación Internet Explorer 6
Service Desk	Software	Aplicaciones	Internet Explorer 7	Instalación Internet Explorer 7
Service Desk	Software	Aplicaciones	Mensajería	Instalación Skype
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación Microsoft Office Outlook
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación Microsoft Office Excel
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación Microsoft Office Word
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación Microsoft Office PowerPoint
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación Microsoft Office Visio
Service Desk	Software	Aplicaciones	Microsoft Office	Instalación Microsoft Office Project
Service Desk	Software	Aplicaciones	Multimedia	Instalación iTunes
Service Desk	Software	Aplicaciones	Quemador de CD	Instalación Nero
Service Desk	Software	Aplicaciones	Red	Cambio de Vlans.
CONTINUA →				

Service Desk	Software	Aplicaciones	Software para DVD	Instalación Power - DVD
Service Desk	Software	Aplicaciones	Transferencia de Archivos	Instalación STP-WIN
Service Desk	Software	Aplicaciones	Visa	Instalación Visa
Service Desk	Software	Aplicaciones	MasterCard_Memberd_Directory	Instalación MasterCard_Memberd_Directory
Service Desk	Software	Aplicaciones	MASTERCARD Edit Package	Instalación MASTERCARD Edit Package
Infraestructura y Networking	Hardware	Servidores	Actualizaciones Firmware	Actualizaciones Firmware
Infraestructura y Networking	Hardware	Servidores	Actualizaciones Micro-Código	Actualizaciones Micro-Código
Infraestructura y Networking	Hardware	Servidores	Alerta Discos	Alerta Discos
Infraestructura y Networking	Hardware	Servidores	Asignación de espacio en SAN	Asignación de espacio en SAN
Infraestructura y Networking	Hardware	Servidores	Baja de servidores	Baja de servidores
Infraestructura y Networking	Hardware	Servidores	Cambio Discos	Cambio Discos
Infraestructura y Networking	Hardware	Servidores	Casos Global Crossing	Casos Global Crossing
Infraestructura y Networking	Hardware	Servidores	Casos IBM	Casos IBM
Infraestructura y Networking	Hardware	Servidores	Casos Maint	Casos Maint
Infraestructura y Networking	Hardware	Servidores	Creación de Raid	Creación de Raid
CONTINUA →				

Infraestructura y Networking	Hardware	Servidores	Formateo Servidores	Formateo Servidores (Linux, AIX, Windows)
Infraestructura y Networking	Hardware	Servidores	Monitoreo San	Monitoreo San
Infraestructura y Networking	Hardware	Servidores	Servidores	Preparación de Servidores (AIX, Linux, Windows) VMWare
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Instalación SQL Server
Infraestructura y Networking	Software	Servidores	Antivirus Servidores	Instalación Antivirus Servidores
Infraestructura y Networking	Software	Servidores	Aplicaciones Discover	Instalación Aplicaciones Discover
Infraestructura y Networking	Software	Servidores	Aplicaciones Linux	Instalación Aplicaciones Linux
Infraestructura y Networking	Software	Servidores	Aplicaciones Mip	Instalación Aplicaciones Mip
Infraestructura y Networking	Software	Servidores	Aplicaciones Servidores Global Crossing	Instalación Aplicaciones Servidores Global Crossing
Infraestructura y Networking	Software	Servidores	Aplicaciones Servidores Gye	Instalación Aplicaciones Servidores Gye
Infraestructura y Networking	Software	Servidores	Aplicaciones Visa	Instalación Aplicaciones Visa
Infraestructura y Networking	Software	Servidores	Aplicaciones VMWare/vsphere	Instalación Aplicaciones VMWare/vsphere
Infraestructura y Networking	Software	Servidores	Carpetas Compartidas	Carpetas Compartidas
Infraestructura y Networking	Software	Servidores	Certificados SSL	Instalación y configuración Certificados SSL
CONTINUA →				

Infraestructura y Networking	Software	Servidores	Correo Electrónico	Correo Electrónico
Infraestructura y Networking	Software	Servidores	Portal Web	Revisión Portal Web
Infraestructura y Networking	Software	Servidores	PSOFT Aplicativo	PSOFT Aplicativo
Infraestructura y Networking	Software	Servidores	PSOFT BDatos	PSOFT BDatos
Infraestructura y Networking	Software	Servidores	PSOFT Calendarizador de Procesos	PSOFT Calendarizador de Procesos
Infraestructura y Networking	Software	Servidores	PSOFT CTI	PSOFT CTI
Infraestructura y Networking	Software	Servidores	PSOFT FTP	PSOFT FTP
Infraestructura y Networking	Software	Servidores	PSOFT Reportes	PSOFT Reportes
Infraestructura y Networking	Software	Servidores	Revisar Permisos Internet	Revisar Permisos Internet
Infraestructura y Networking	Software	Servidores	SCOM	Administración SCOM
Infraestructura y Networking	Software	Servidores	Sistemas Seguridades	Sistemas Seguridades
Infraestructura y Networking	Software	Aplicaciones	SMS	Instalación agente SMS
Infraestructura y Networking	Software	Aplicaciones	TSM	Instalación agente TSM
Infraestructura y Networking	Software	Aplicaciones	WAS Pasivos	Revisión WAS Pasivos
CONTINUA →				

Infraestructura y Networking	Software	Aplicaciones	People Soft	Inconsistencia Base de Datos
Infraestructura y Networking	Software	Aplicaciones	People Soft	Clave Caducada
Infraestructura y Networking	Software	Aplicaciones	People Soft	Lentitud Despliegue Información
Infraestructura y Networking	Software	Aplicaciones	People Soft	No Carga AS400 Web Hats
Infraestructura y Networking	Software	Aplicaciones	People Soft	Caída Comunicación Central Riesgo (no puede abrir el archivo)
Infraestructura y Networking	Software	Aplicaciones	People Soft	Caída Proceso Lotes (no se carga número tarjeta)
Infraestructura y Networking	Software	Aplicaciones	People Soft	Carga Promociones de Cobranzas
Infraestructura y Networking	Software	Aplicaciones	People Soft	Demoras en la vista 360
Infraestructura y Networking	Software	Aplicaciones	People Soft	No parametrización de Agentes (no visualización casos creados)
Infraestructura y Networking	Software	Aplicaciones	People Soft	People Soft Falla Canal de Comunicación
Infraestructura y Networking	Software	Aplicaciones	People Soft	Venta Potencial/Oportunidad (al atar un contacto no existe)
Infraestructura y Networking	Software	Aplicaciones	People Soft	Usuario no puede loguear en Sistema PS
Infraestructura y Networking	Software	Aplicaciones	Permisos	Asigna permisos de Internet (usuario nuevo)
Infraestructura y Networking	Software	Aplicaciones	Internet Information Server	Configuración IIS
CONTINUA →				

Infraestructura y Networking	Software	Aplicaciones	Base de datos	Depuración Logs
Infraestructura y Networking	Hardware	Periféricos	Red	Creación nuevo punto de red
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Movimiento de datos
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Actualización de datos
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Crear bases de datos
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Configurar bases de datos
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Activar bases de datos
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Desactivar bases de datos
Infraestructura y Networking	Software	Aplicaciones	Base de datos	Eliminar bases de datos
Service Desk	Software	Aplicaciones	DLP McAfee	Instalación del agente en estaciones de trabajo
Service Desk	Software	Aplicaciones	Sophos	Instalación del agente en estaciones de trabajo
Service Desk	Software	Aplicaciones	AS400	Reseteos de Claves: Gestor, CAO, PRUEBAID, DESARRID, WEBID, TESTPE, GESTORPE, AUTPE
Service Desk	Software	Aplicaciones	Backdoor	Reseteo de Claves
Service Desk	Software	Aplicaciones	People Soft	Reseteo de Claves
Service Desk	Software	Aplicaciones	Active Directory	Reseteo de Claves
CONTINUA →				



Control Tecnológico	Software	Aplicaciones	Generación de pines	Generación de pines nuevos
Control Tecnológico	Software	Aplicaciones	AS400 Gestor	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	AS400 Gestor	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	AS400 Gestor	Creación, modificación, eliminación de usuarios (externos)
Control Tecnológico	Software	Aplicaciones	AS400 CAO	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	AS400 CAO	Creación, modificación, eliminación de usuarios (externos)
Control Tecnológico	Software	Aplicaciones	AS400 Desarrollo y Pruebas	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Active Directory	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Cubos	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	People Soft	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	People Soft	Creación, modificación, eliminación de usuarios (externos)
Control Tecnológico	Software	Aplicaciones	DLP McAfee	Habilitación de periféricos almacenamiento masivo
Control Tecnológico	Software	Aplicaciones	Backdoor	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Backdoor	Creación, modificación, eliminación de usuarios (externos)
CONTINUA →				

Control Tecnológico	Software	Aplicaciones	JDEdwards	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Powerlock	Habilitación de subida y bajada de archivos AS400
Control Tecnológico	Software	Aplicaciones	SFTP Jscape	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	SFTP Jscape	Creación, modificación, eliminación de usuarios (externos)
Control Tecnológico	Software	Aplicaciones	VPN Juniper	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Iron Port	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Bridge	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Administración de Contratos	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Risk Control	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	Siglo 21	Creación, modificación, eliminación de usuarios (internos)
Control Tecnológico	Software	Aplicaciones	SFTP Jscape	Reseteo de Claves usuarios internos
Control Tecnológico	Software	Aplicaciones	SFTP Jscape	Reseteo de Claves usuarios internos
Control Tecnológico	Software	Aplicaciones	Risk Control	Reseteo de Claves usuarios internos
Control Tecnológico	Software	Aplicaciones	Solicitud de respaldos AS400	Solicitud de respaldos
CONTINUA →				

Centro de Cómputo	Hardware	Servidores	Casos IBM	Casos IBM plataforma AS400
Centro de Cómputo	Software	Aplicaciones	AS400	Actualización de zonas Dineros y Visa
Service Desk	Software	Aplicaciones	AS400	Configuración de macro para impresión de reportes generados por usuario en el AS400
Centro de Cómputo	Software	Aplicaciones	AS400	Conversión spools a texto
Centro de Cómputo	Software	Aplicaciones	Barcelona	Creación de alarmas monitoreo de servicios
Centro de Cómputo	Software	Aplicaciones	Content Manager OnDemand	Creación de aplicaciones para almacenamiento estados de cuenta y reportes en ondemand
Centro de Cómputo	Software	Aplicaciones	Filenet	Creación de aplicaciones para digitalización documentos en filenet
Centro de Cómputo	Software	Aplicaciones	Barcelona	Creación y actualización de dashboard (vistas) para monitoreo de servicios
Centro de Cómputo	Software	Aplicaciones	AS400	Creación y configuración de colas de impresión en el AS400
Service Desk	Software	Aplicaciones	Grabación CD	Grabación medios magnéticos
Service Desk	Software	Aplicaciones	Impresiones	Impresión de label's
Centro de Cómputo	Software	Aplicaciones	Impresiones	Impresión de pines
Centro de Cómputo	Software	Aplicaciones	Impresiones	Impresión de reportes
Centro de Cómputo	Software	Aplicaciones	Impresiones	Reimpresión de comprobantes
Service Desk	Software	Aplicaciones	Claves	Reseteo de claves AS400 y CAO Gráfico en ambiente de producción y pruebas
Service Desk	Software	Aplicaciones	Content Manager OnDemand	Reseteo de claves Content Manager
Centro de Cómputo	Software	Aplicaciones	AS400	Revisión de incidentes reportados por usuario en el AS400
				CONTINUA →

Service Desk	Software	Aplicaciones	Impresiones	Soporte problemas de impresión en el AS400
Centro de Cómputo	Software	Aplicaciones	FTP/SFTP	Transmisión de archivos de insertos para Urbano Express
Control Tecnológico	Software	Aplicaciones	AS400	Acceso sistema FTP AS400
Control Tecnológico	Software	Aplicaciones	Content Manager OnDemand	Acceso sistema Content Manager
Centro de Cómputo	Hardware	Aplicaciones	AS400	Configurar recursos Hardware

### 3.8. Servicios que manejan las áreas de Sistemas

En la tabla 2, se presenta un listado de los principales servicios y el área responsable.

**Tabla 2.**  
Servicios y áreas responsables

No.	SERVICIOS	DESCRIPCIÓN	RESPONSABLE
1	Habilitar la comunicación entre dos puntos, enlaces WAN.	Se realiza el análisis y la necesidad de comunicación para implementar una solución de comunicación entre dos puntos que necesita acceder a la red de Diners.	Comunicaciones
2	Habilitar permisos de acceso desde/hacia redes externas que se encuentran en la DMZ.	Se habilita los permisos en el Firewall de borde para el acceso desde/hacia las redes de Proveedores y Socios de Negocio.	Comunicaciones
3	Habilitar comunicaciones VPN punto a punto.	Se realiza las configuraciones según el requerimiento previamente aprobado manteniendo los estándares de seguridad y encriptación del canal.	Comunicaciones
4	Habilitar nuevas redes LAN.	Se habilita nuevas redes internas conforme requerimiento de la Empresa o remodelación de las mismas.	Comunicaciones
5	Seguridad Perimetral.	Control de permisos entrantes y salientes a la red interna en los Firewalls de DMZ e Internet.	Comunicaciones
6	Administración del acceso desde/hacia la red del portal en el Hosting de Global Crossing.	Se realiza el análisis y la necesidad de la Empresa para implementar o mejorar soluciones en nuestro portal y elaborar el requerimiento al SOC que administra el Firewall de borde en el Hosting de Global crossing.	Comunicaciones
			CONTINUA →

7	Administración y monitoreo de las redes LAN, WAN y Telefónico a nivel nacional.	Cumplir los ANS propuestos y contratados	Comunicaciones
8	Diseño y configuración de Redes LAN y WAN.	Permite ampliar la entrega de los servicios que Dinera/Ínterin va desarrollando y/o mejorando.	Comunicaciones
9	Actualización Tecnológica.	Diseñar, dimensionar y configurar la nueva infraestructura tecnológica tanto a nivel de equipos como de conectividad permitiendo mejorar de manera más óptima los servicios que ofrece la Empresa.	Comunicaciones
10	Centro de Contingencia GYE.	Diseñar, configurar y administrar la infraestructura de networking de nuestro DataCenter en Guayaquil.	Comunicaciones
11	Nodo Alterno, Centro de Contingencia UIO	Diseñar, Dimensionar y configurar un DataCenter de contingencia en Quito a nivel de comunicaciones que permita poder comunicarse a Quito con el DataCenter de GYE en caso de desastre total del DataCenter principal de Quito.	Comunicaciones
12	Voz y Telefonía IP	Diseño y configuración de un sistema de voz sobre IP y telefonía IP tanto interprovincial como local.	Comunicaciones
13	Administración de la Central Telefónica	Controlar los niveles de servicio telefónico a la Empresa de tal manera de cumplir con los ANS ofrecidos.	Comunicaciones
			CONTINUA →

14	Instalación de una extensión telefónica.	Se habilita una extensión telefónica al usuario con el nivel de salida y permisos que se soliciten.	Comunicaciones
15	Instalación y configuración de acceso de troncales (analógicas, Digitales, E1) y servicios 1800.	Se habilita en la Central telefónica el acceso de troncales que la Empresa solicita y también los accesos de los servicios 1800.	Comunicaciones
16	Servicios de CCD para Call Center	Se habilita y controla el servicio CCD para los diferentes servicios que presta el Call Center.	Comunicaciones
17	Monitoreo de todo el sistema telefónico provisto por CNT y operadoras de telefonía celular	Se realiza un control diario de la calidad del servicio de todo el sistema telefónico.	Comunicaciones
18	SOPORTE A USUARIOS CALL CENTER SISTEMA GENESYS	Se realiza un soporte de todos los inconvenientes que tienen los usuarios del Call Center respecto al CTI Genesys.	SERVIDORES
19	SOPORTE A USUARIOS CALL CENTER SISTEMA PEOPLE SOFT	Se realiza un soporte de todos los inconvenientes que tienen los usuarios del Call Center en PeopleSoft y la integración con CTI Genesys.	SERVIDORES
20	REVISIÓN Y MONITOREO DE SERVICIOS PLATAFORMA GENESYS	Se realiza un monitoreo y control de todos los servicios y aplicaciones que conforman el sistema de CTI Genesys.	SERVIDORES
21	CREACIÓN DE USUARIOS, CAMPAÑAS, LISTAS DE MARCACIÓN, ETC., EN PLATAFORMA GENESYS	Se administran y se crean todos los objetos de telefonía que tienen que ver con el funcionamiento de Call Center en la Plataforma CTI Genesys.	SERVIDORES
CONTINUA →			

22	CONFIGURACION DE CAMPAÑAS, LISTAS DE MARCACION Y USUARIOS DE CALL CENTER EN SISTEMA PEOPLE SOFT	Se realizan tareas de creación y usuarios, campañas, listas de marcación y consultas para la creación de campañas en el sistema People Soft. Todo esto relacionado al PS y la integración con el CTI Genesys.	SERVIDORES
23	ADMINISTRACIÓN DE PLATAFORMA GENESYS.	Se realiza la administración, depuración y control de la Plataforma Genesys.	SERVIDORES
24	DESARROLLOS RELACIONADOS CON EL CTI.	Se da mantenimiento y se realizan algunos desarrollos de aplicativos que son parte de la integración PS-Genesys y de los diversos procesos que son parte de la integración.	SERVIDORES
25	Habilitar el permiso de acceso a Internet de un usuario en el servidor ISA y/o Websense.	Se habilita el permiso de Internet en base al perfil de usuario y a la solicitud.	SERVIDORES
26	Configuración e Instalar un Servidores Web para publicación de sitios.	Instalar y configurar un servidor web para una funcionalidad requerida con los niveles de parches adecuados, probado y funcionando.	SERVIDORES
27	Adquisición de un nombre de dominio	Validar la disponibilidad, adquirir un nombre de dominio en el internet si existiere o sugerir el mismo.	SERVIDORES
28	Instalación de un Certificado Digital	Instalar certificados digitales en los sitios web de la organización	SERVIDORES
29	Preparación de un nuevo servidor físico Windows	Instalar el sistema operativo con los niveles de parches adecuados.	SERVIDORES
			CONTINUA →



30	Preparación de un nuevo servidor virtual Windows	Creación del nuevo servidor de acuerdo a los requerimientos de hardware y software.	SERVIDORES
31	Preparación de un nuevo servidor AIX físico	Instalación y configuración del sistema operativo, configuración de recursos de hardware y software de acuerdo a requerimientos.	SERVIDORES
32	Preparación de un nuevo servidor AIX con LPARS	Instalación de Sistema Operativo VIOS y configuración e instalación de sistema operativo en particiones LPARS	SERVIDORES
33	Preparación de un nuevo servidor Linux físico	Instalación de sistema operativo, y configuraciones de acuerdo a requerimientos.	SERVIDORES
34	Preparación de un nuevo servidor Linux virtual	Instalación y configuración del sistema operativo, configuración de recursos de hardware y software de acuerdo a requerimientos.	SERVIDORES
35	Administración de hardware de los servidores	Administración de elementos de hardware, discos, CPU, memoria. Configuraciones, distribución, disponibilidad.	SERVIDORES
36	Administración de software de los servidores	Administrar el software, sistema operativo, aplicaciones, nuevos parches, verificación de disponibilidad y rendimientos adecuados de acuerdo a ANS establecidos	SERVIDORES
37	Administración de las seguridades de los servidores	Eliminar vulnerabilidades, manejo adecuado de credenciales de usuario, niveles de parches de seguridad.	SERVIDORES
			CONTINUA →

38	Creación de Bases de Datos SQL Server	Creación y configuración de nuevas bases de datos de acuerdo a requerimientos de las aplicaciones	SERVIDORES
39	Eliminación de Bases de Datos SQL Server	Eliminar bases de datos que no se usan o han sido migradas a otros equipos	SERVIDORES
40	Administración de espacio de Bases de Datos SQL Server	Depuración de logs, incremento de espacio de acuerdo a crecimiento de las bases de datos, depuración de información.	SERVIDORES
41	Tuning de bases de datos SQL Server	Mejoras de rendimiento, configuraciones de parámetros de uso de recursos, revisión de queries, e indexaciones	SERVIDORES
42	Migraciones de bases de datos SQL Server	Migraciones a nuevas versiones o nuevos servidores de bases de datos.	SERVIDORES
43	Configuraciones de bases de datos SQL Server	Configuración de parametrizaciones de las bases de datos, uso de recursos, asignación de espacio, archivos de data y logs.	SERVIDORES
44	Administrar seguridades de una base de datos SQL Server	Configurar usuarios, permisos, roles, accesos.	SERVIDORES
45	Creación de esquemas de Bases de Datos Oracle	Creación de nuevos esquemas de bases de datos de acuerdo a requerimientos de las aplicaciones	SERVIDORES
46	Eliminación de esquemas de Bases de Datos Oracle	Eliminación de los esquemas que ya no se utilicen, o que hayan sido migrados a otros servers o bases de datos	SERVIDORES
			CONTINUA →

47	Administración de espacio de Bases de Datos Oracle	Monitoreo de espacio disponible, incremento de espacio necesario, depuración de información, depuración de objetos, movimiento de data.	SERVIDORES
48	Tuning de bases de datos Oracle	Monitoreo de rendimiento, optimización de queries, indexaciones, modificación de parámetros de rendimiento, reportes de opciones de mejora, monitoreo de carga.	SERVIDORES
49	Movimiento de data en bases de datos Oracle	Exportación e importación de data, entre bases de datos y/o servidores.	SERVIDORES
50	Respaldos de bases de datos Oracle	Obtención de respaldos periódicos.	SERVIDORES
51	Contingencia de bases de datos Oracle	Montar infraestructura para contingencia de la base de datos, monitoreo de disponibilidad de contingencia.	SERVIDORES
52	Réplica de bases de datos Oracle	Armar la réplica de la base de datos Oracle, tener una réplica en línea, pruebas de replicación.	SERVIDORES
53	Administrar servidores de procesos del sistema CRM Peoplesoft	Monitoreo de rendimiento y disponibilidad, configuración de parametrizaciones, y administración de recursos y carga de procesos	SERVIDORES
54	Administrar servidores de aplicaciones del sistema CRM Peoplesoft	Monitoreo de rendimiento y disponibilidad, configuración, parametrizaciones, y administración de recursos y carga de aplicativo, balanceo de carga.	SERVIDORES
			CONTINUA →

55	Administrar servidores web del sistema CRM Peoplesoft	Monitoreo de rendimiento y disponibilidad, configuración de balanceo de carga de servidores, parametrizaciones, y administración de recursos, configuración de parámetros de uso de recursos.	SERVIDORES
56	Administrar integración de sistema CRM Peoplesoft con AS400	Configuración de integración con Hats, login, webservices, pasarelas.	SERVIDORES
57	Administrar integración de sistema CRM Peoplesoft con CTI-Genesys	Configuración de integración, webservices, sincronizaciones.	SERVIDORES
58	Configuraciones de filtro de correo smtp Linux	Configuración de parámetros, colas, flujo de correo	SERVIDORES
59	Reportaría de filtro de correo smtp Linux	Reportes de correos entrantes y salientes	SERVIDORES
60	Administración de seguridad de smtp brightmail	Creación y administración de usuarios, grupos de filtrado, políticas.	SERVIDORES
61	Configuraciones de filtro de correo smtp brightmail	Configuración de parámetros, colas, flujo de correo	SERVIDORES
62	Reporteria de filtro de correo smtp brightmail	Reportes de correos entrantes y salientes	SERVIDORES
63	Administración de seguridad de smtp brightmail	Creación y administración de usuarios, grupos de filtrado, políticas.	SERVIDORES
64	Creación de buzones de correo electrónico	Creación de nuevos buzones, grupos de distribución	SERVIDORES
65	Administración de seguridad de Exchange	Permisos, accesos owa	SERVIDORES
66	Reportaría de Exchange	Reportes de correos, entregas, recepción, errores, etc.	SERVIDORES
			CONTINUA →

67	Administración del sistema de antivirus de la organización.	Administrar el sistema de antivirus, políticas, grupos, actualización de definiciones	SERVIDORES
68	Actualizaciones de información en bases de datos	Actualizar información de bases de datos específicas ejemplo: Focus Financiero	SERVIDORES
69	Actualización de información de sistemas específicos	Actualizar información de sistemas específicos ejemplo: Fiel Magister	SERVIDORES
70	Administración del sistema de BlackBerry de gerencias y usuarios	Administración de disponibilidad y rendimiento del servicio, permisos.	SERVIDORES
71	Monitoreo de disponibilidad de los servicios de datawarehouse	Verificación de disponibilidad, rendimiento	SERVIDORES
72	Monitoreo de disponibilidad y rendimiento de los servidores	Sistema de monitoreo proactivo de todos los servidores, configuraciones de alertas y umbrales de criticidad.	SERVIDORES
73	Monitoreo de disponibilidad y rendimiento de los sistemas que funcionan en los servidores	Monitoreo diario de los sistemas que funcionan en todos los servidores, verificación de rendimiento y disponibilidad.	SERVIDORES
74	Migraciones de bases de datos	Migraciones a nuevas versiones o nuevos servidores.	SERVIDORES
75	Administración de servidores de archivos	Administración de permisos de carpetas, seguridad de las mismas, migraciones de información, etc.	SERVIDORES
76	Monitoreo de disponibilidad del sistema Bridge	Monitoreo del servidor y el sistema bridge con DCI.	SERVIDORES
77	Administración de WAS del portal web	Administración de rendimiento, disponibilidad, configuraciones	SERVIDORES
CONTINUA →			

78	Administración de base de datos del portal Web	Monitoreo de disponibilidad y rendimiento, respaldos de la base de datos	SERVIDORES
79	Administración del servidor web del portal	Disponibilidad, rendimiento, configuraciones	SERVIDORES
80	Administración de los servicios web de la empresa	Sitios web como citotusa, botón de pagos, etc.	SERVIDORES
81	Instalación de software base de PC	Instalar el software básico que requiere el usuario para el funcionamiento básico del equipo PC	HELPDESK
82	Instalación de software en los equipos de computación	Instalar el software requerido y con los respectivos permisos en los equipos de computación.	HELPDESK
83	Atención de Requerimientos de usuarios	Atender a un usuario telefónicamente y resolver su problema técnico de hardware o software.	HELPDESK
84	Instalación de Equipos en Eventos y Capacitaciones	Preparación, instalación, pruebas de funcionamiento para eventos especiales y salas de capacitación	HELPDESK
85	Instalación de equipos en Sucursales y Puntos de Servicio	Preparación, instalación, envío, pruebas de funcionamiento.	HELPDESK
86	Reseteo de Claves Internas y Externas	Reseteo de Claves del personal interno y Bancos Asociados.	HELPDESK
87	Mantenimiento de equipos A Nivel Nacional	Mantenimiento y actualizaciones en los Equipos a nivel nacional (hardware y software)	HELPDESK
88	Soporte a Kioscos	Instalación de aplicativos, mantenimiento, soporte internet	HELPDESK
89	Soporte remoto	Soporte al usuario remotamente para resolver problemas técnicos.	HELPDESK
			CONTINUA →

90	Movimiento de equipos	Soporte técnico ante traslados de equipos de computación.	HELPDESK
91	Instalación de aplicativos en forma masiva	Instalación de aplicaciones en todas las máquinas de la Organización.	HELPDESK
92	Instalación y monitoreo de Antivirus	Instalación del agente en todos los equipos, instalación de las actualizaciones, monitoreo diario de amenazas en todos los equipos de la organización.	HELPDESK
93	Manejo de bodega de equipos tecnológicos	Ingresos, movimientos y bajas de equipos de computación.	HELPDESK
94	Soporte y Activación de servicios empresariales en dispositivos móviles.	Activación de correo y políticas de seguridad en los equipos celulares BlackBerry.	HELPDESK
95	Soporte en Garantías de Equipos de computación.	Diagnóstico, informes técnicos, solicitud de garantías, cambios de partes.	HELPDESK
96	Reposición de partes y piezas de los equipos de computación.	Cambios de Partes externa o internas de los equipos de Computación.	HELPDESK
97	Soporte a entidades externas	Soporte en aplicativos que utilizan los bancos asociados	HELPDESK
98	Elaboración de Reportes	Elaboración de reportes del área.	HELPDESK
99	Mantenimiento del inventario tecnológico.	Ingreso, bajas, actualizaciones del inventario de equipos de computación. Reportaría, evaluaciones técnicas para cambios o compras masivas.	HELPDESK
100	Soportes a usuarios VIP	Soporte especial a usuarios especiales (Presidencia, Familiares y 4to piso)	HELPDESK
			CONTINUA →

101	Soporte Video Conferencia.	Pruebas, soporte para el funcionamiento de Video conferencia Quito - Guayaquil.	HELPDESK
102	Soporte Datacard	Atención de requerimientos, bitácora de funcionamiento, soporte conjunto con la empresa VideorTec ante daños, respaldos del disco duro.	HELPDESK
103	Centro de atención al usuario.	Recepción de llamadas, registro de incidencias, diagnostico de las incidencias, escalamiento, seguimientos, cierres de incidencias.	HELPDESK
104	Preparación de Equipos.	Preparación de equipos nuevos o usados con el software base.	HELPDESK
105	Atención de requerimientos de compra para equipos nuevos.	Informes técnicos, recepción y monitoreo del proceso de compra de equipos tecnológicos nuevos	HELPDESK
106	Evaluaciones de hardware y software	Instalación, pruebas de funcionamiento de equipos y software nuevos	HELPDESK
107	Soporte del sistema de turnos	Soporte del sistema de turnos	HELPDESK
108	Soportes eventuales	Soportes en pruebas de nuevos aplicativos, contingencia, reinicio de aplicativos principales, VLANS.	HELPDESK
109	Sistema de Proveeduría	Mantenimiento, creación usuarios, departamentos y asignación de permisos.	HELPDESK



### CAPITULO IV

#### 4. Funciones que interactúan entre las áreas

De los datos vistos en la tabla 1 y 2, se pueden determinar las funciones que interactuar para obtener los procesos transversales y orientados al servicio de la nueva estructura de TI. De aquí en adelante como se puede ver en la figura 3, Infraestructura y Networking pasa a ser parte del área de Operación del Servicio.

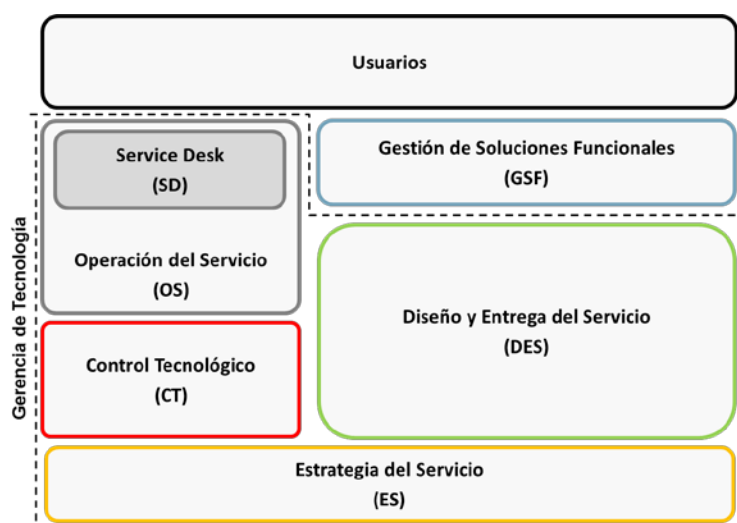


Figura 3. Nueva estructura de TI

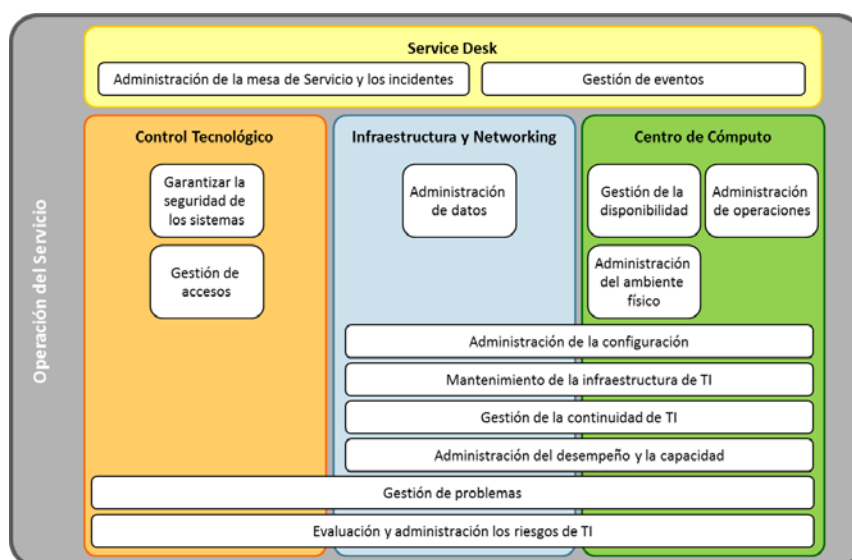


Figura 4. Mapa de procesos Operación del Servicio

## 4.1. Inventario de procesos objetivos

En la tabla 3 se presenta el inventario de los procesos objetivos del área Operación de Servicios.

**Tabla 3.**  
Inventario de procesos objetivos

Proceso objetivo	#	Subproceso objetivo
Administración de datos	1	Ciclo de vida de base de datos
	2	Soporte de base de datos
Administración de la configuración	3	Configuración de hardware
	4	Configuración de sistema operativo y software
	5	Mantenimiento de redes LAN
	6	Mantenimiento de redes WAN
Administración de la mesa de servicio y los incidentes	7	Soporte a usuarios en Service Desk
Administración de operaciones	8	Procesamiento de transacciones y disponibilidad de la información
	9	Servicio de back up
	10	Servicio de recovery
	11	Depuración de archivos
	12	Soporte a usuarios
Administración del desempeño y la capacidad	13	Administración del desempeño y la capacidad
Administración del ambiente físico	14	Administración del ambiente físico
Adquisición y mantenimiento de la infraestructura de TI	15	Mantenimiento de hardware
	16	Mantenimiento de software
Evaluación y administración los riesgos de TI	17	Evaluación y administración los riesgos de TI
Garantizar la seguridad de los sistemas	18	Administración de la seguridad de la información
	19	Monitoreo de seguridad
	20	Paso a producción
	21	Solicitud de respaldos
	22	Rotación de respaldos
	23	Custodia de respaldos
	24	Seguridad y control administrativo
CONTINUA →		

Gestión de accesos	25	Mantenimiento de usuarios
Gestión de eventos	26	Gestión de eventos
Gestión de la continuidad de TI	27	Contingencia Autorizador
	28	Contingencia Gestor
	29	Contingencia Peoplesoft
Gestión de la disponibilidad	30	Monitoreo de aplicaciones
	31	Monitoreo de centrales telefónicas, equipos de comunicación y enlaces
	32	Monitoreo de transacciones
	33	Monitoreo de servidores y discos
Gestión de problemas	34	Gestión de problemas

#### 4.1.1. Definiciones Importantes

Dentro de las definiciones más utilizadas en las áreas tenemos las siguientes:

**Evento:** Alerta o notificación entregada por las herramientas de monitoreo indicando un mal funcionamiento de un componente, el deterioro de un servicio o una alerta preventiva.

**Incidente:** Falla inesperada en alguno de los componentes de la infraestructura o de los procesos de operación del usuario que requiere ser atendido por el Service Desk.

**Problema:** Incidente cuya causa raíz no ha sido encontrada y por lo tanto debe ser analizado por los expertos en la materia para determinar una solución definitiva.

**Plan de capacidad:** El plan de capacidad se usa para gestionar los recursos de infraestructura requeridos para proveer servicios de TI. El plan contiene la proyección de demanda de negocio para los distintos componentes de la infraestructura y las opciones valoradas para proveer los objetivos de nivel de servicio acordados.

**ANS:** Acuerdo entre un proveedor de servicio de TI y un cliente o usuario. El ANS describe el servicio de TI, documenta los Objetivos de nivel de servicio y

especifica las responsabilidades del proveedor de servicio de TI y del cliente o usuario.

**KPI (indicador clave de desempeño):** Métrica empleada para ayudar a gestionar un proceso, servicio de TI o actividad. Muchas métricas pueden medirse pero sólo las más importantes se definen como KPIs y son empleadas para gestionar de forma activa e informar sobre los procesos, los servicios de TI o las actividades. Los KPIs deben ser seleccionados de tal forma que aseguren el control de la eficiencia, la efectividad, y la rentabilidad.

**Riesgo inherente:** Una posible amenaza que podría causar daño o pérdidas, o afectar la habilidad de alcanzar objetivos planteados. Es el riesgo en su estado natural, sin control asociado.

**Riesgo Residual:** Una posible amenaza que podría causar daño o pérdidas, o afectar la habilidad de alcanzar los objetivos planteados, pero cuyo impacto o probabilidad ha sido mitigado a través de la ejecución de un conjunto de controles asociados a las fallas que puede materializar dicho riesgo.

## 4.2. Diagrama de Flujo de Modelo Operativo de TI

Los siguientes diagramas de flujo se rigen con los documentos habilitantes del Anexo A.

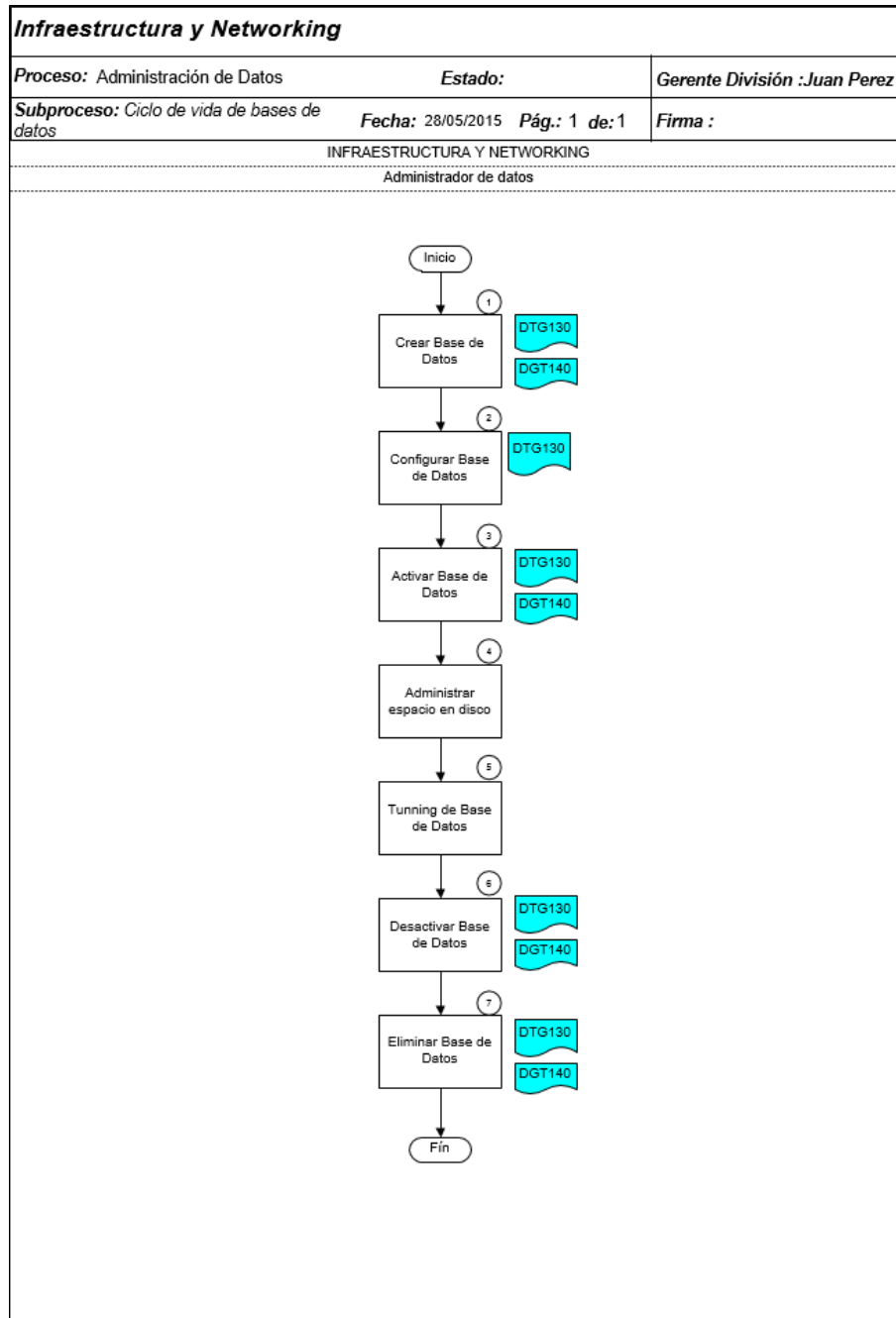


Figura 5. Proceso: Administración de Datos  
Subproceso: Ciclo de vida de Base de Datos

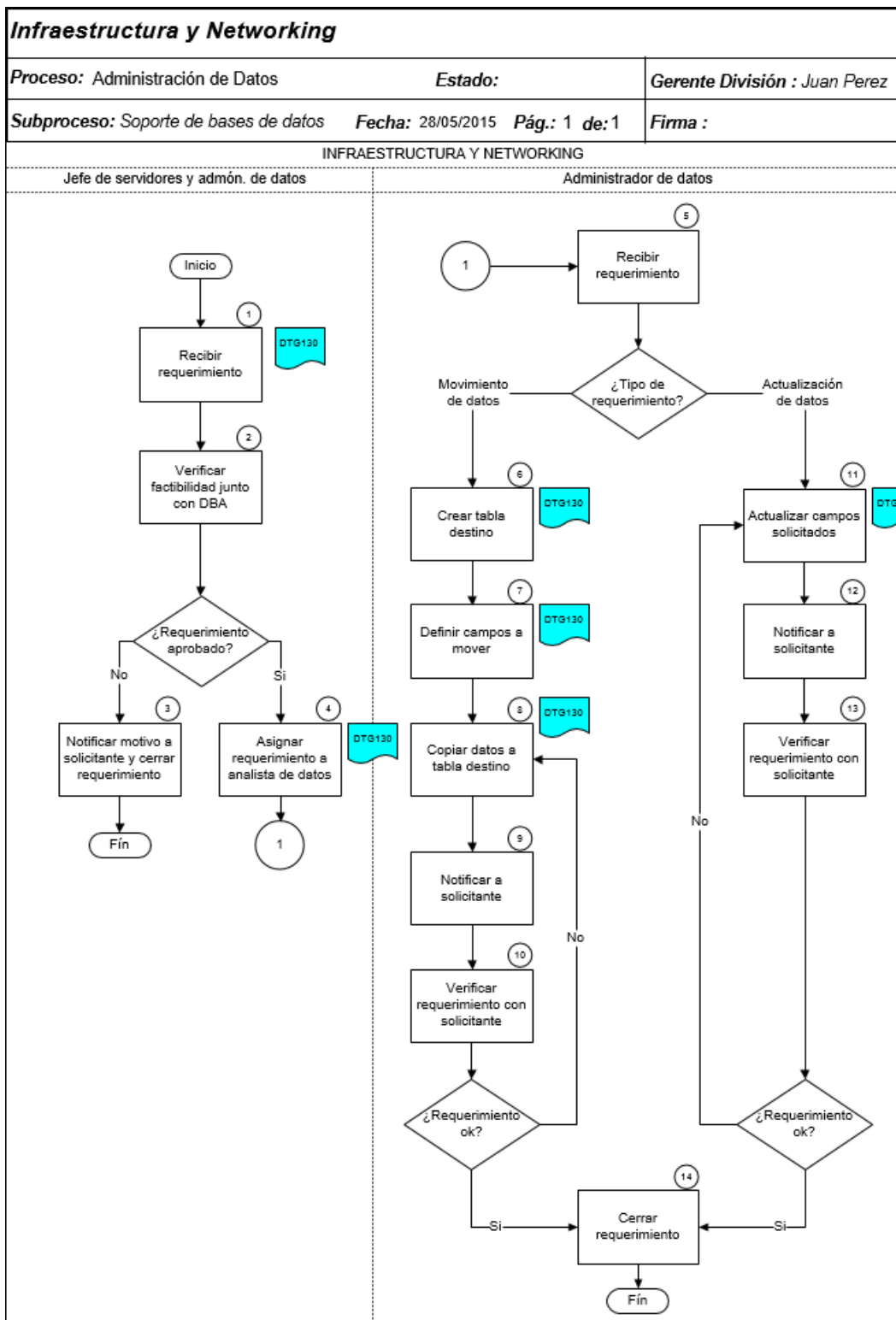


Figura 6. Proceso: Administración de Datos  
Subproceso: Soporte de Bases de Datos

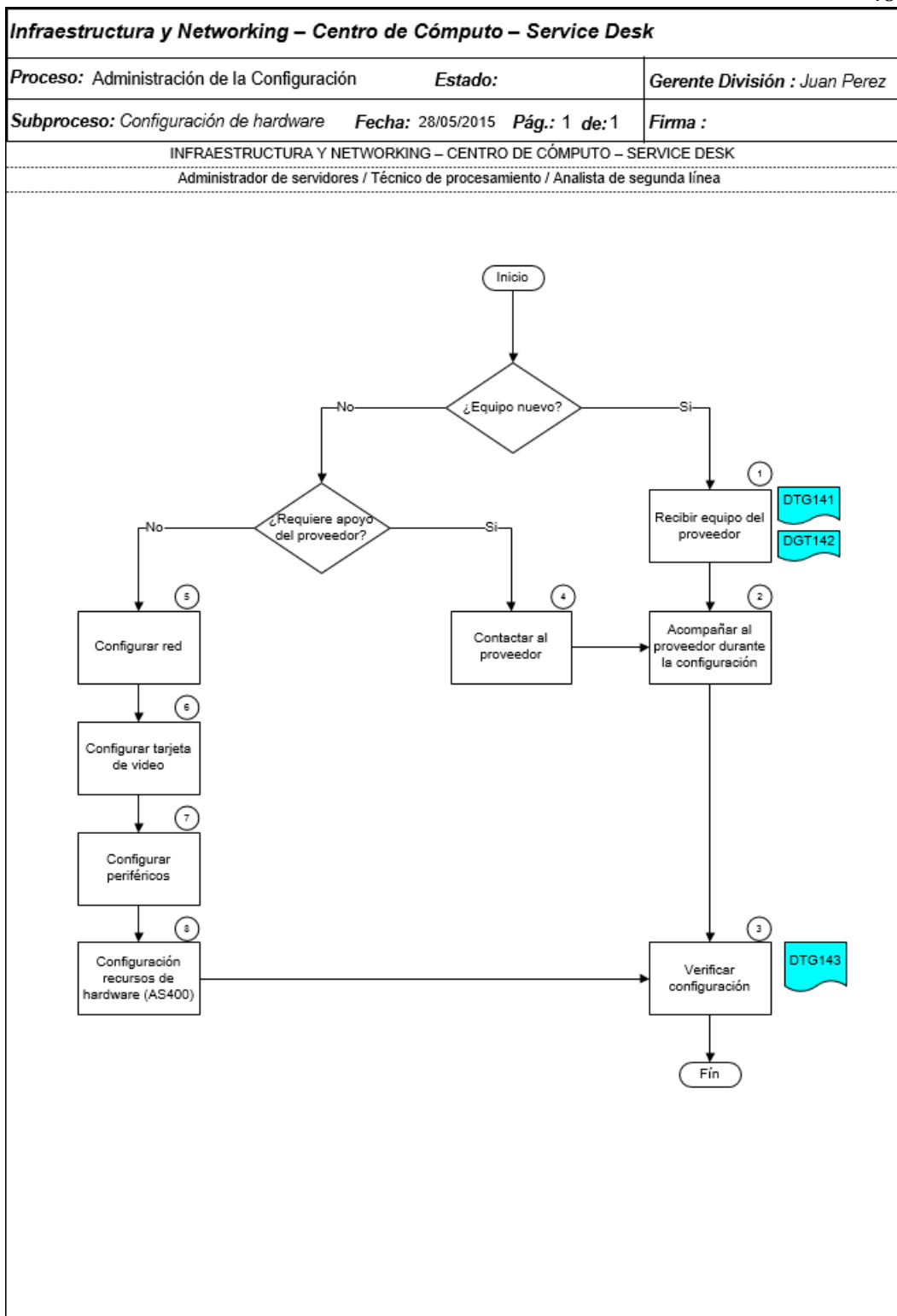


Figura 7. Proceso: Administración de la Configuración  
Subproceso: Configuración de Hardware

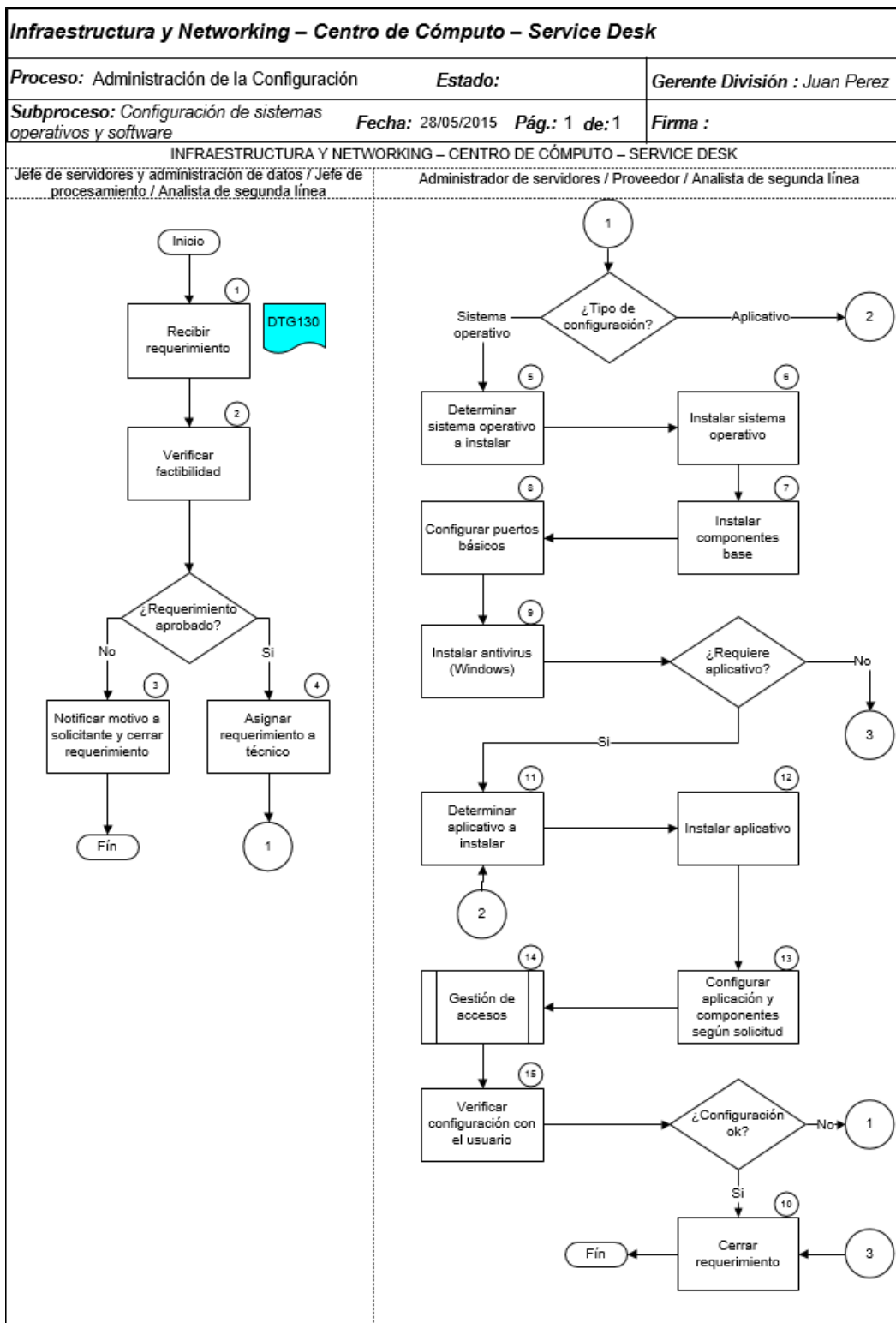


Figura 8. Proceso: Administración de la Configuración  
Subproceso: Configuración de Sistemas Operativos y Software



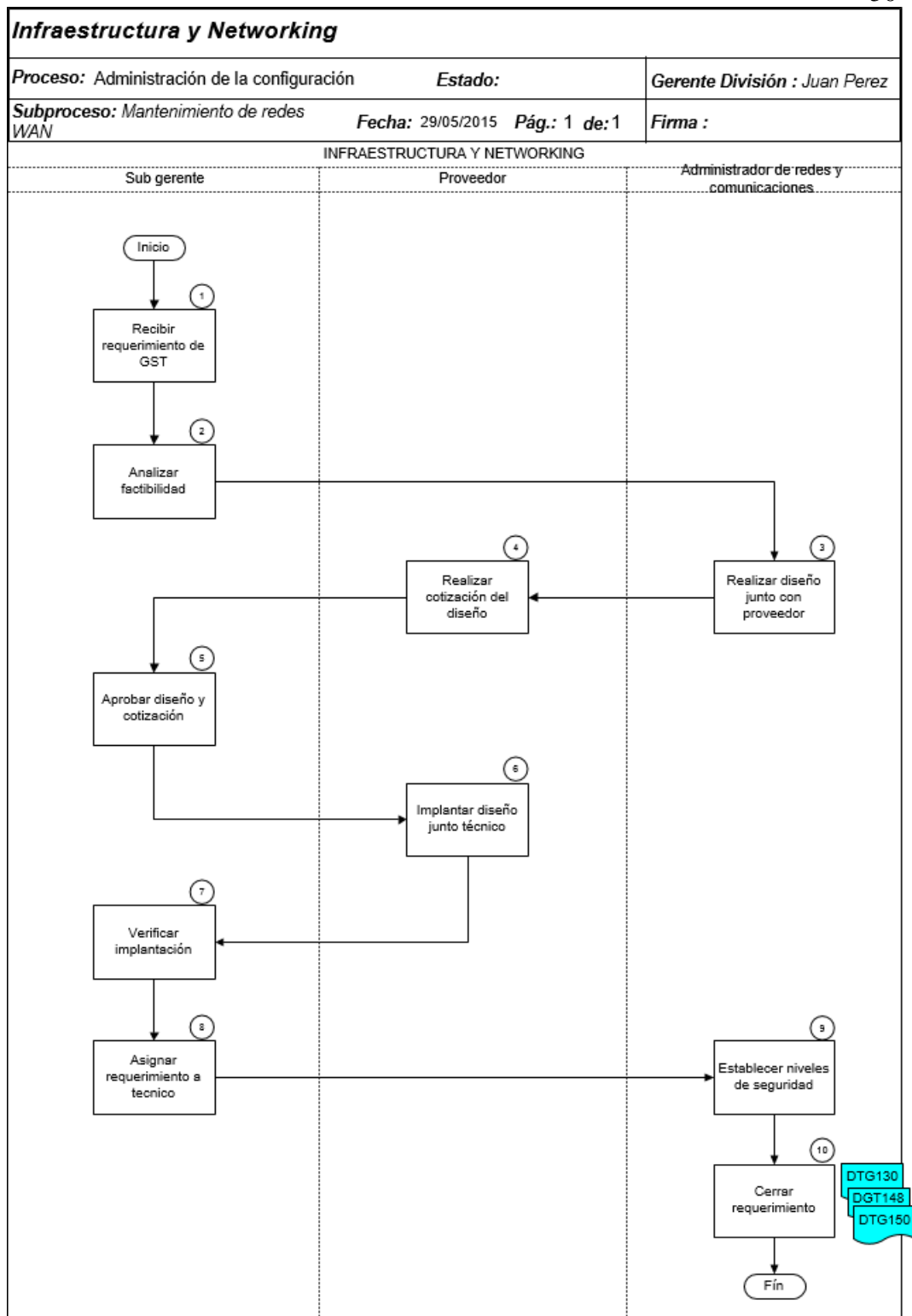


Figura 9. Proceso: Administración de la Configuración  
Subproceso: Mantenimiento de Redes WAN

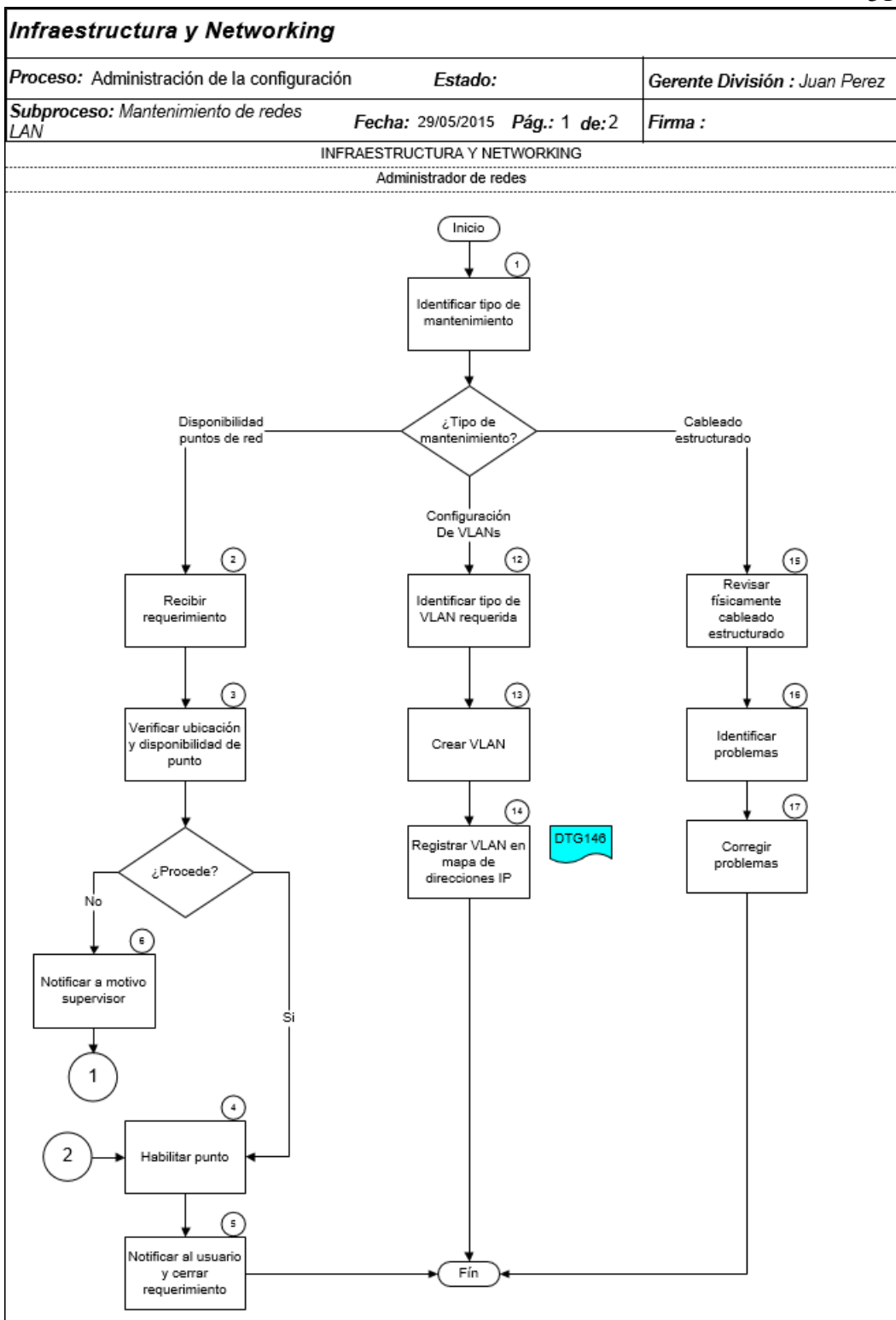


Figura 10. Proceso: Administración de la Configuración  
Subproceso: Mantenimiento de Redes LAN

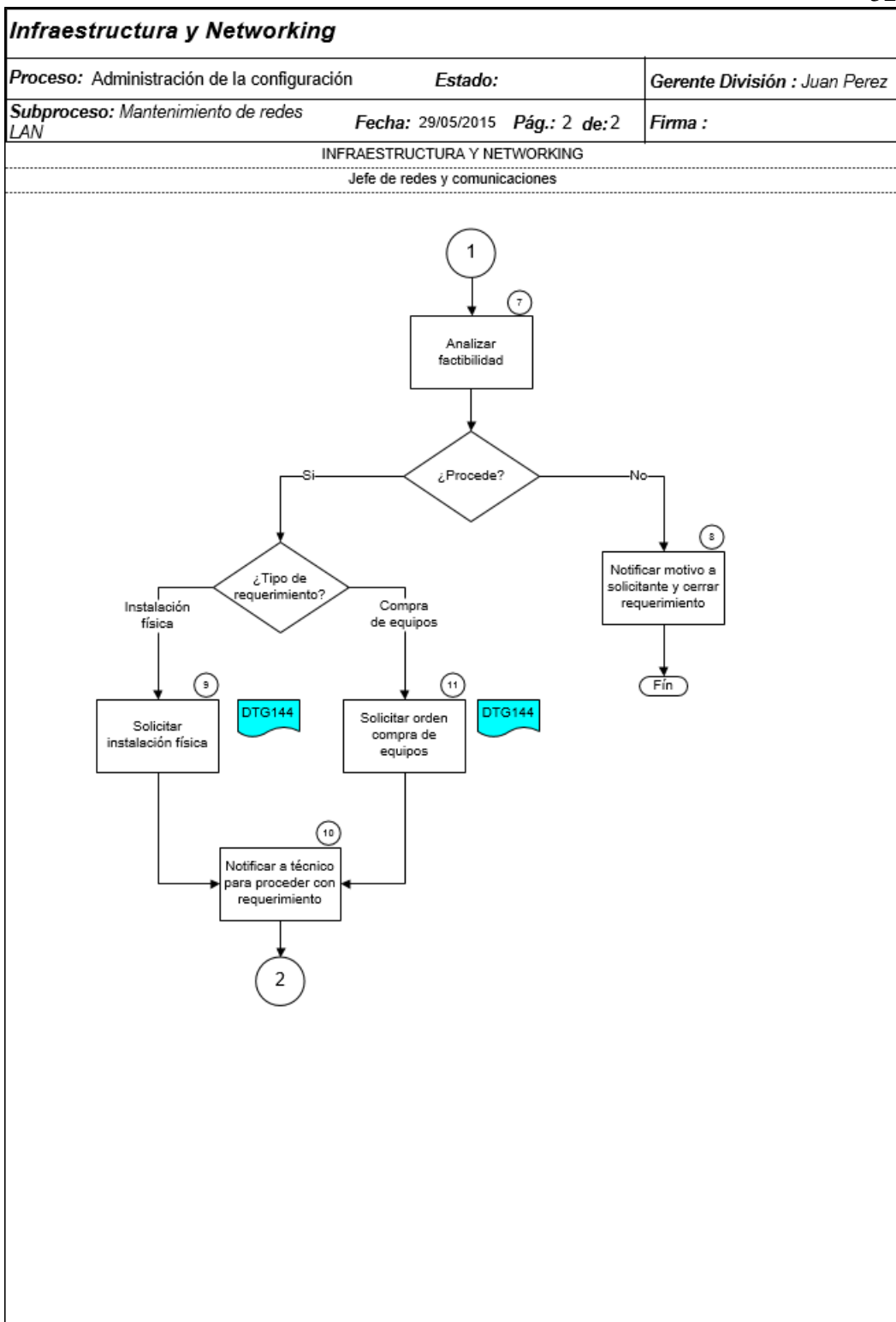


Figura 11. Proceso: Administración de la Configuración  
Subproceso: Mantenimiento de Redes LAN

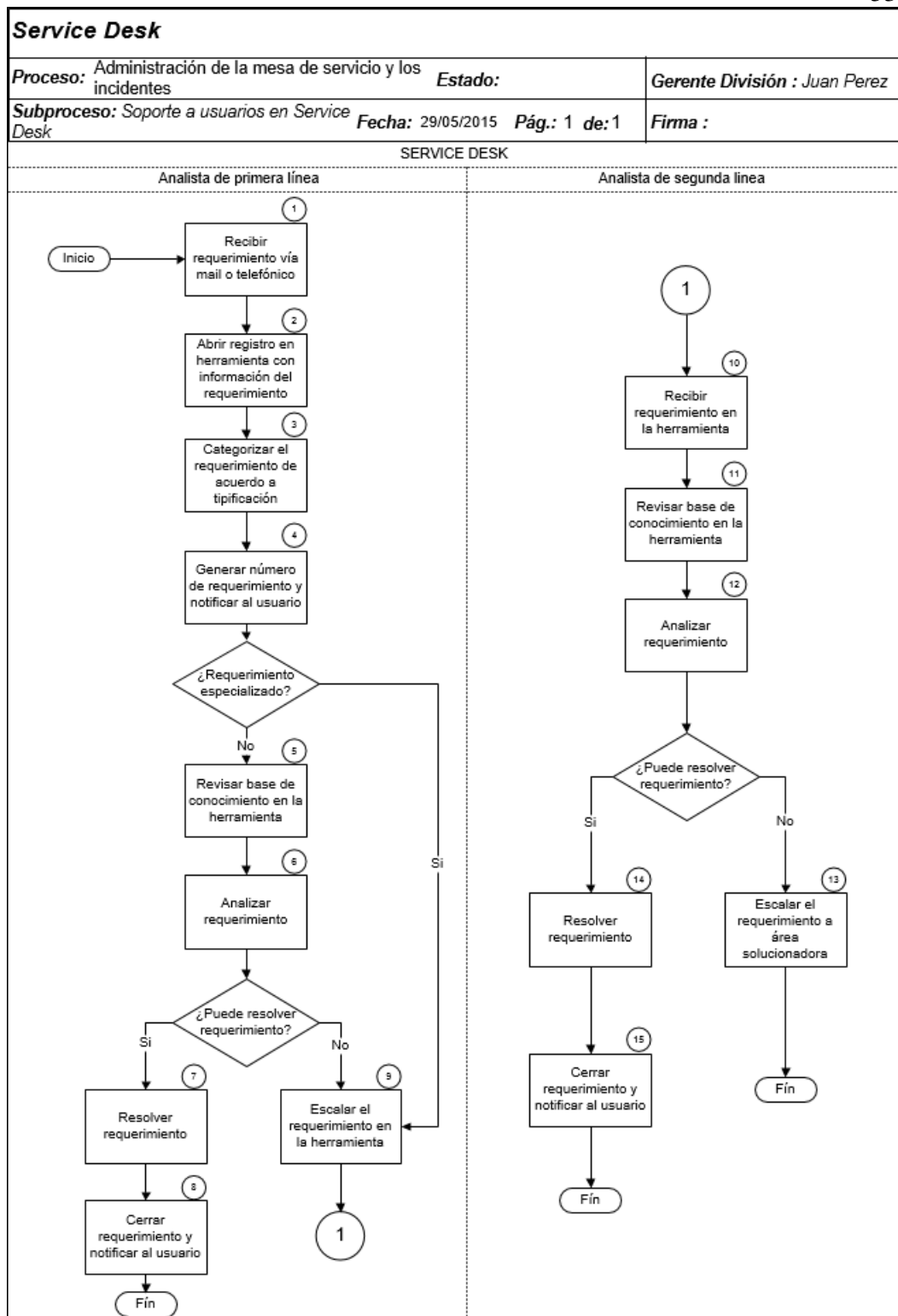


Figura 12. Proceso: Administración de la mesa de servicio y los incidentes  
Subproceso: Soporte a Usuarios en Service Desk

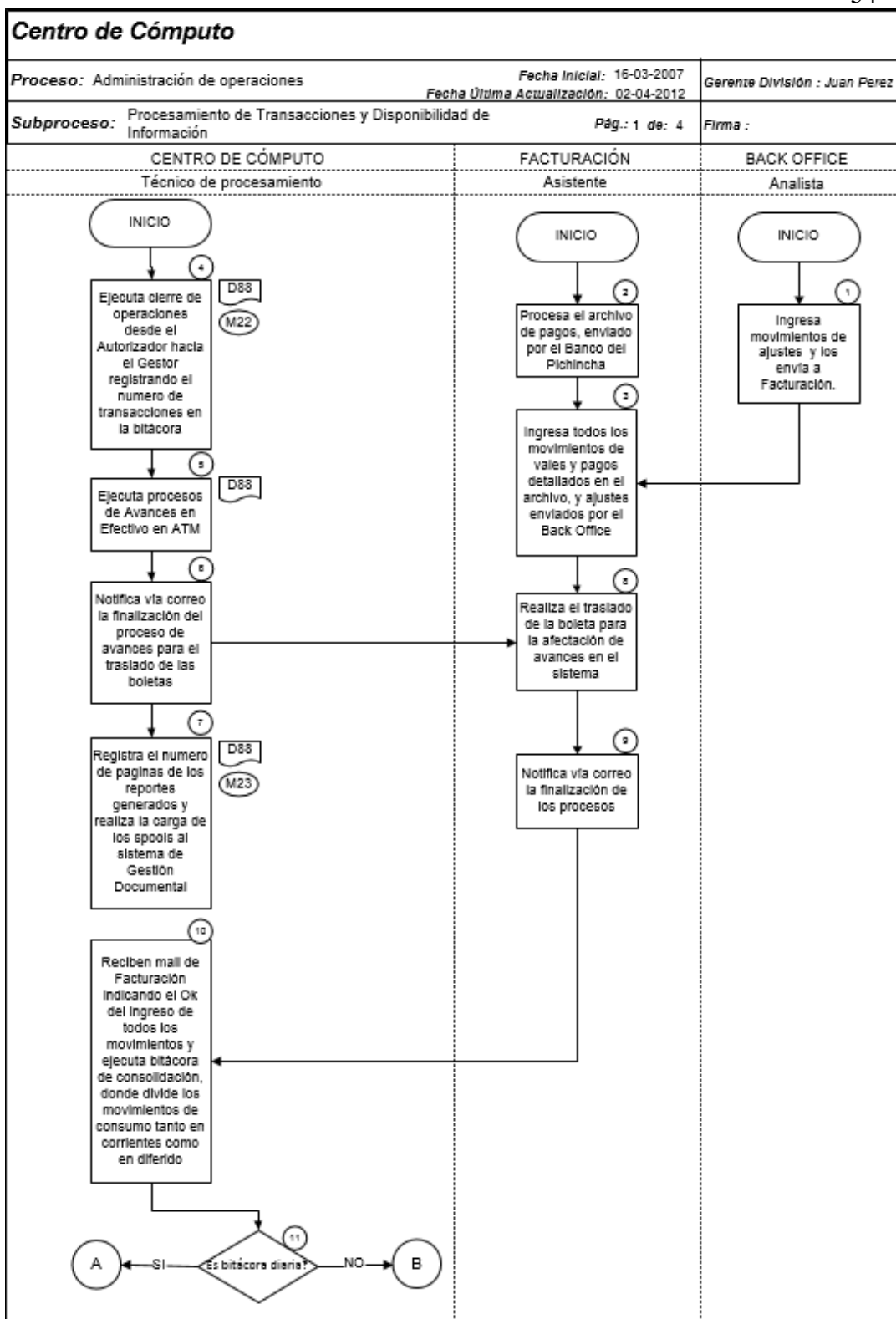


Figura 13. Proceso: Administración de operaciones  
Subproceso: Procesamiento de Transacciones y Disponibilidad de Información

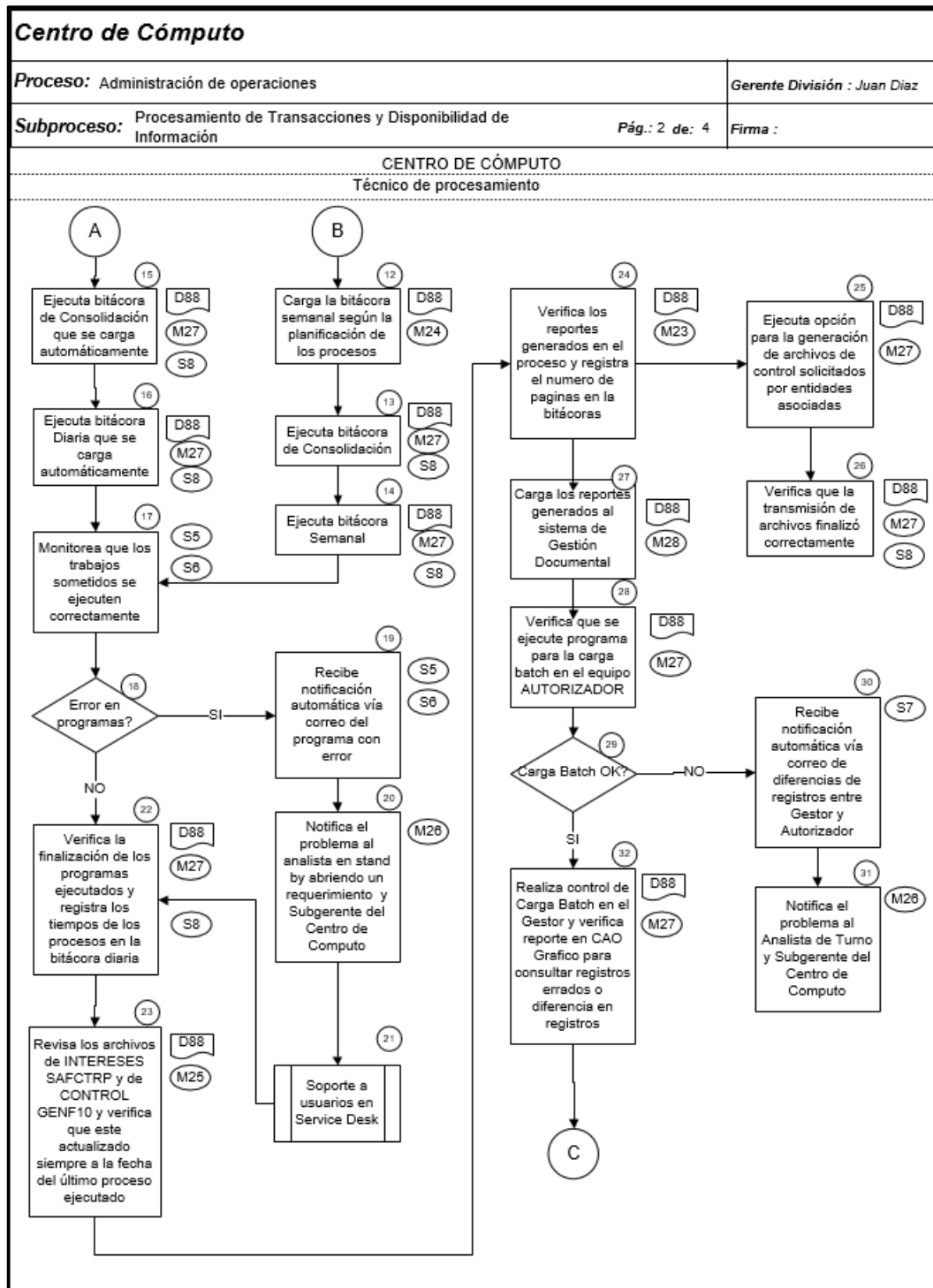


Figura 14. Proceso: Administración de operaciones  
 Subproceso: Procesamiento de Transacciones y Disponibilidad de Información

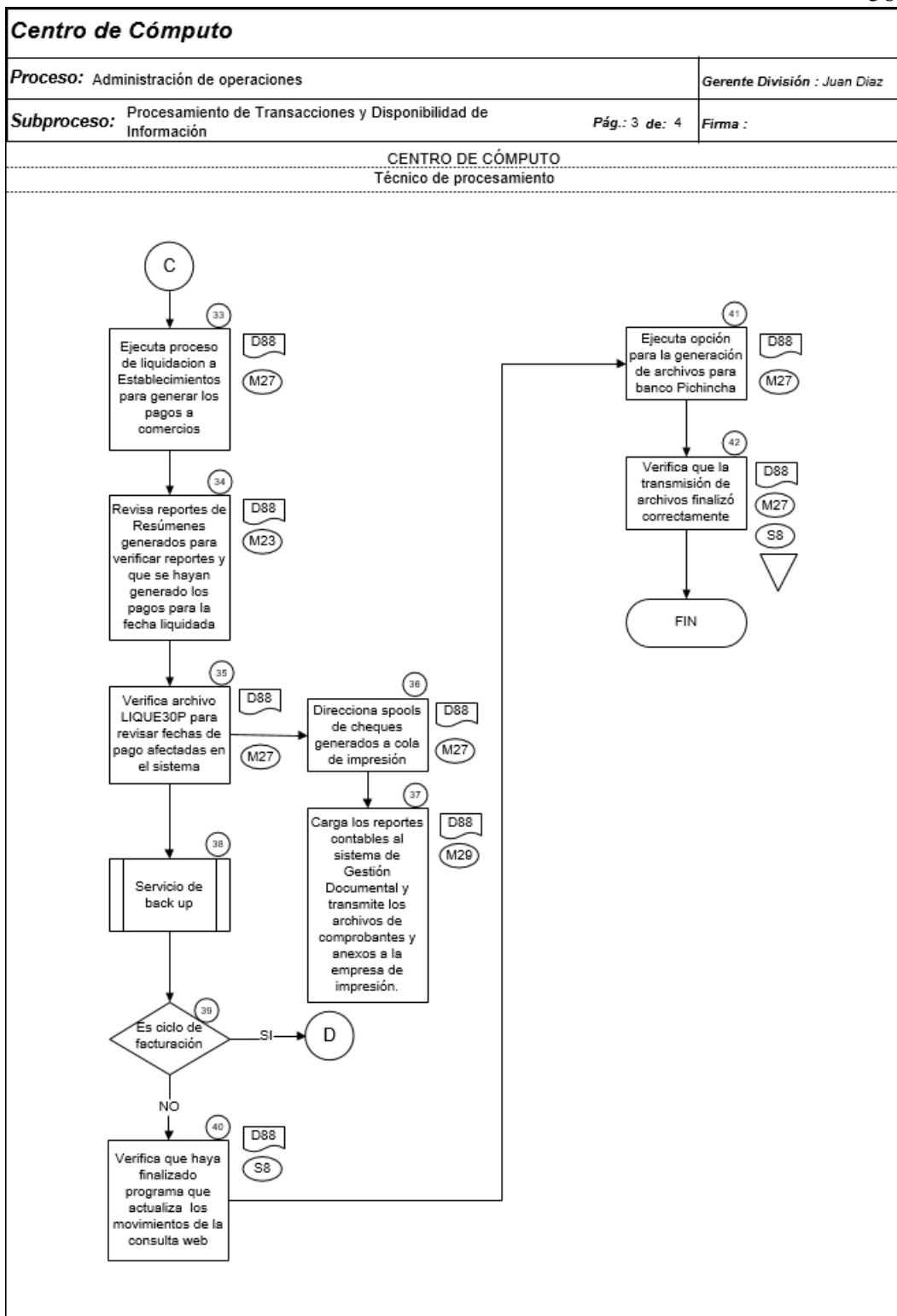


Figura 15. Proceso: Administración de operaciones  
Subproceso: Procesamiento de Transacciones y Disponibilidad de Información

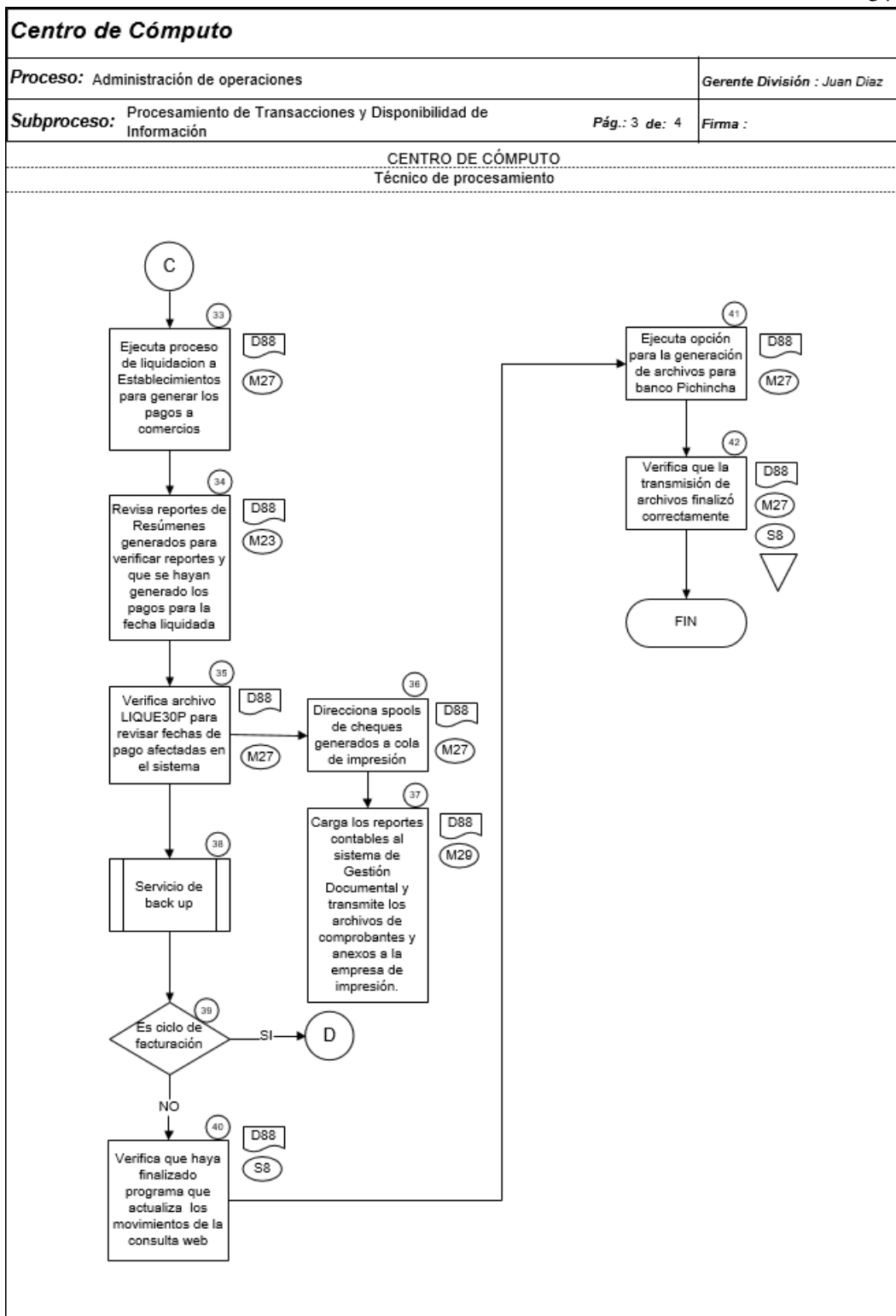


Figura 16. Proceso: Administración de operaciones  
Subproceso: Procesamiento de Transacciones y Disponibilidad de Información



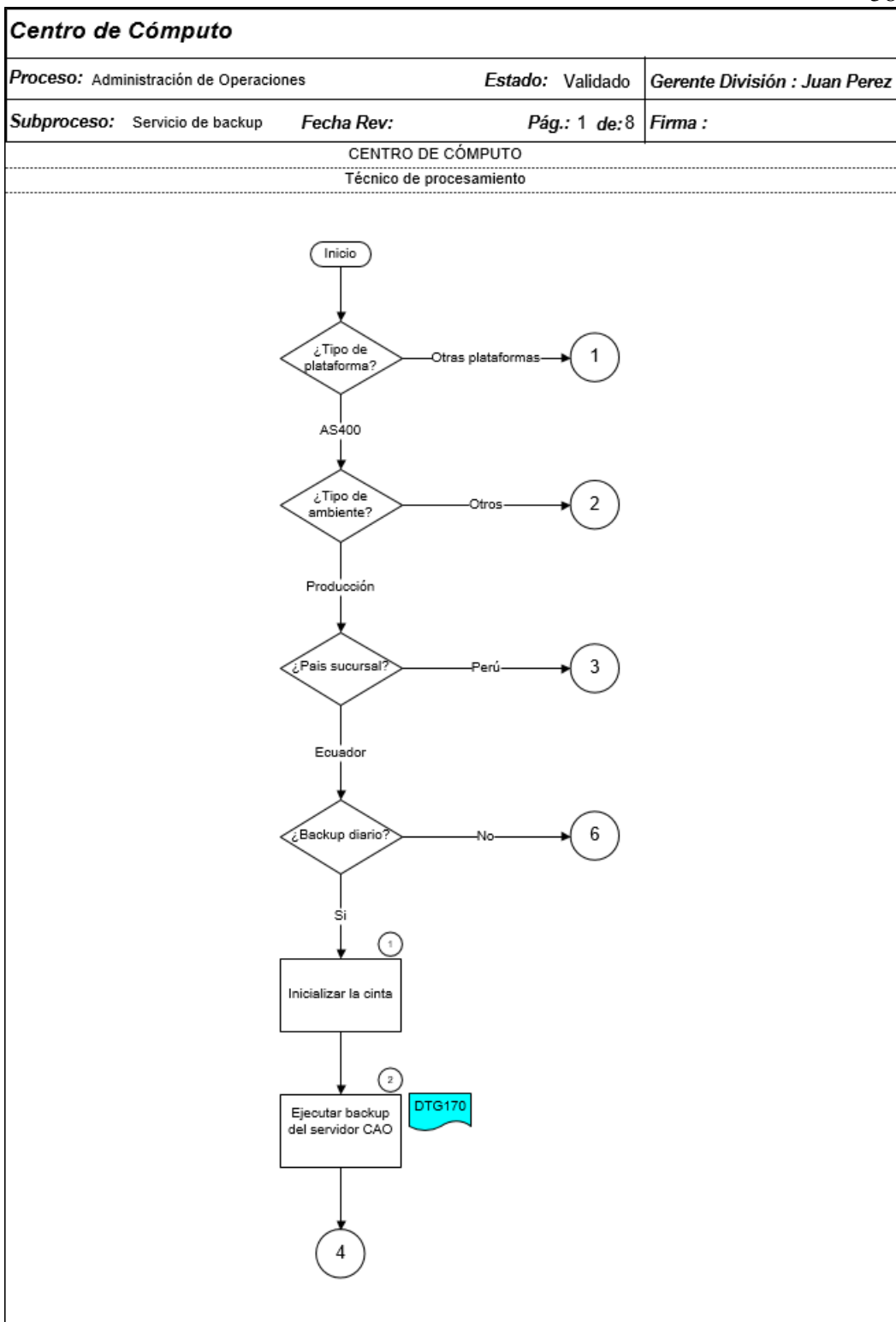


Figura 17. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

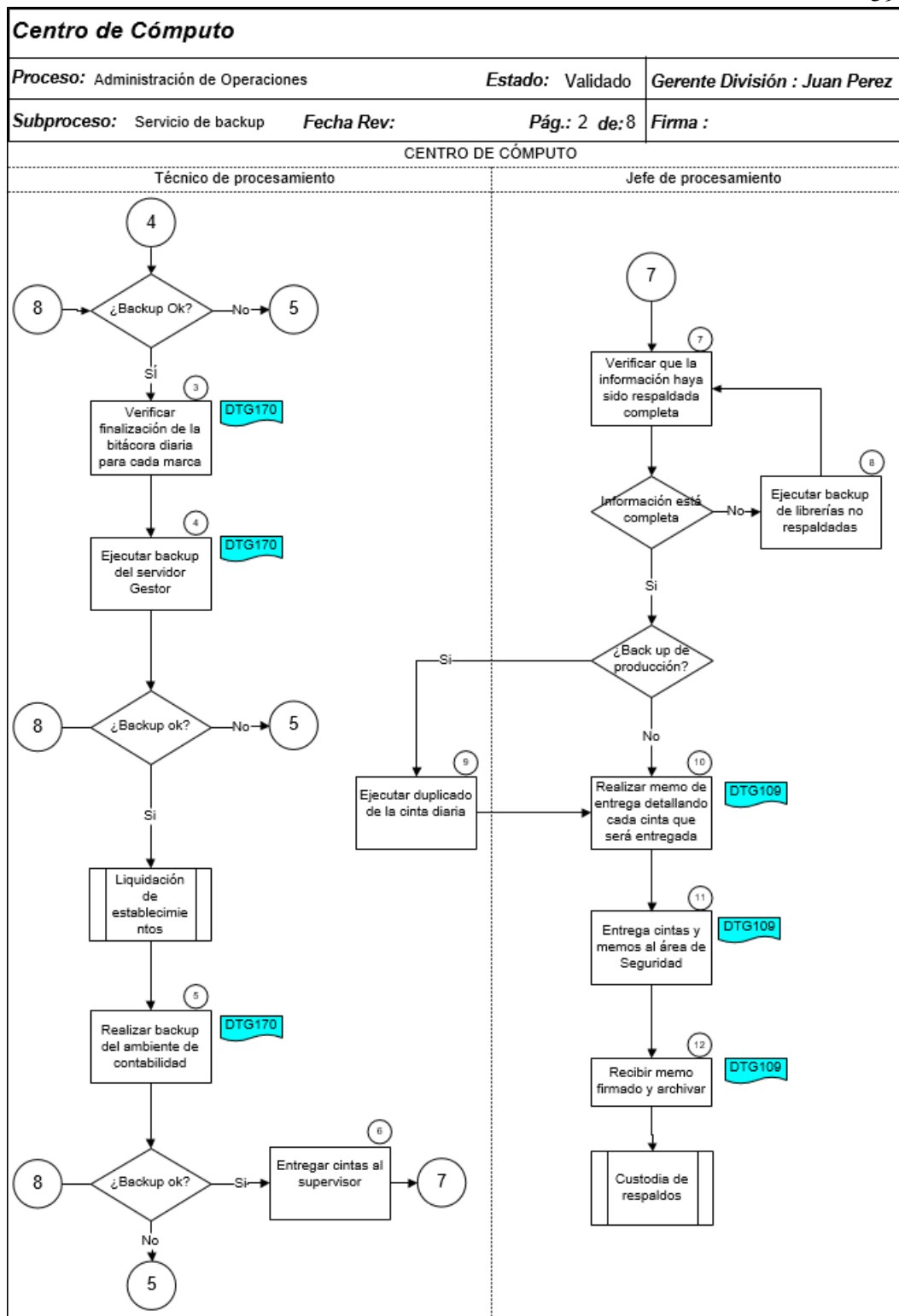


Figura 18. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

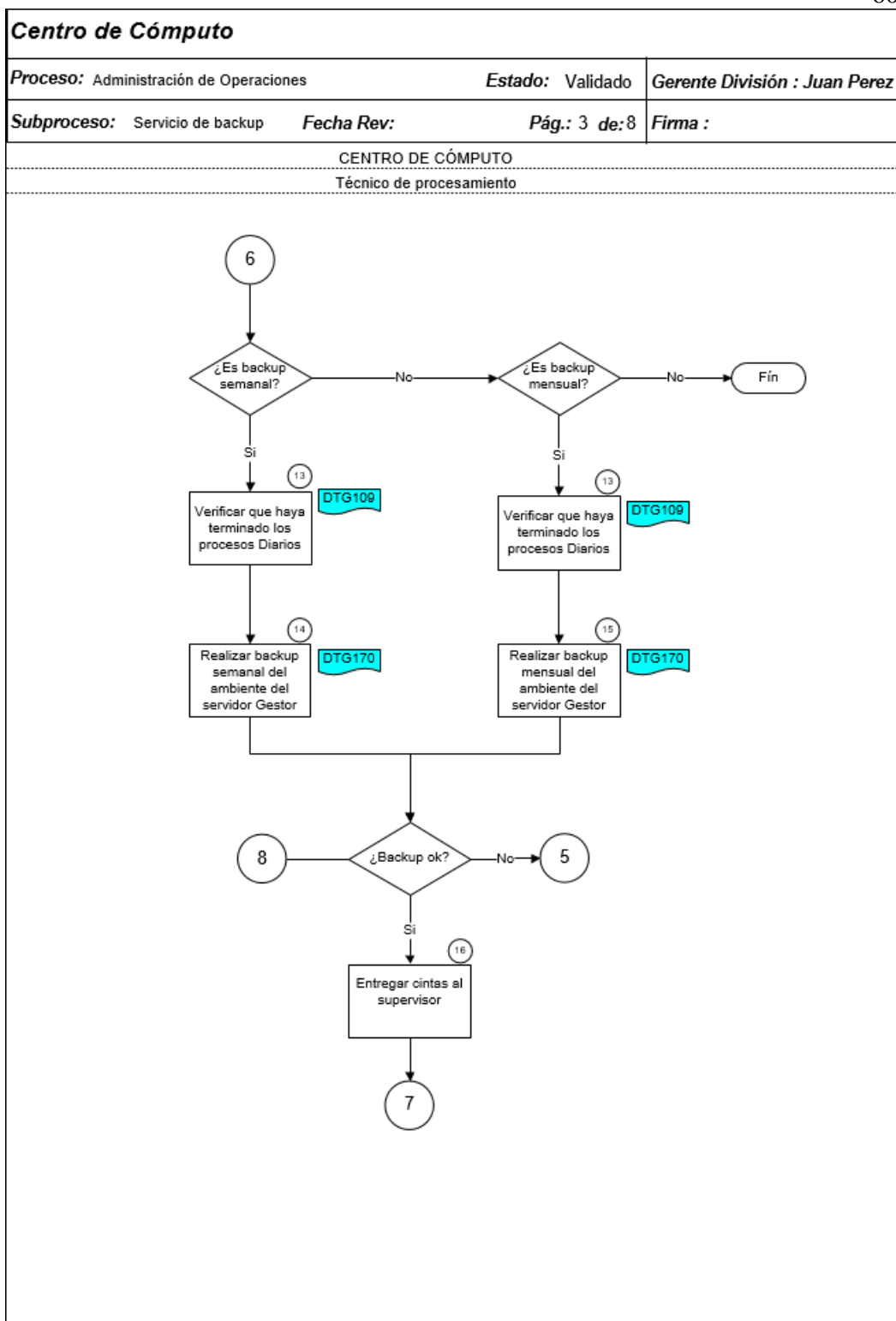


Figura 19. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

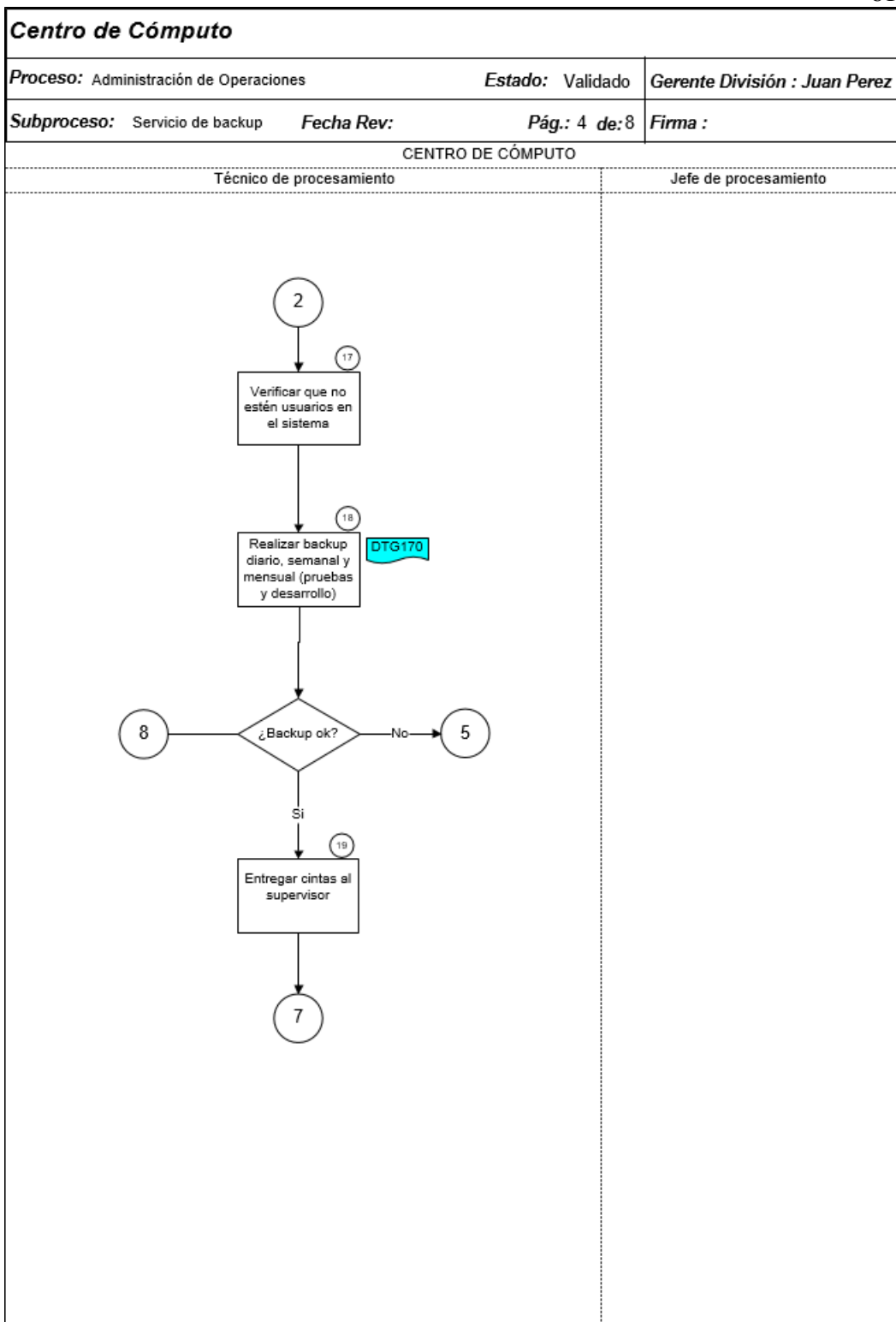


Figura 20. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

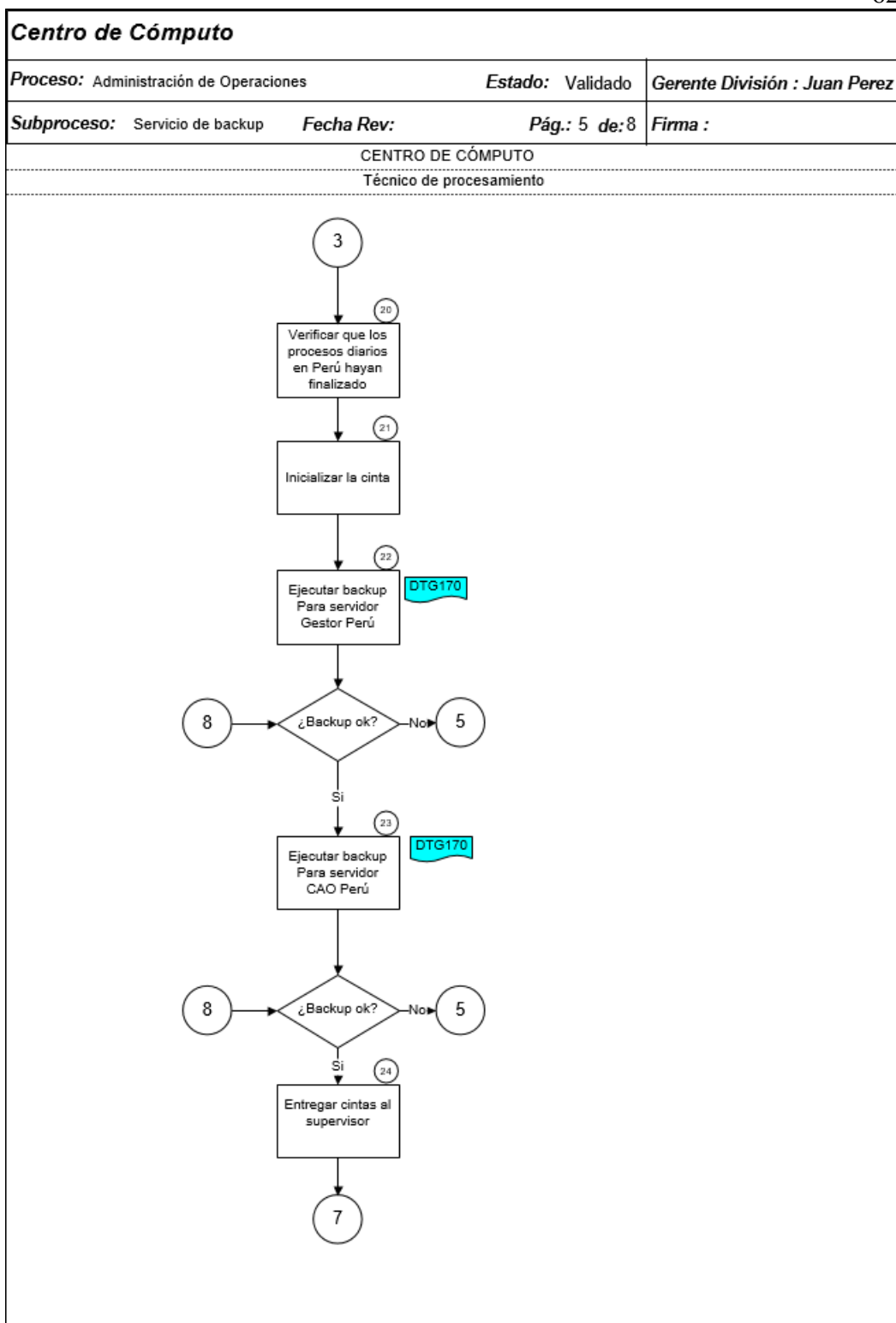


Figura 21. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

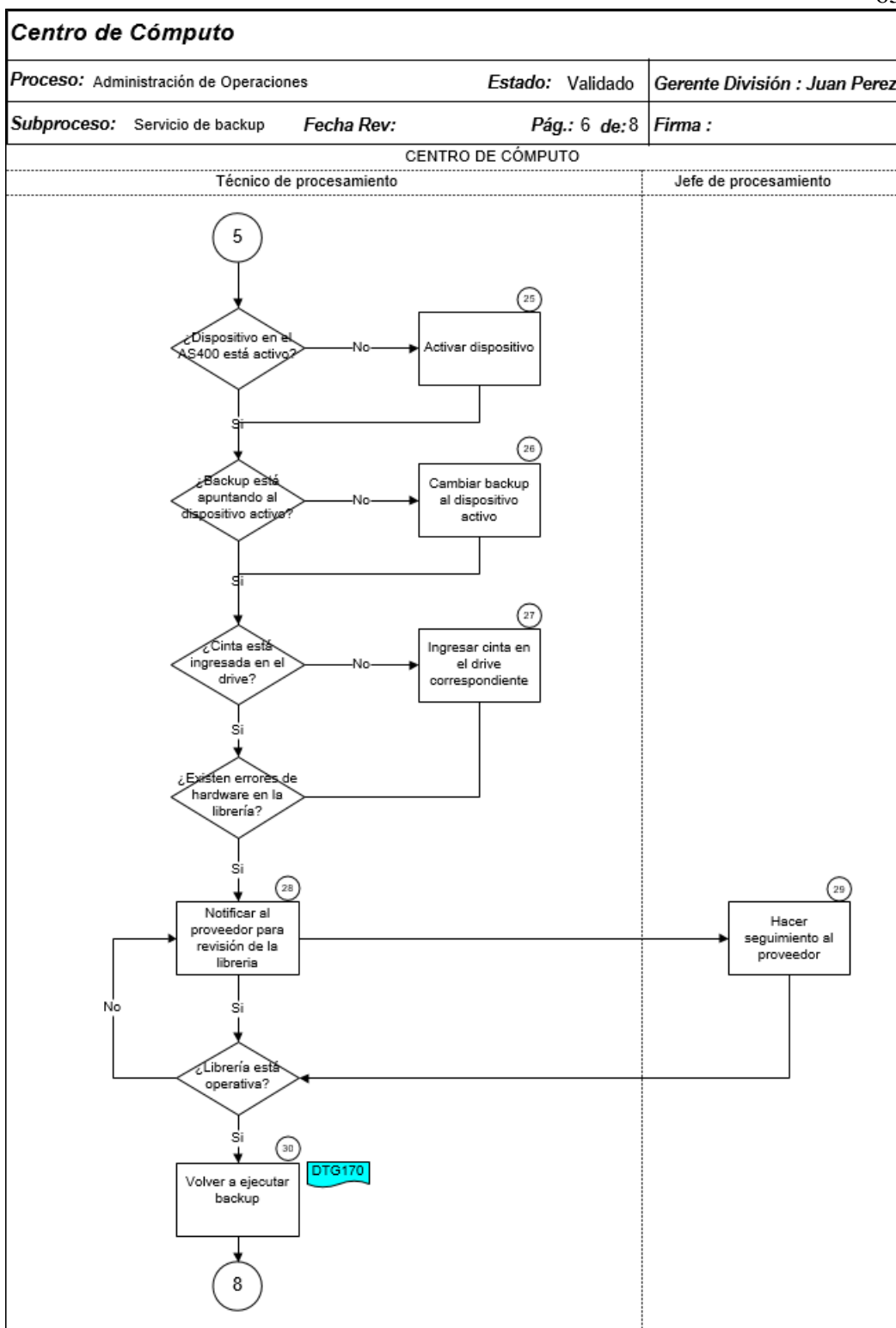


Figura 22. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

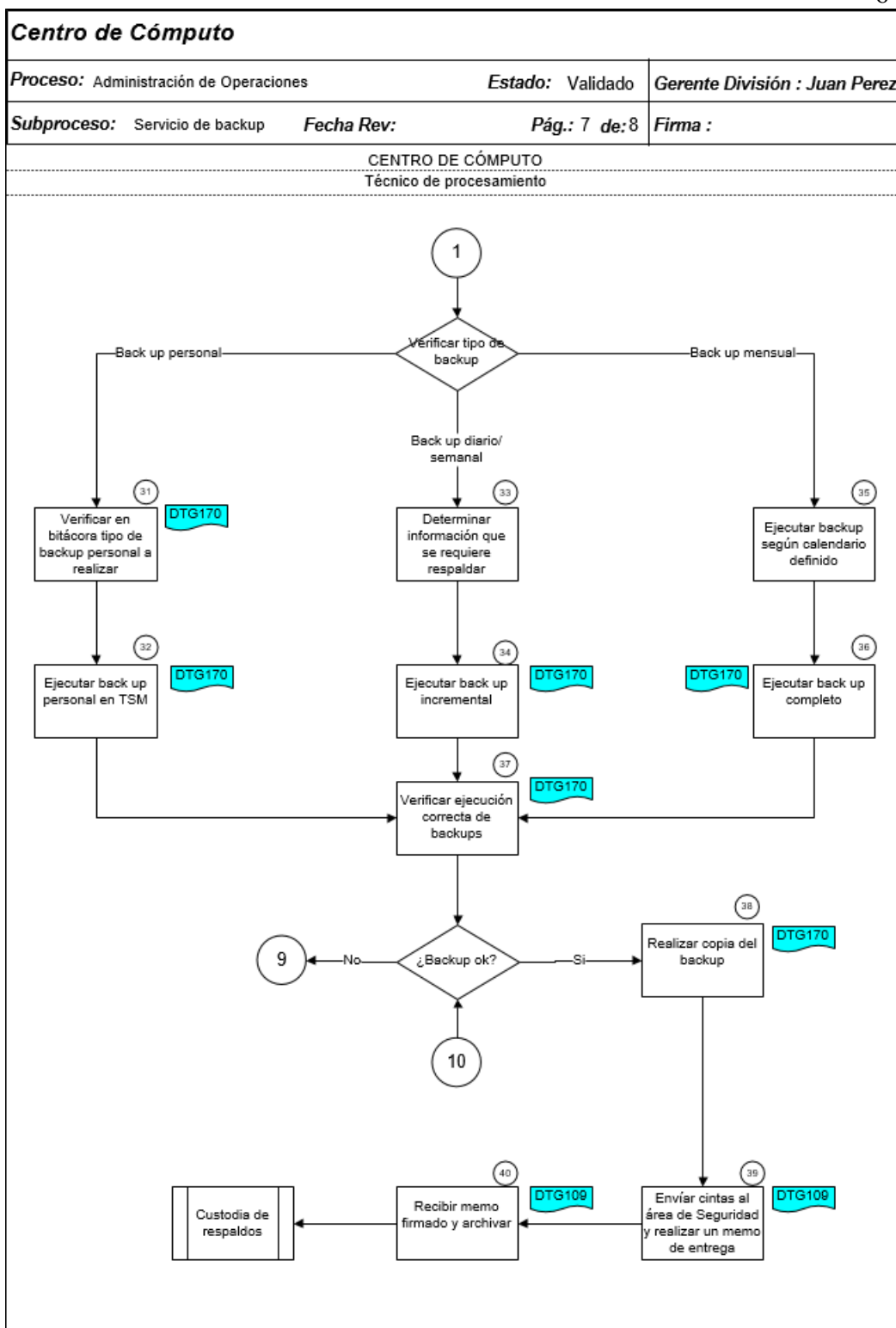


Figura 23. Proceso: Administración de operaciones  
Subproceso: Servicio de backup

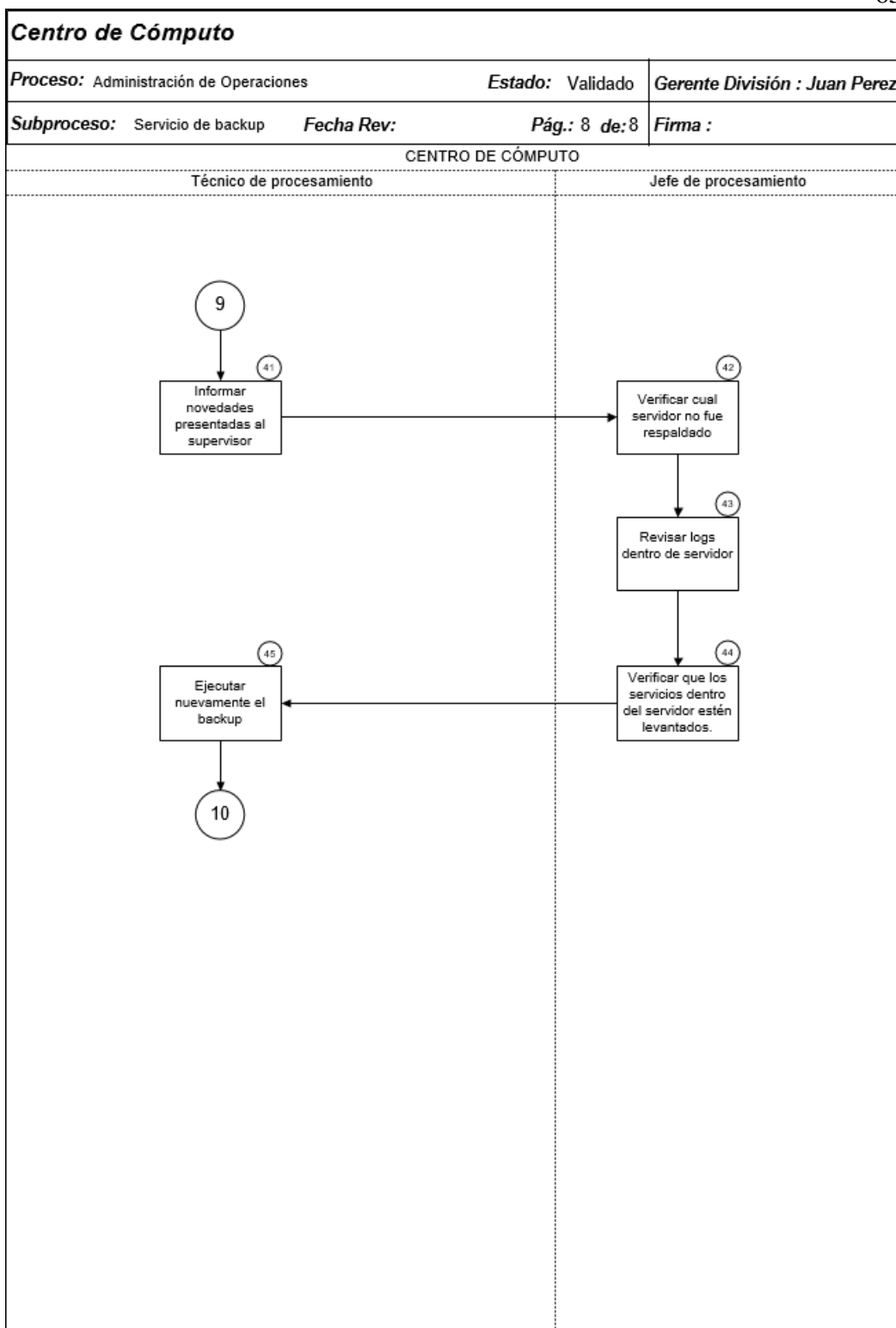


Figura 24. Proceso: Administración de operaciones  
Subproceso: Servicio de backup



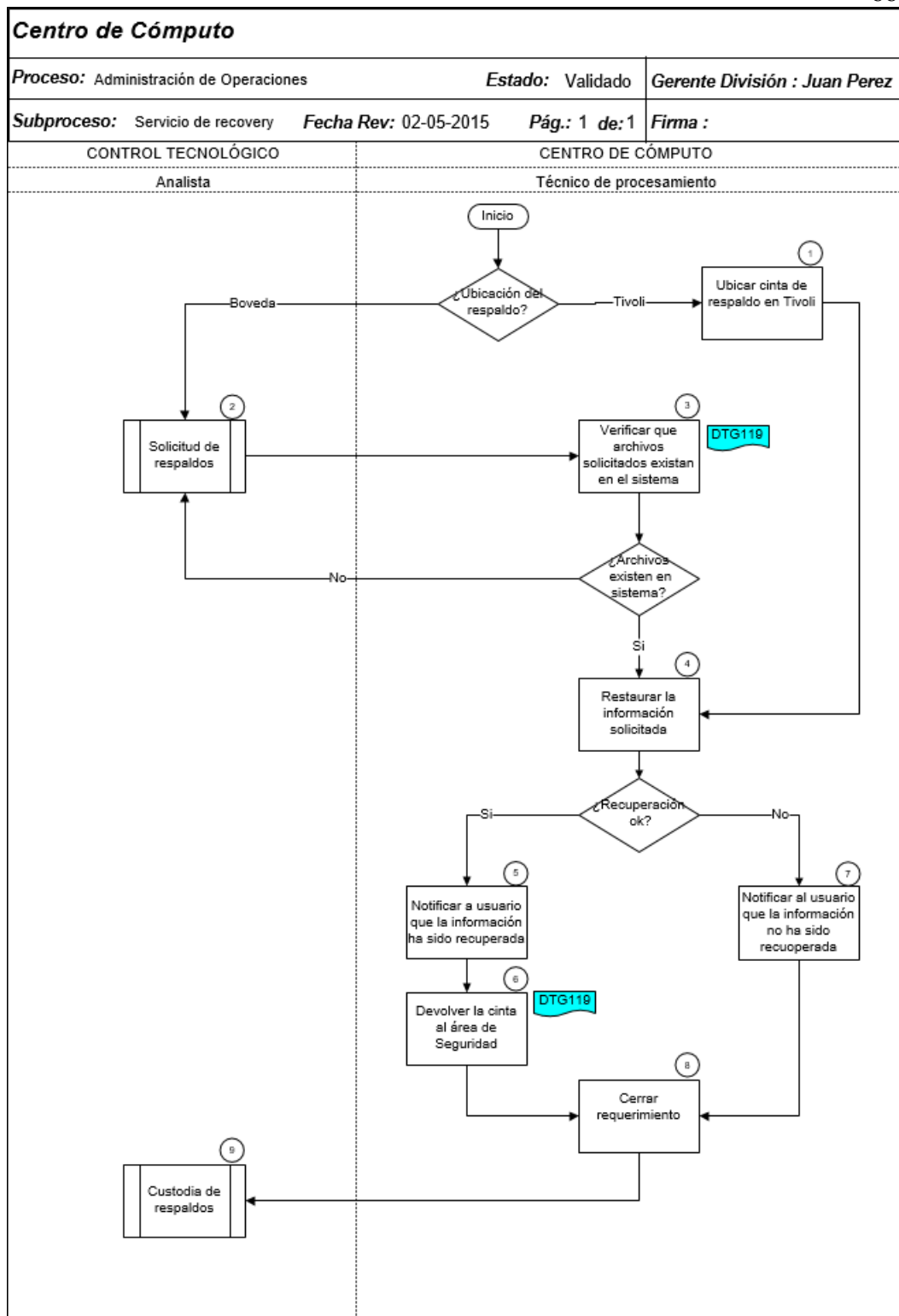


Figura 25. Proceso: Administración de operaciones  
Subproceso: Servicio de recovery

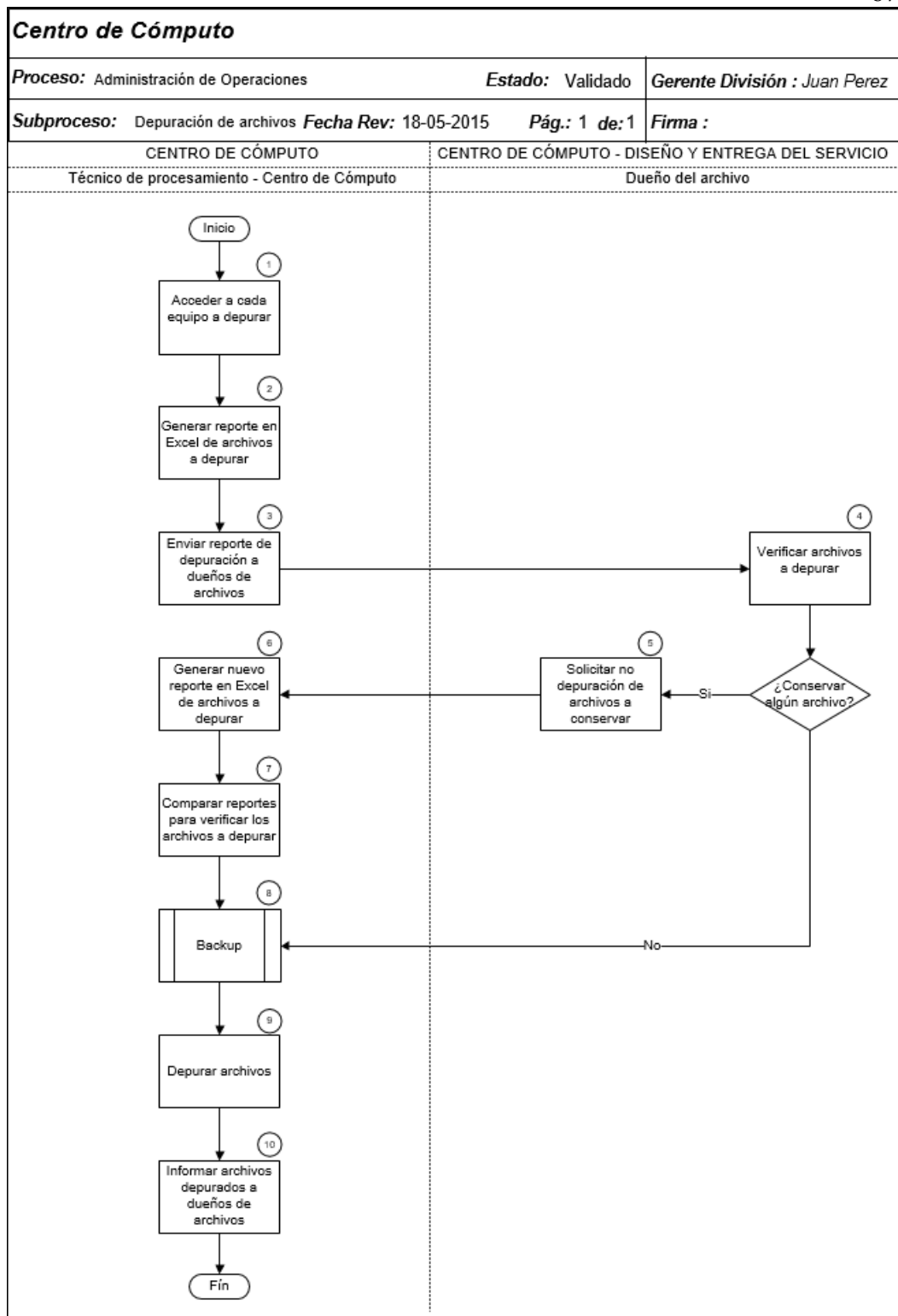


Figura 26. Proceso: Administración de operaciones  
Subproceso: Depuración de archivos

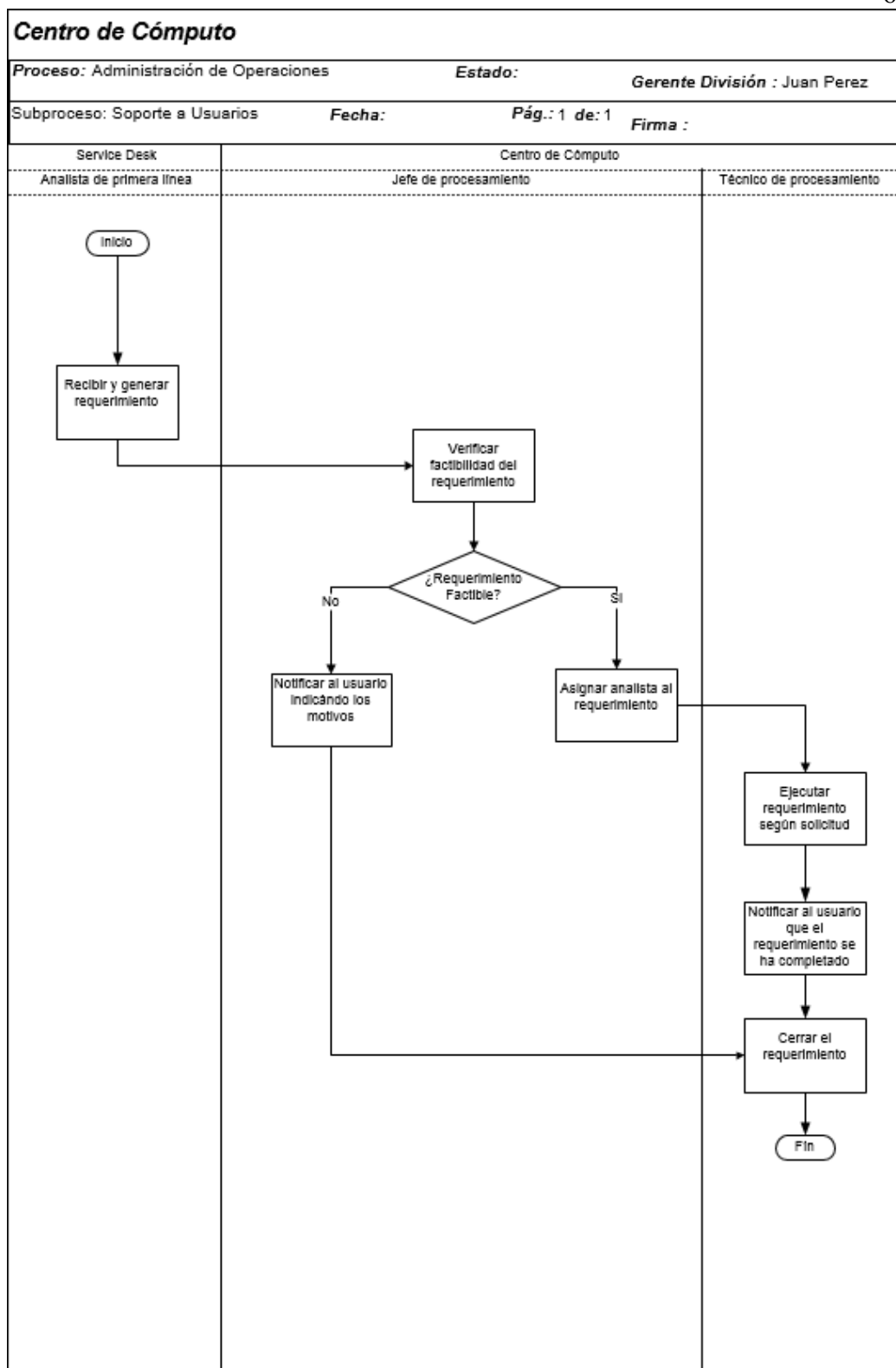


Figura 27. Proceso: Administración de operaciones  
Subproceso: Soporte a usuarios

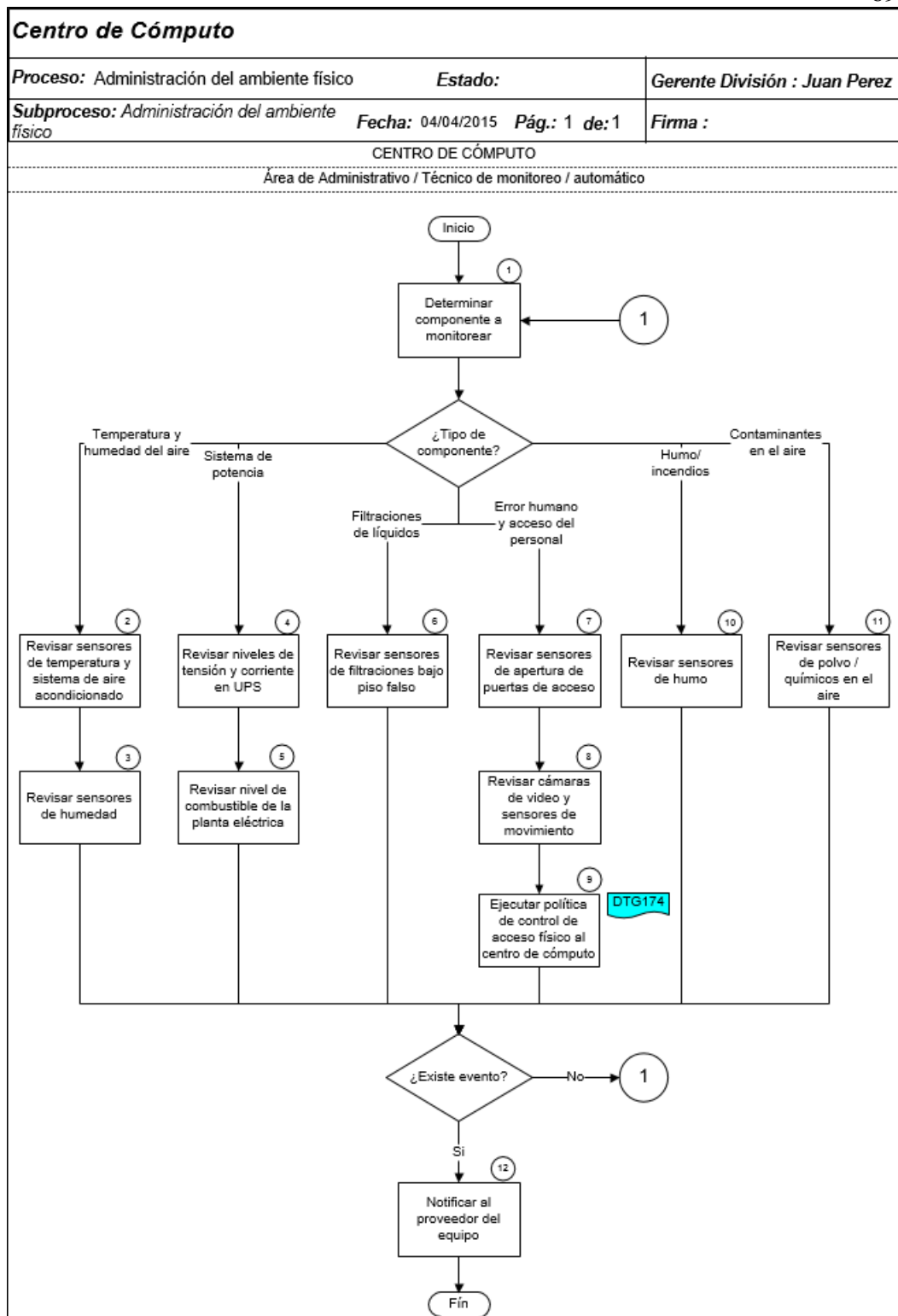


Figura 28. Proceso: Administración del ambiente físico  
Subproceso: Soporte a usuarios

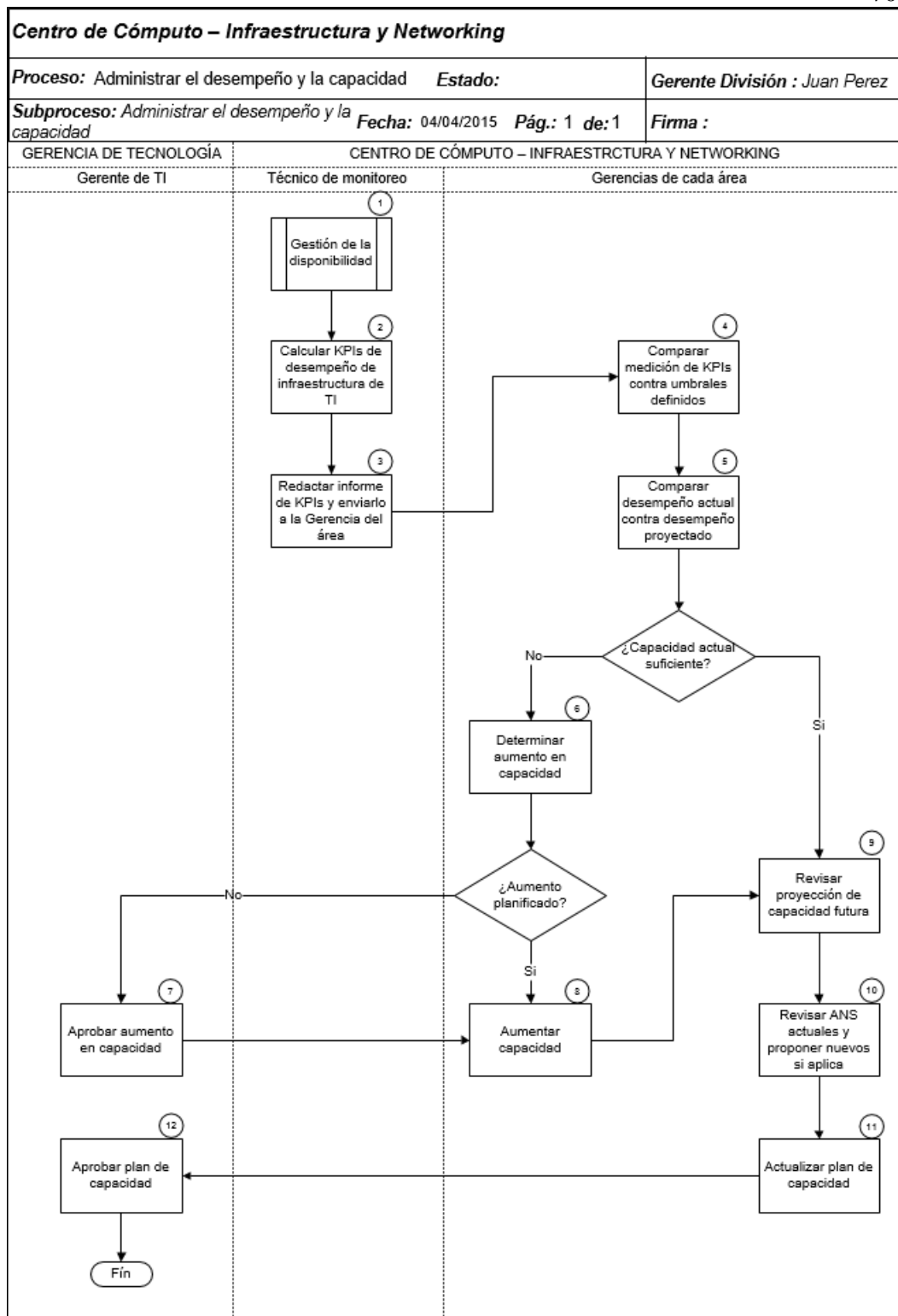


Figura 29. Proceso: Administrar el desempeño y la capacidad  
Subproceso: Administración del Ambiente Físico

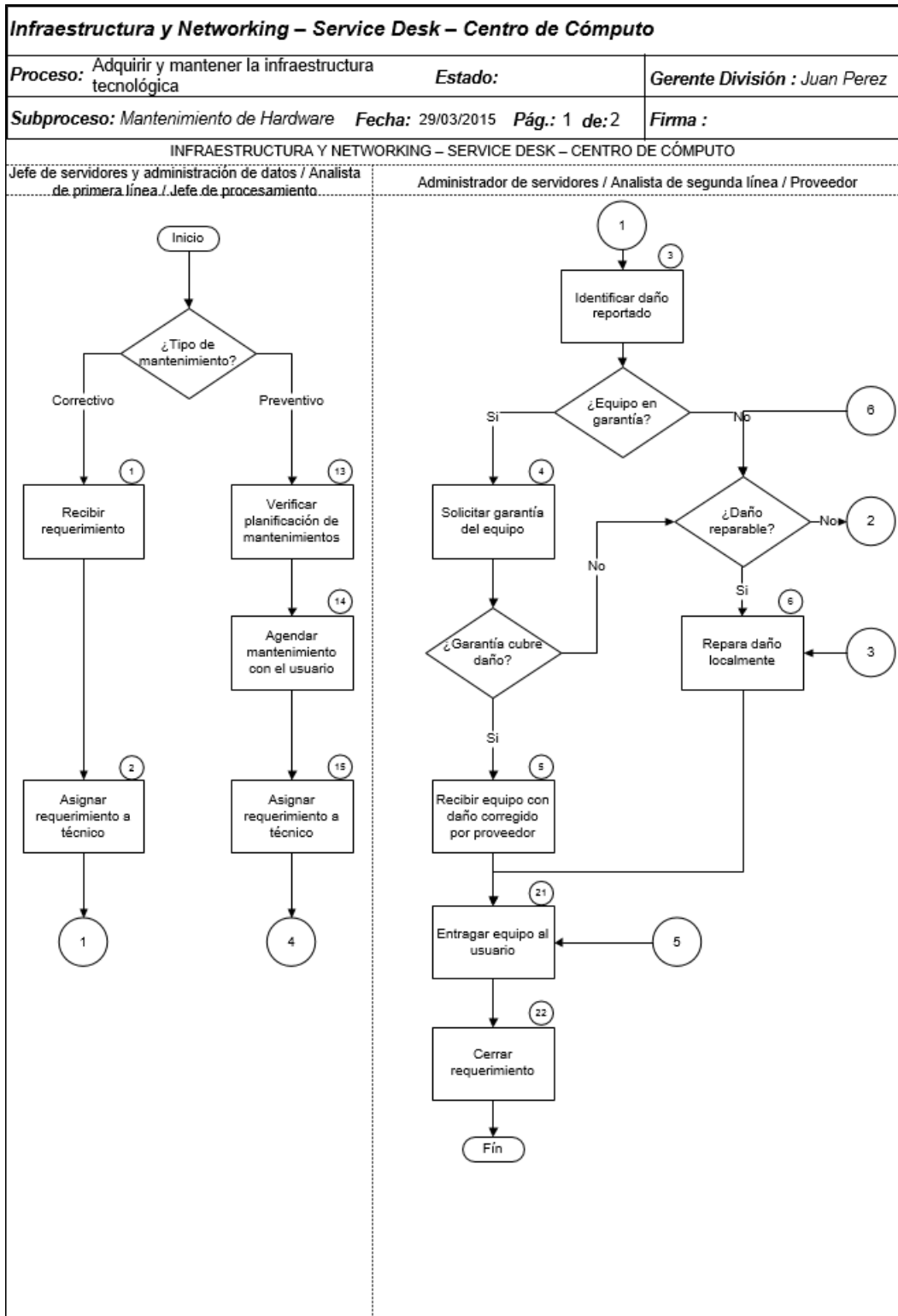


Figura 30. Proceso: Adquirir y mantener la infraestructura de TI  
Subproceso: Mantenimiento de hardware

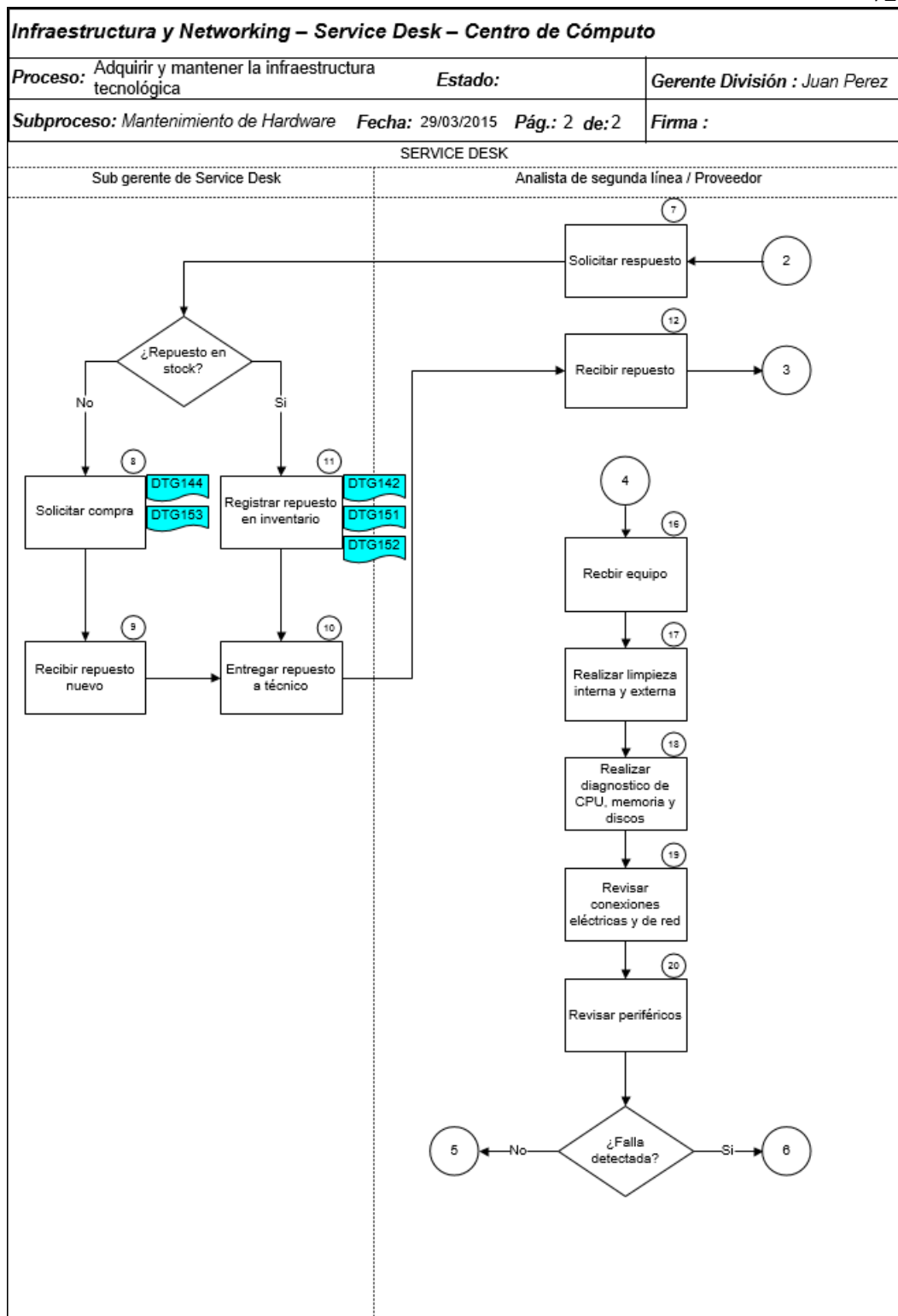


Figura 31. Proceso: Adquirir y mantener la infraestructura de TI  
Subproceso: Mantenimiento de hardware

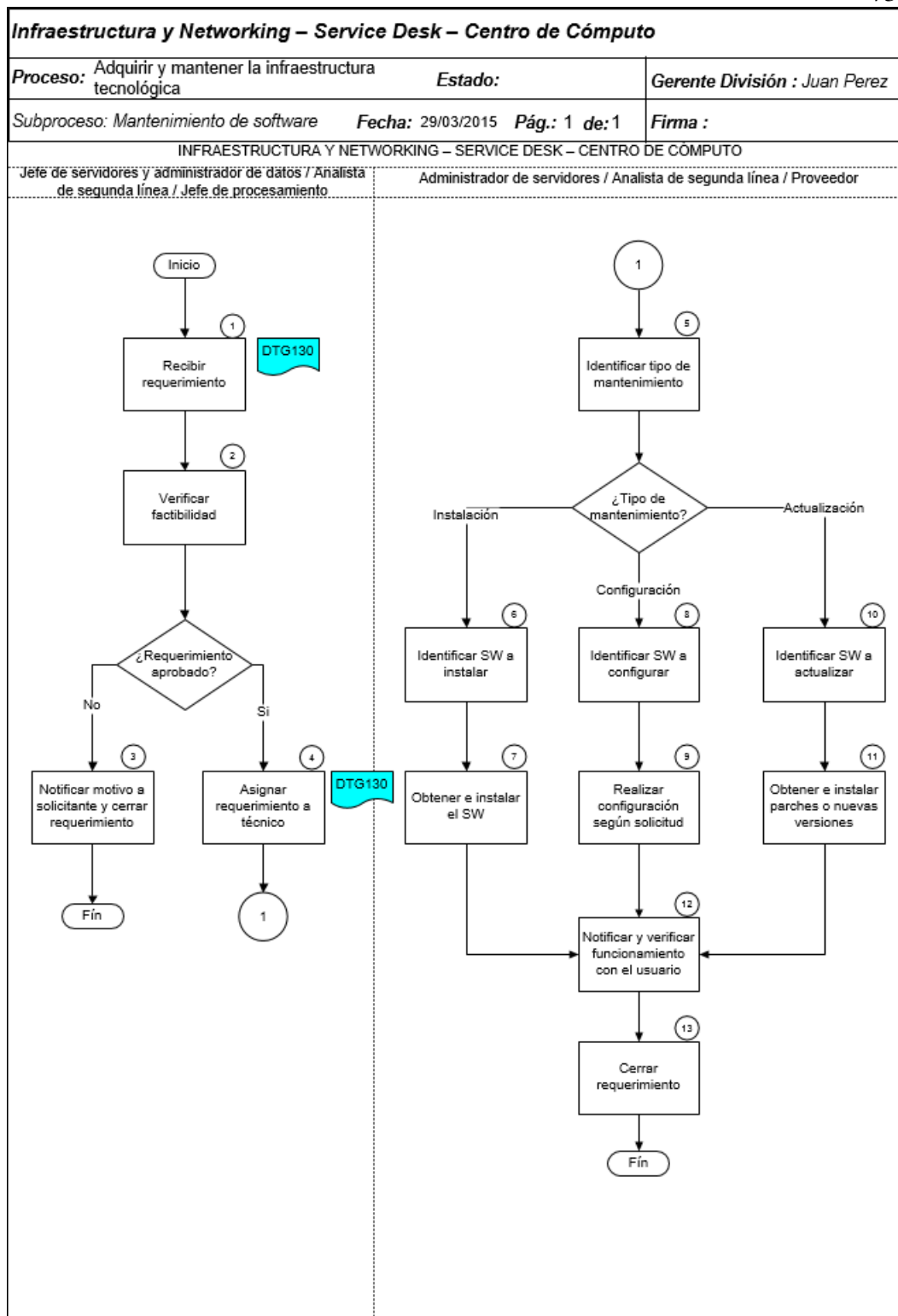


Figura 32. Proceso: Adquirir y mantener la infraestructura de TI  
Subproceso: Mantenimiento de software



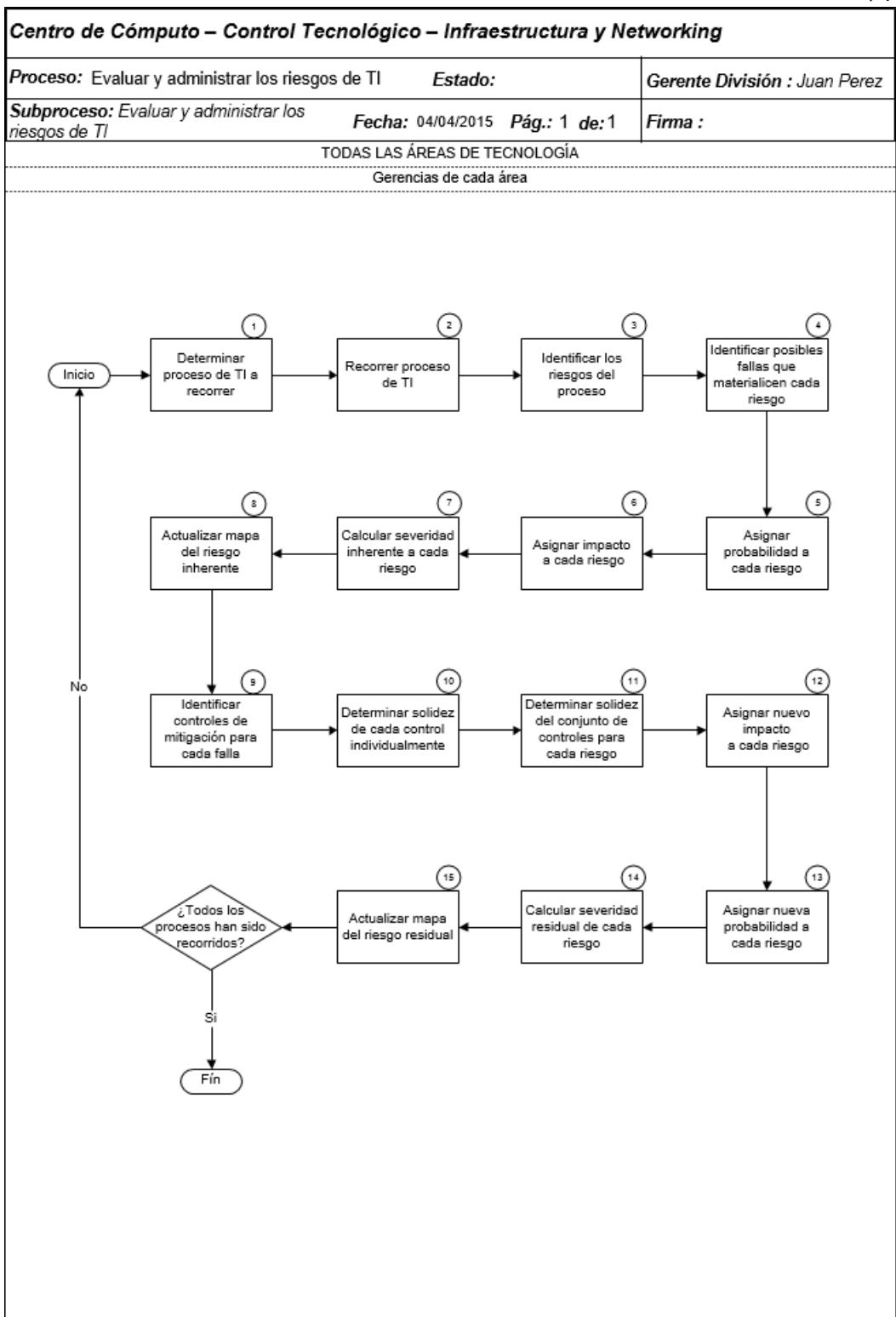


Figura 33. Proceso: Evaluar y administrar los riesgos de TI  
 Subproceso: Evaluar y Administrar los riesgos de TI

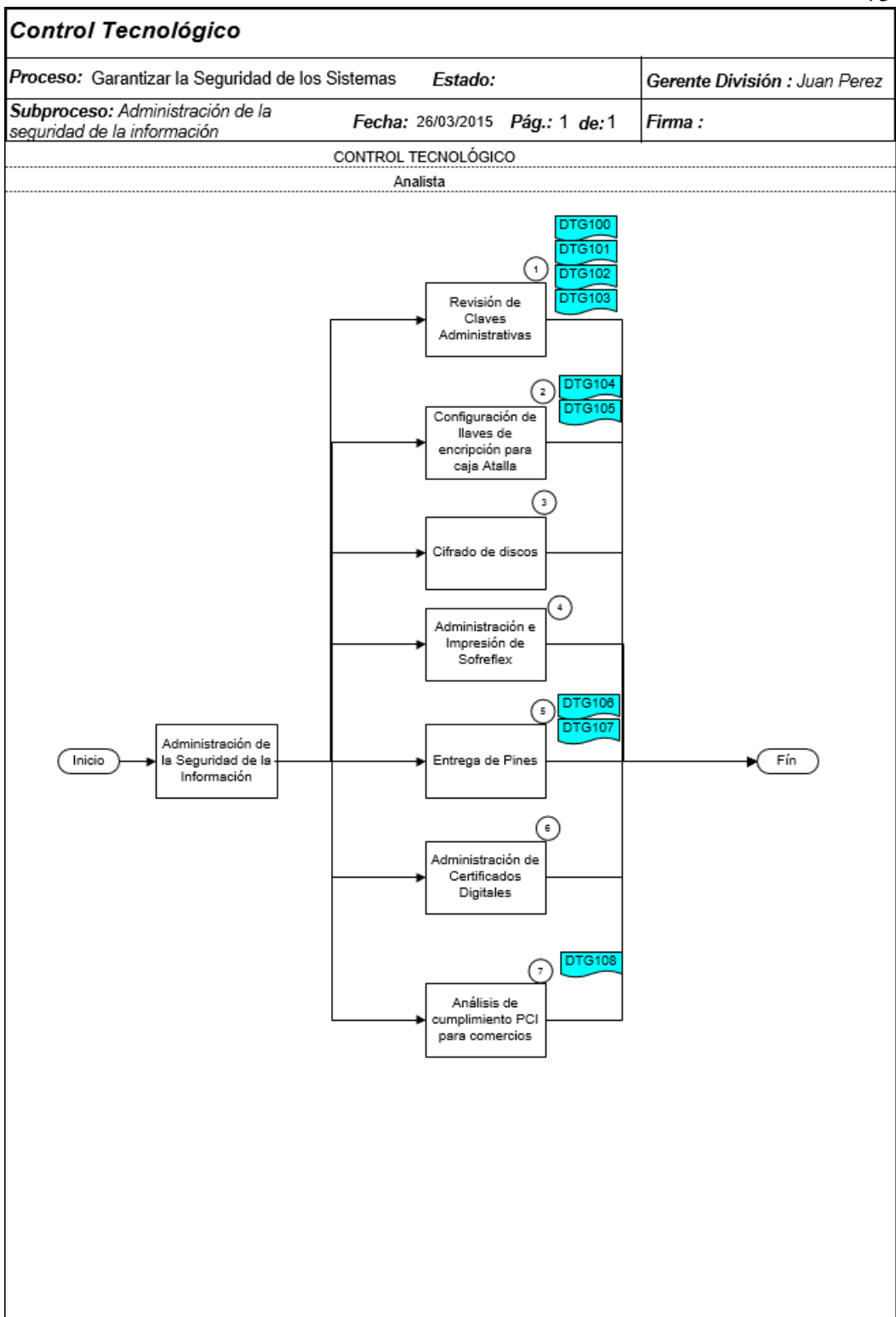


Figura 34. Proceso: Garantizar la seguridad de los sistemas  
 Subproceso: Administración de la seguridad de la información

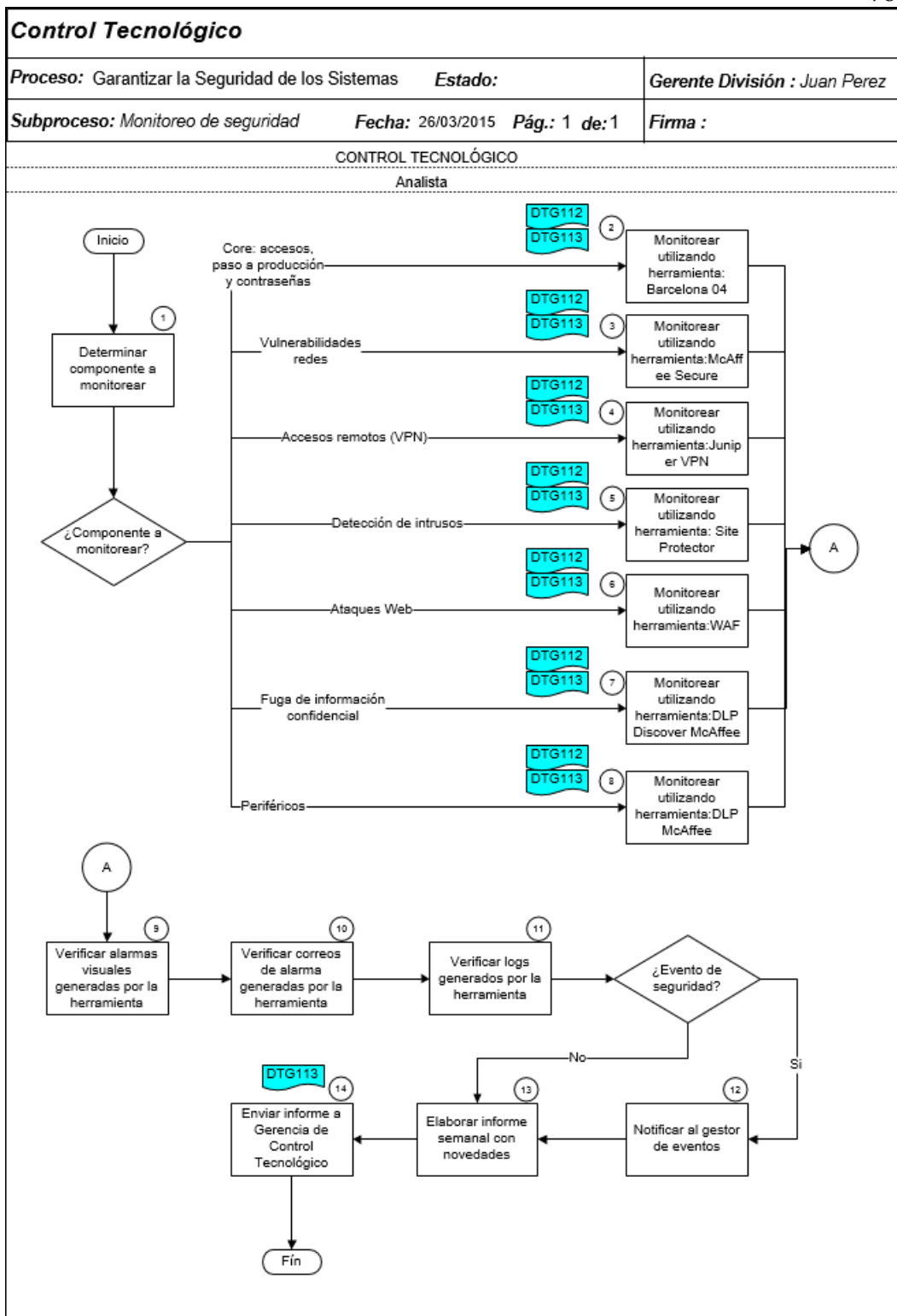


Figura 35. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Monitoreo de seguridad

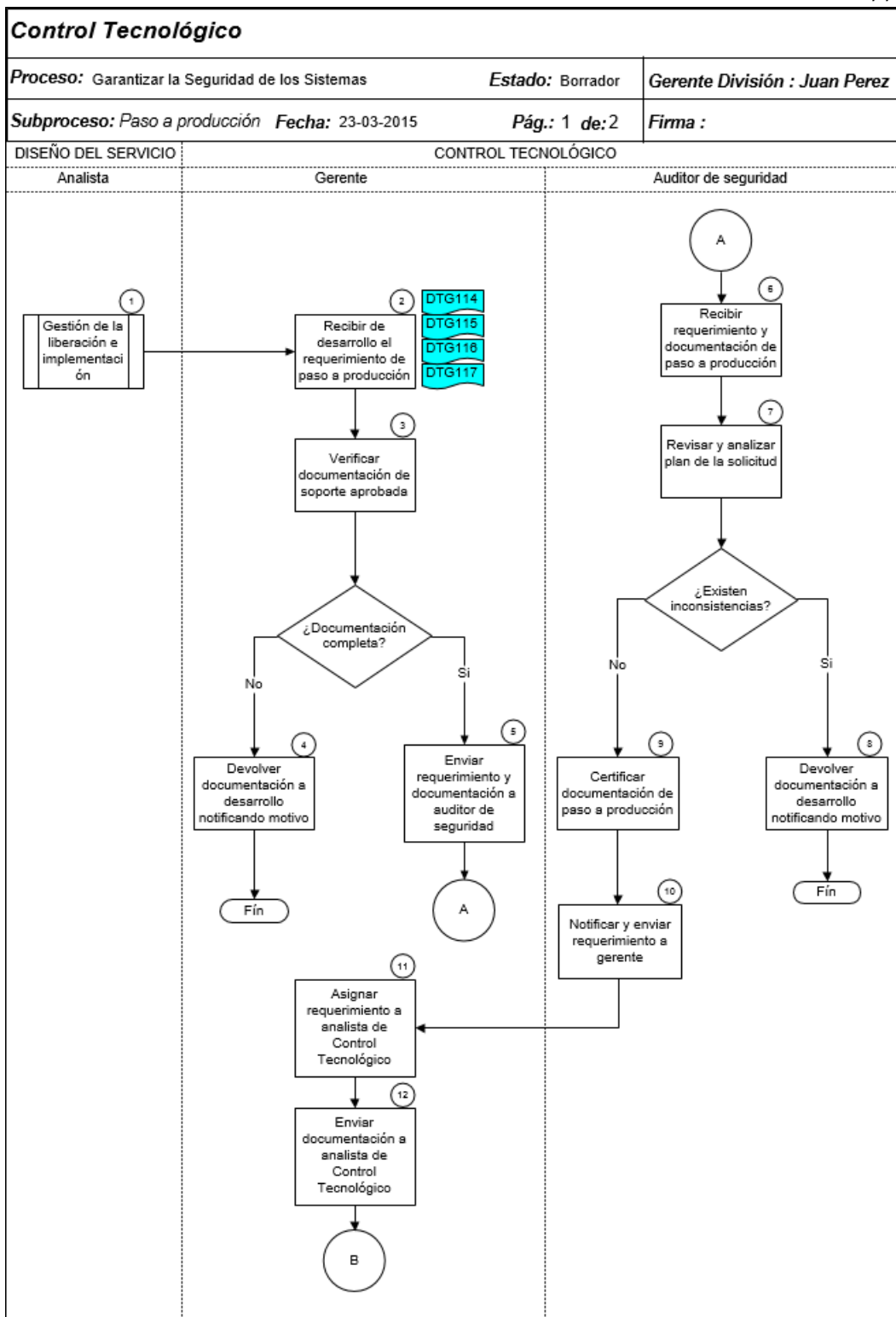


Figura 36. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Paso a producción

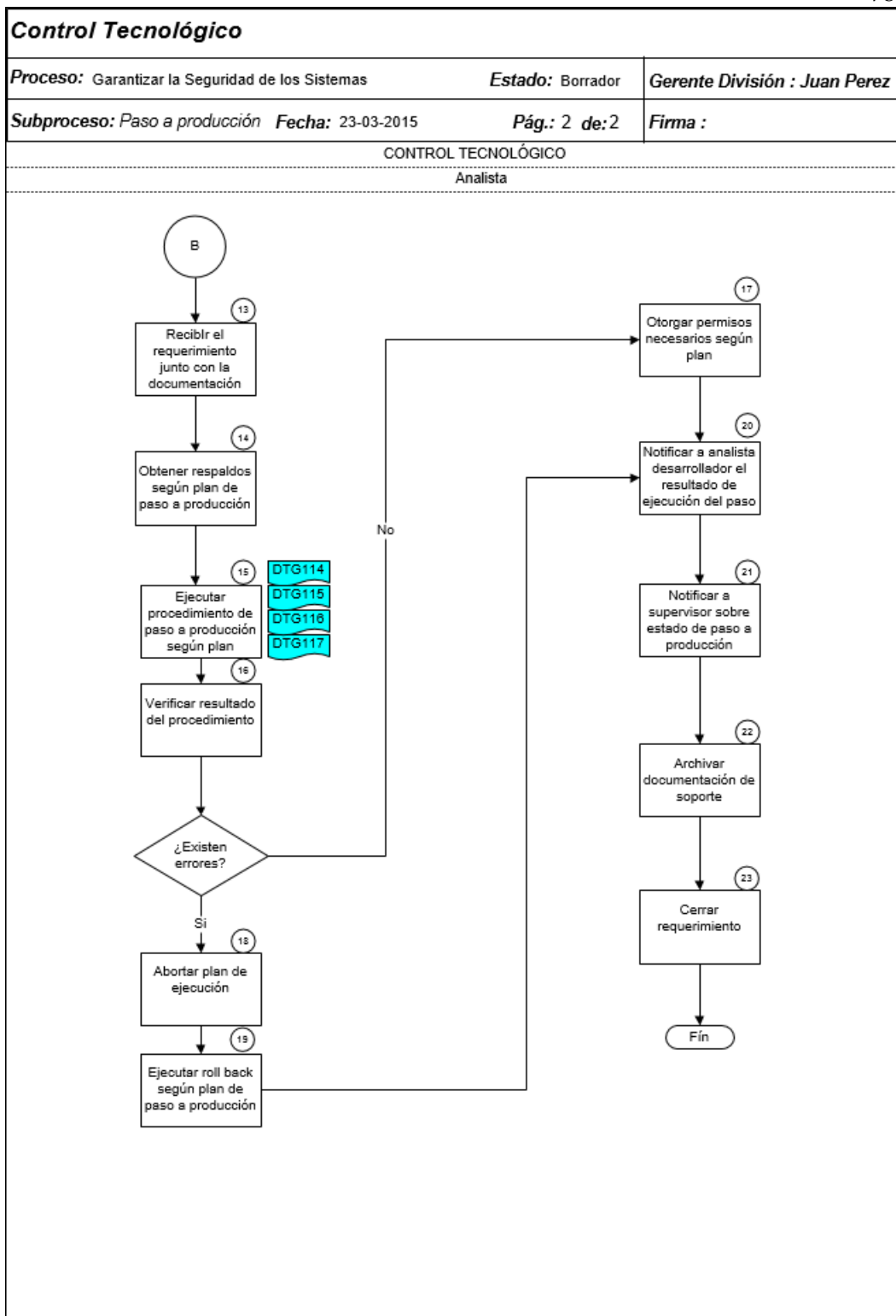


Figura 37. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Paso a producción

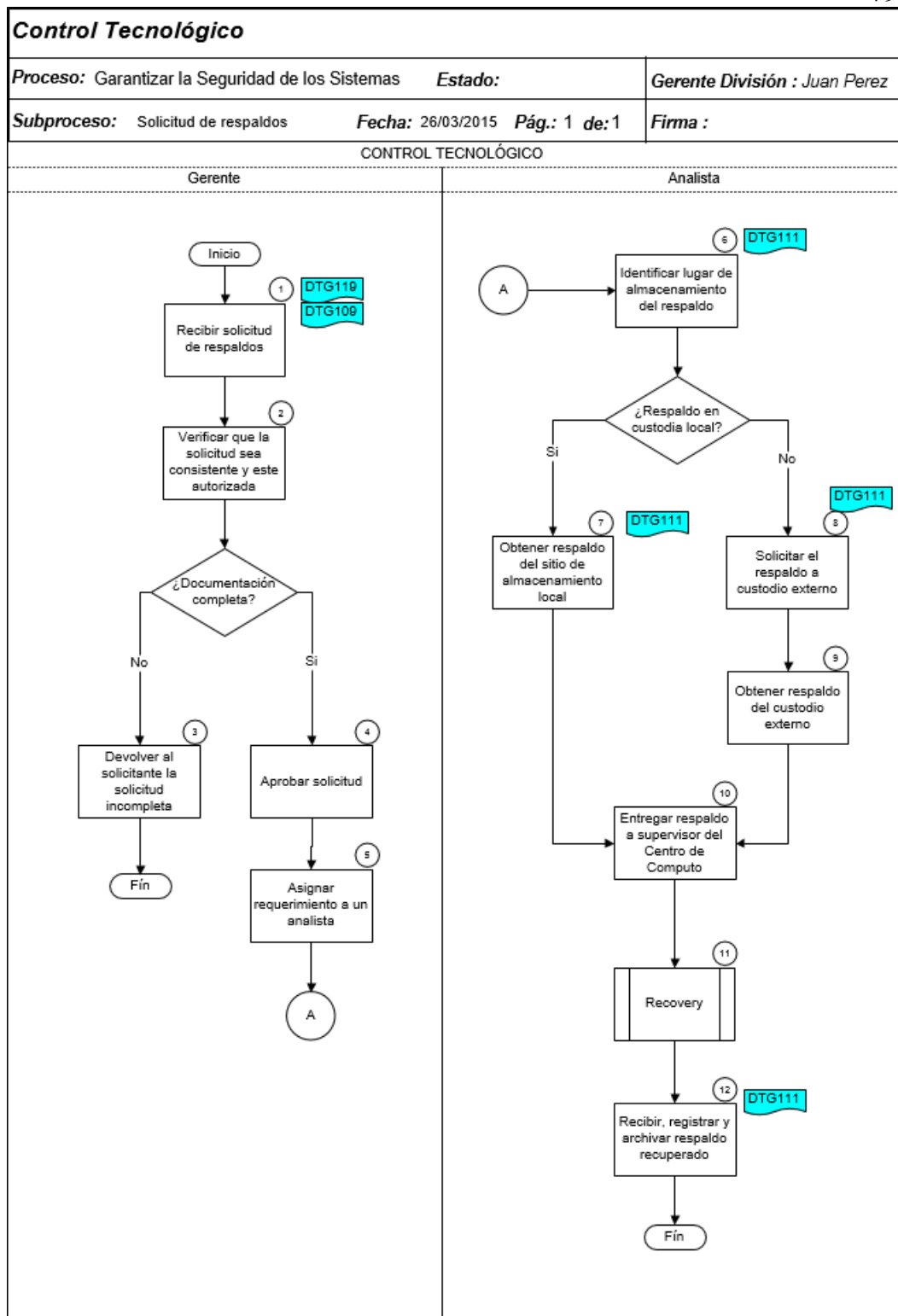


Figura 38. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Solicitud de respaldos

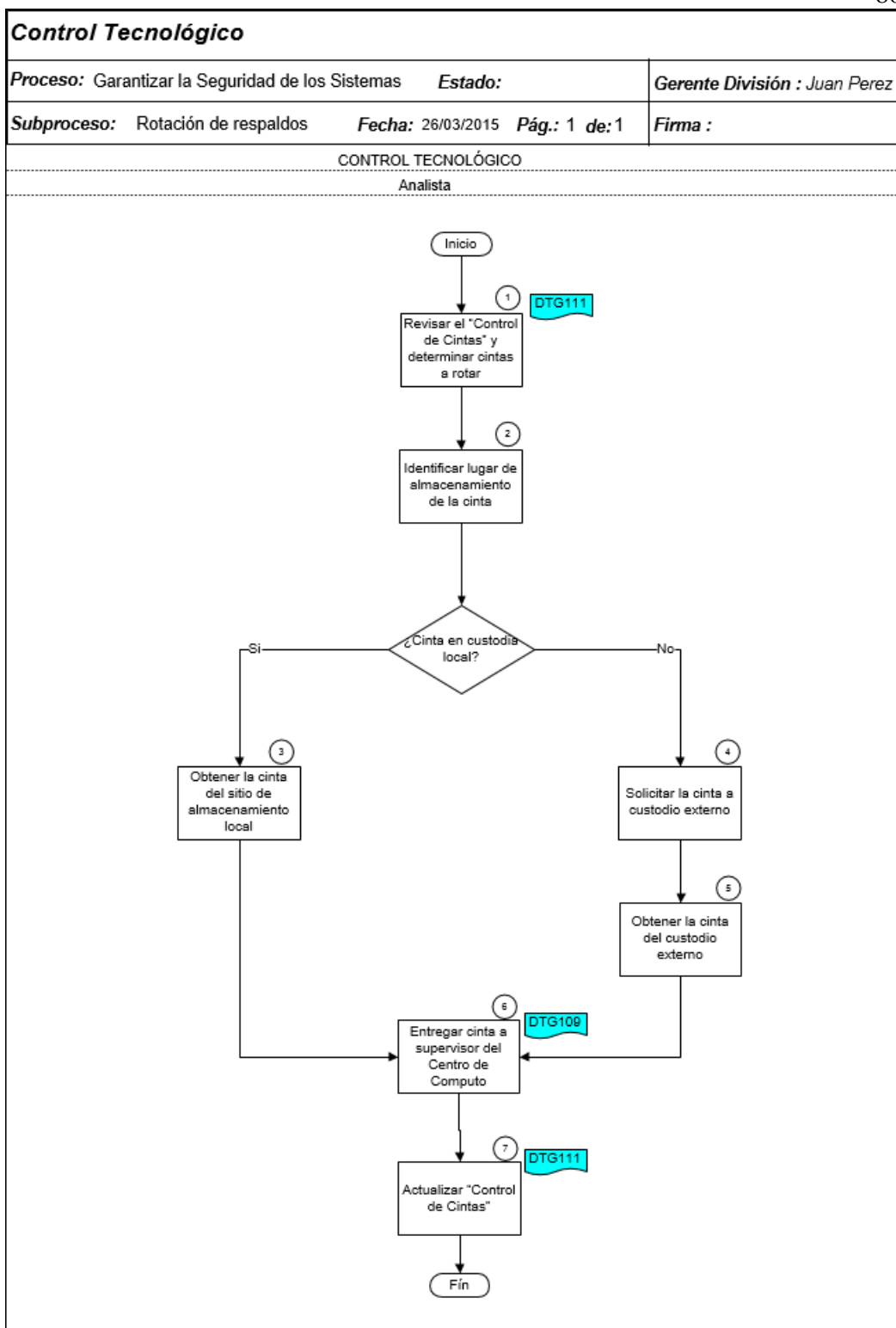


Figura 39. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Rotación de respaldos

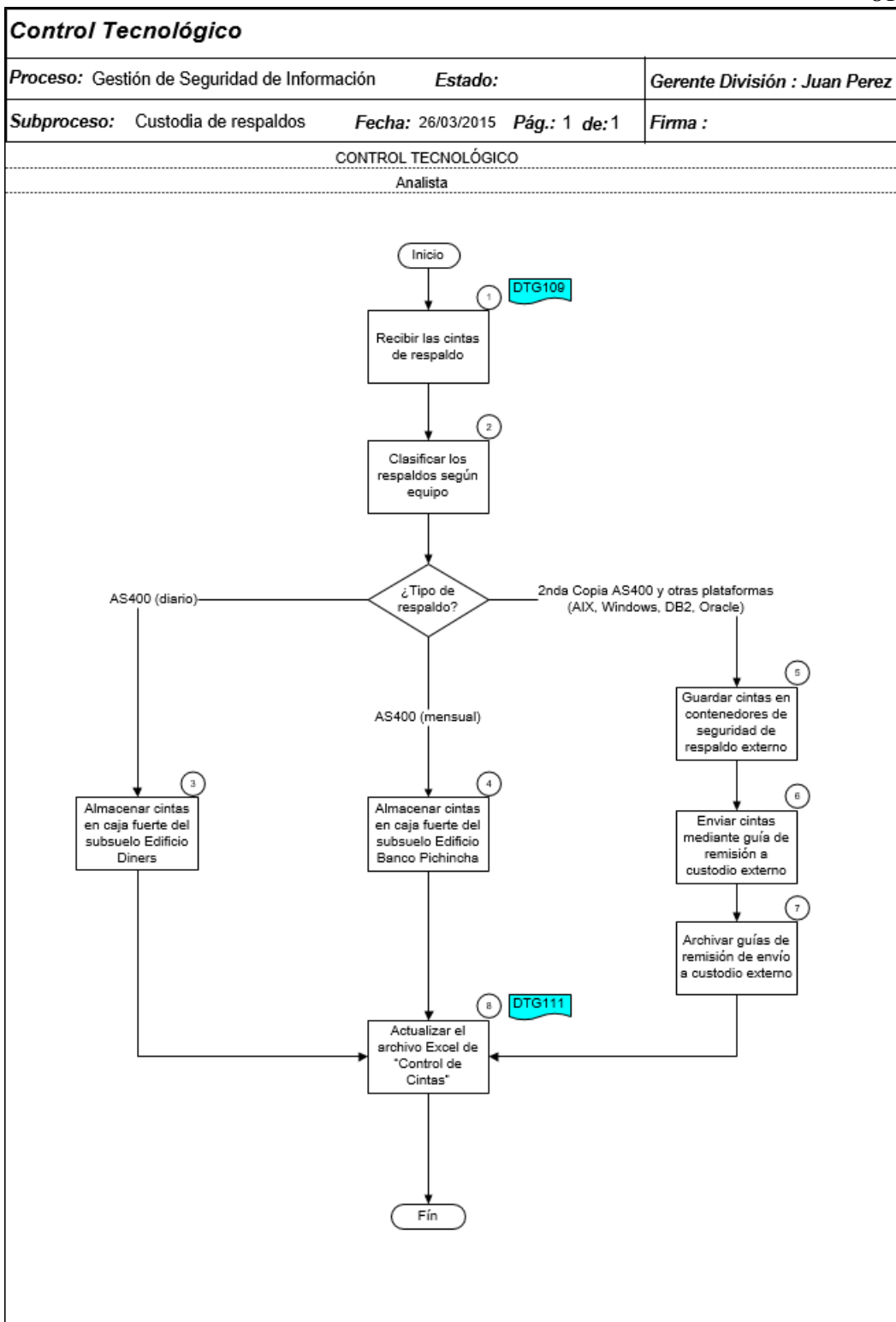


Figura 40. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Custodia de respaldos



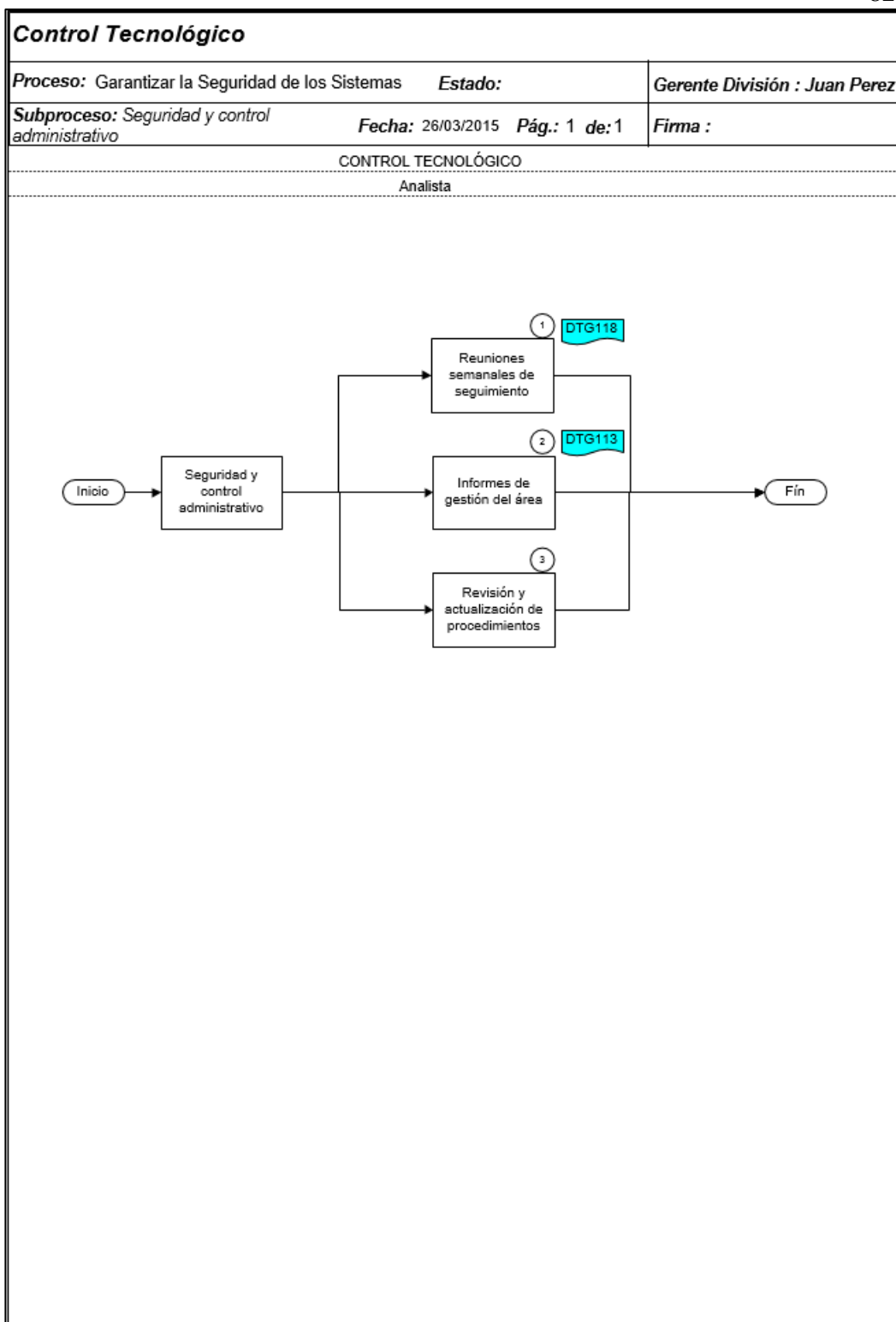


Figura 41. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Seguridad y control administrativo

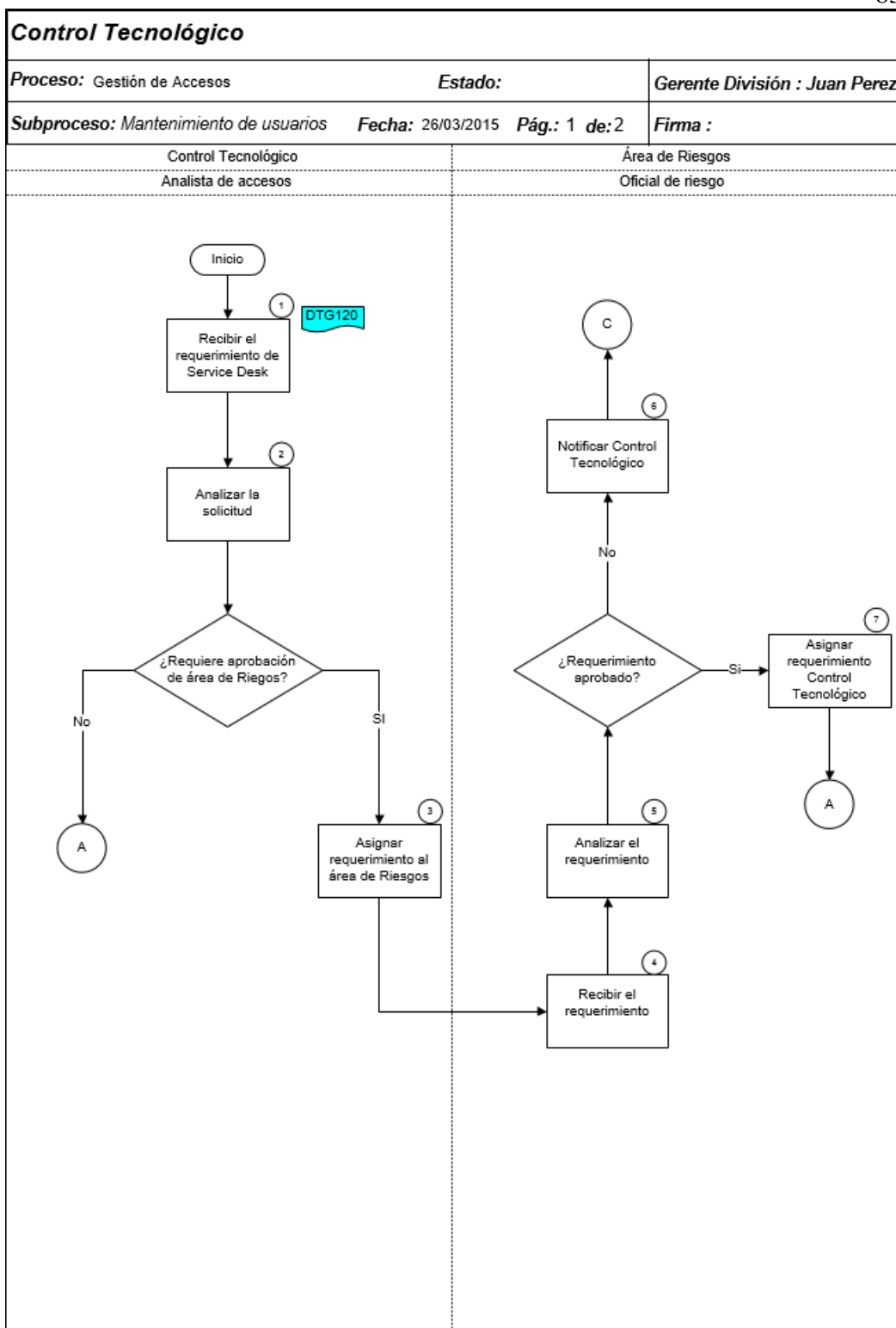


Figura 42. Proceso: Gestión de accesos  
Subproceso: Mantenimiento de usuarios

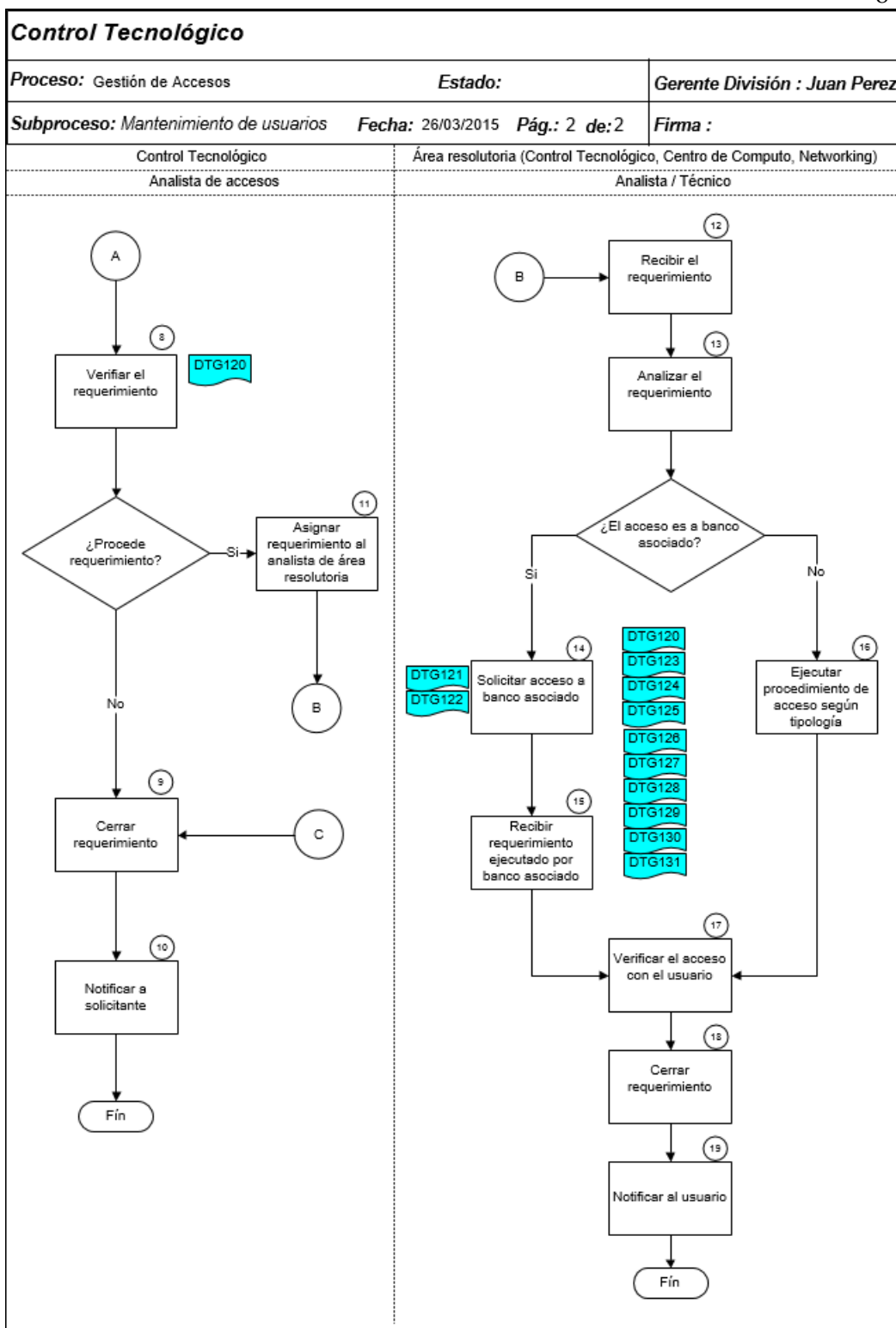


Figura 43. Proceso: Gestión de accesos  
Subproceso: Mantenimiento de usuarios

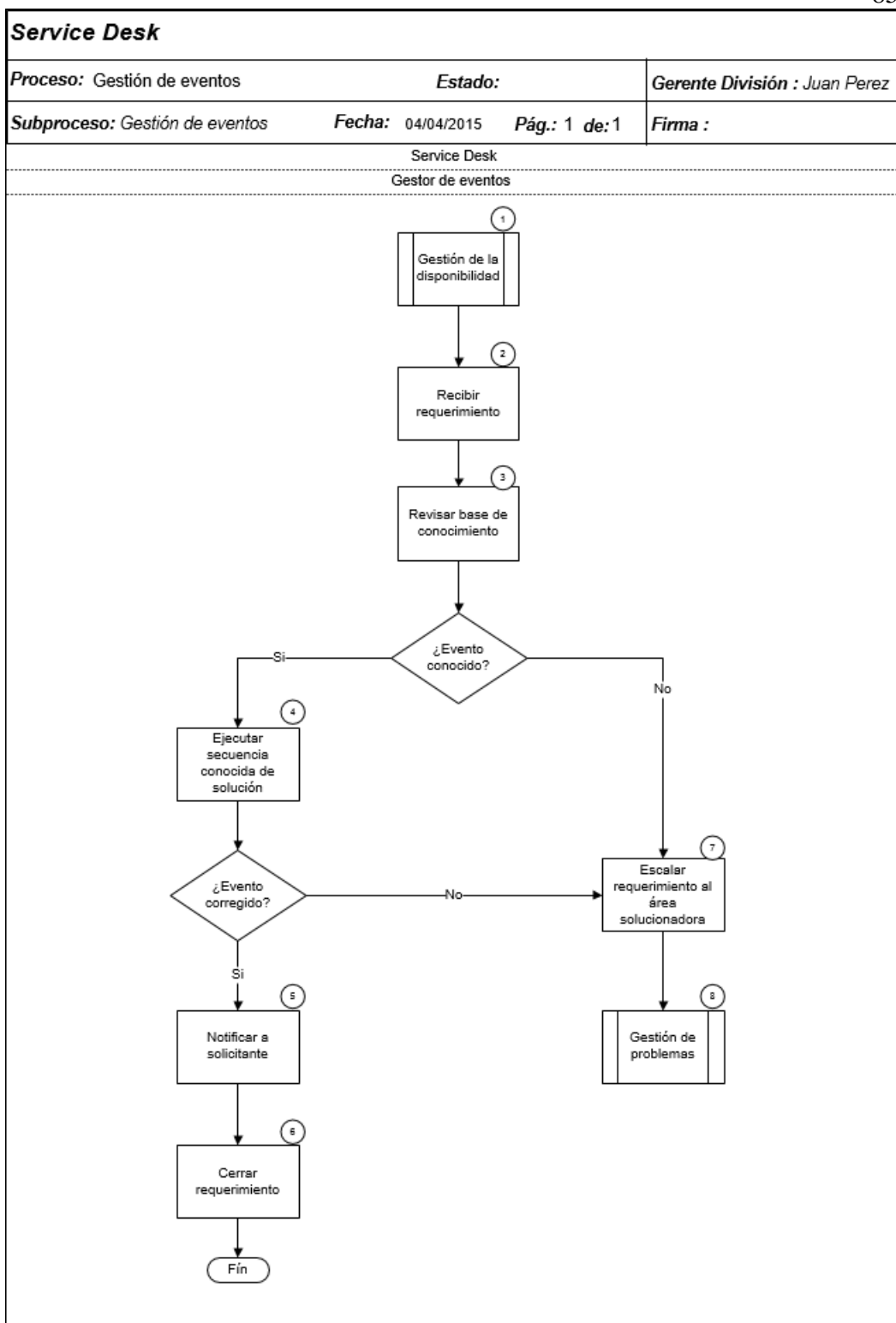


Figura 44. Proceso: Gestión de eventos

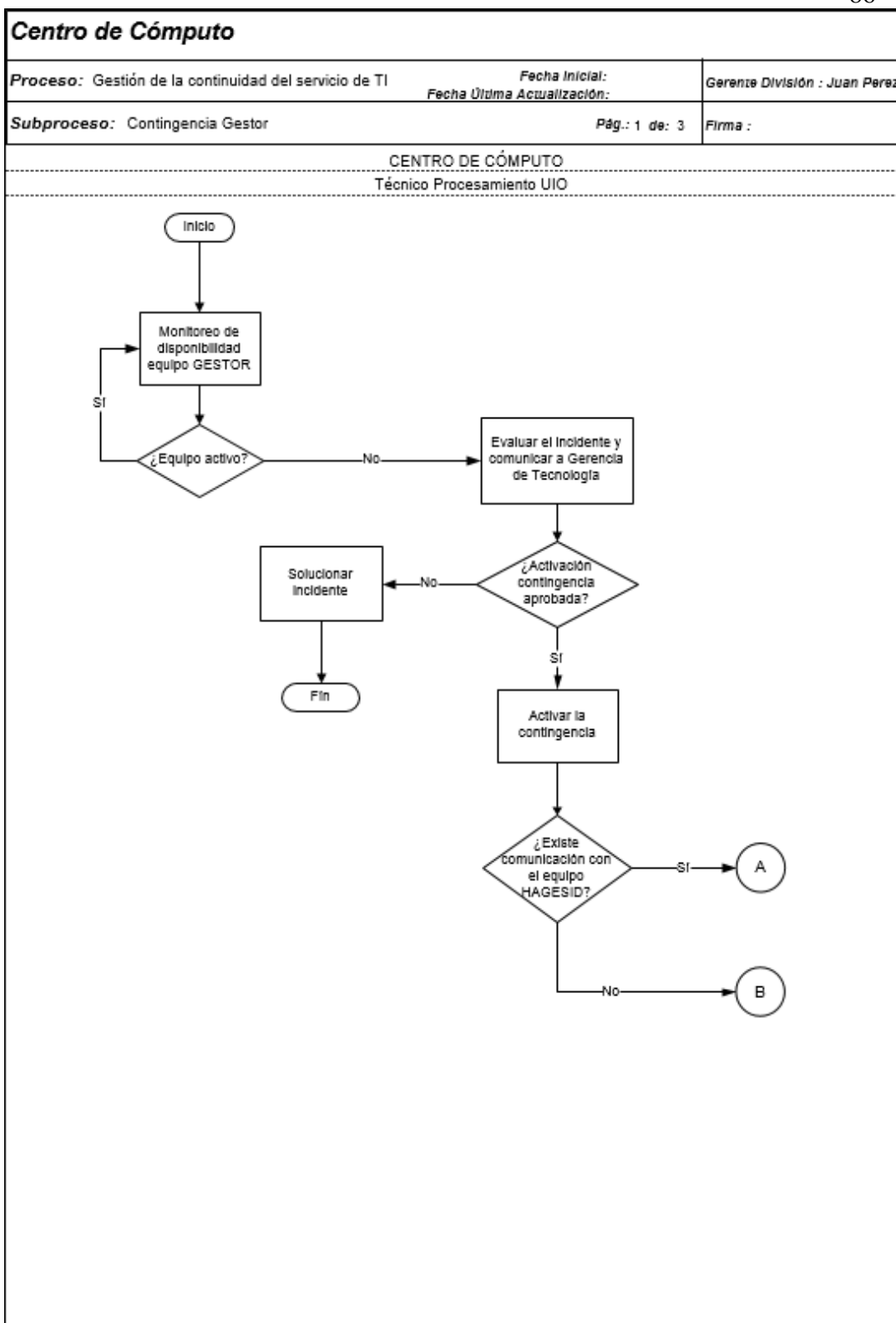


Figura 45. Proceso: Gestión de la continuidad de TI  
Subproceso: Contingencia Peoplesoft

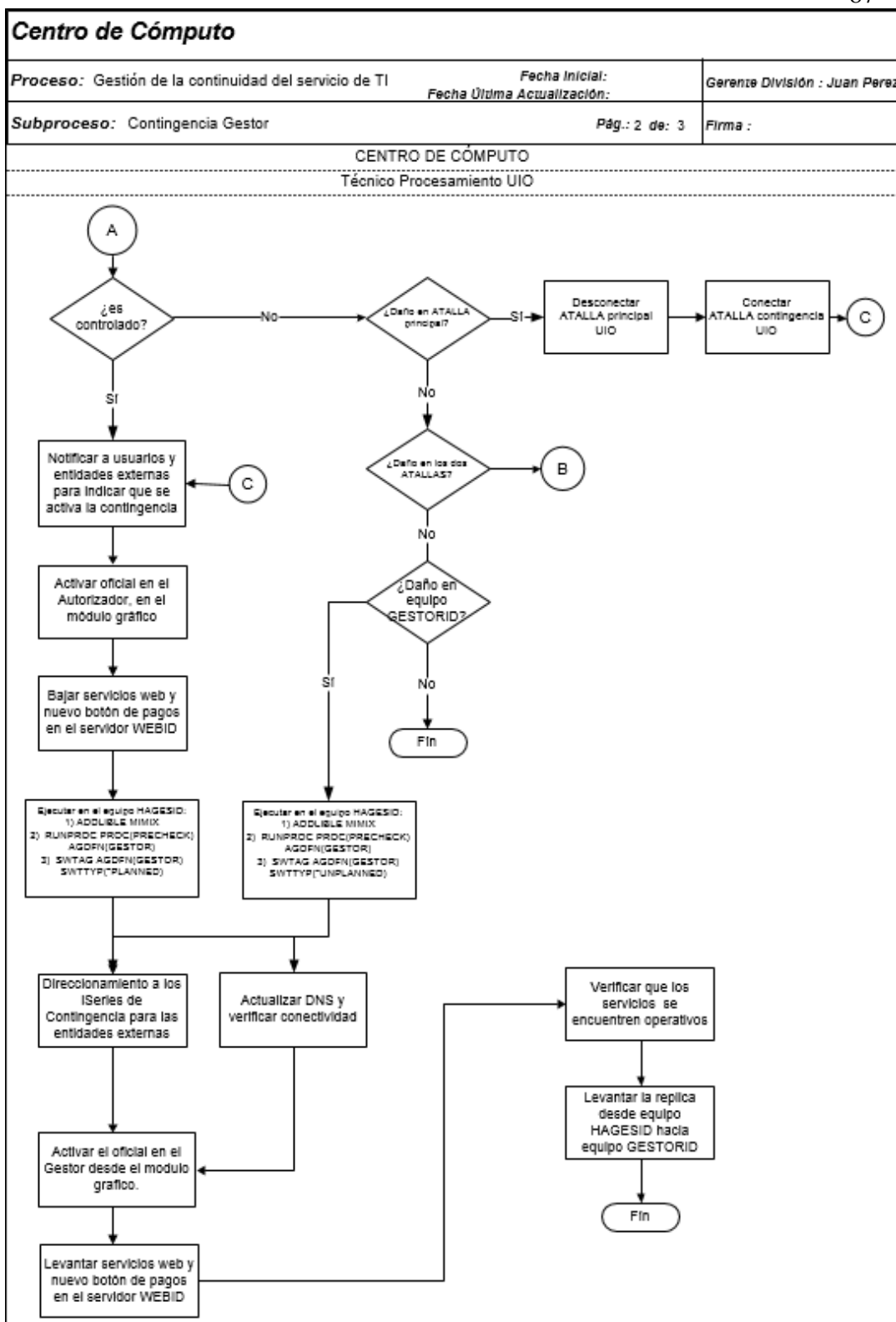


Figura 46. Proceso: Gestión de la continuidad de TI  
Subproceso: Contingencia Gestor

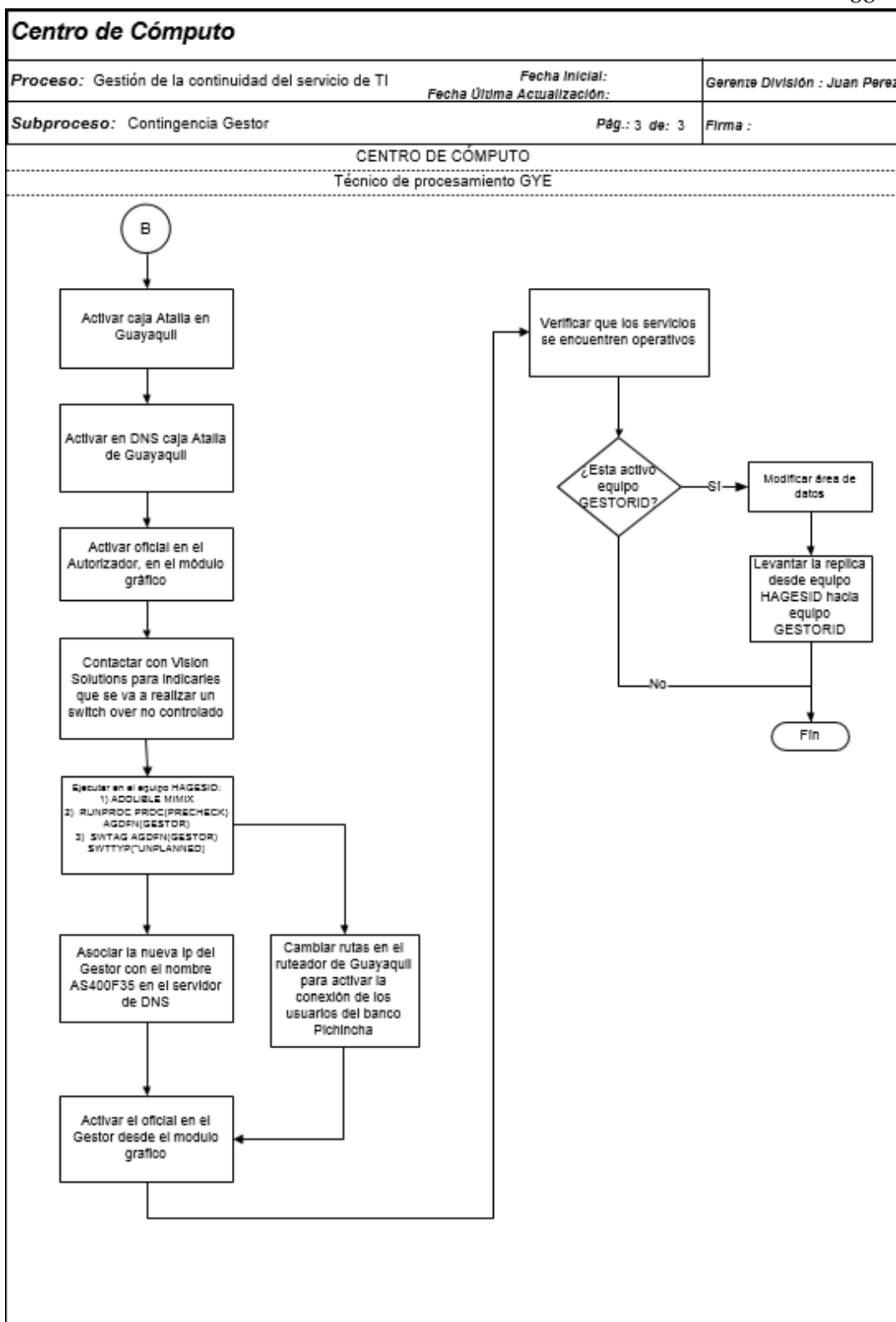


Figura 47. Proceso: Gestión de la continuidad de TI  
Subproceso: Contingencia Gestor

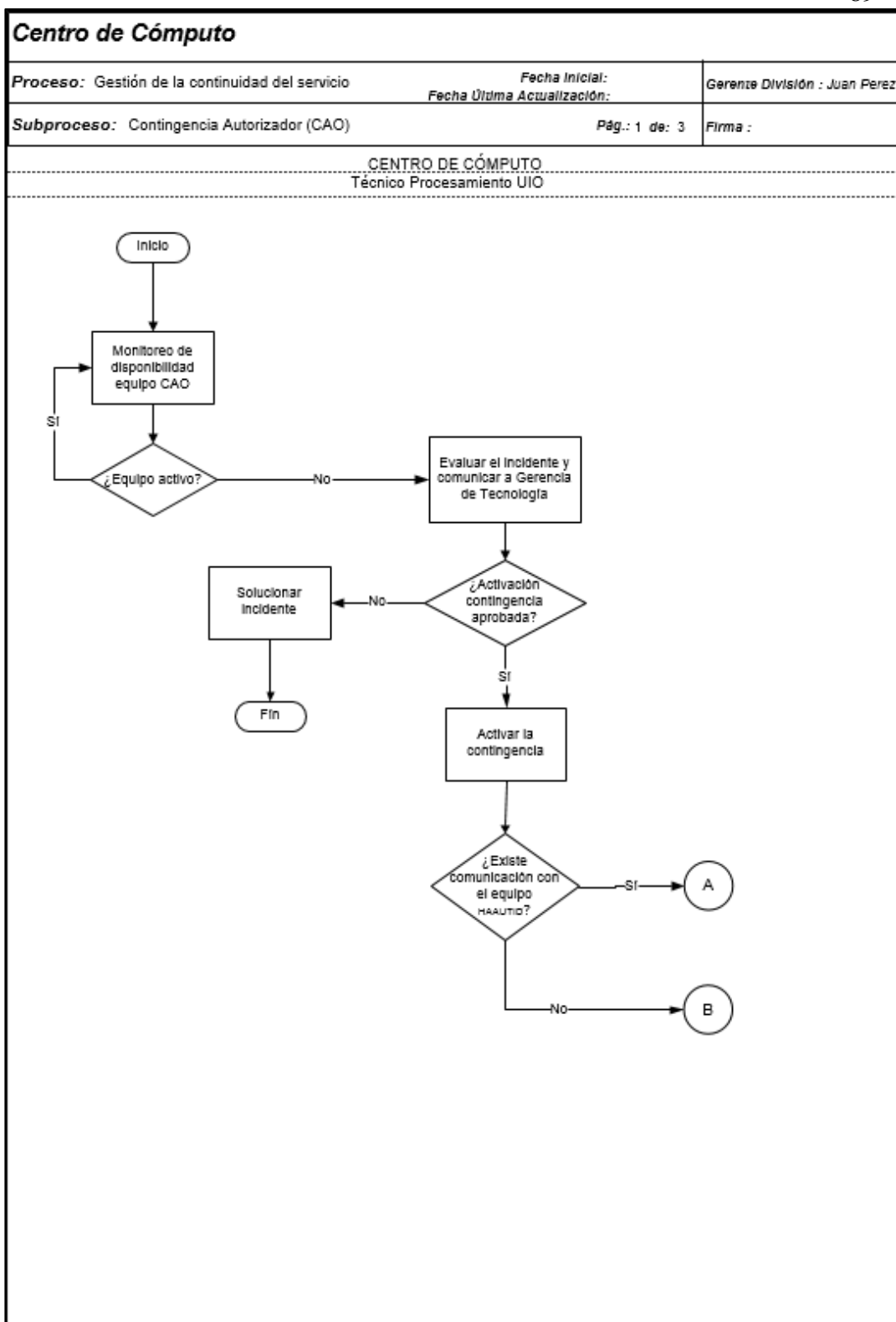


Figura 48. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Contingencia Autorizador



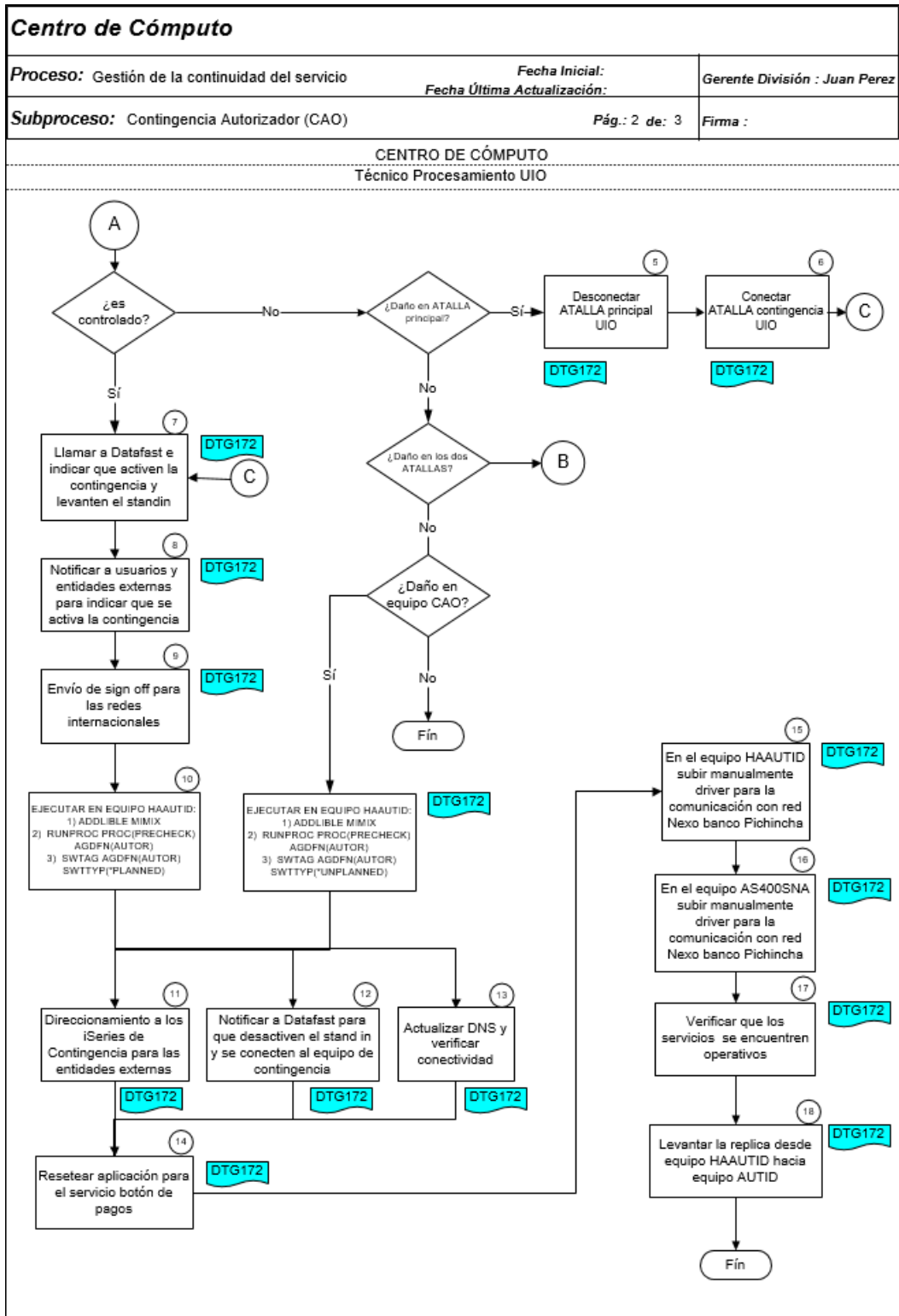


Figura 49. Proceso: Gestión de la continuidad del servicio  
Subproceso: Contingencia Autorizador

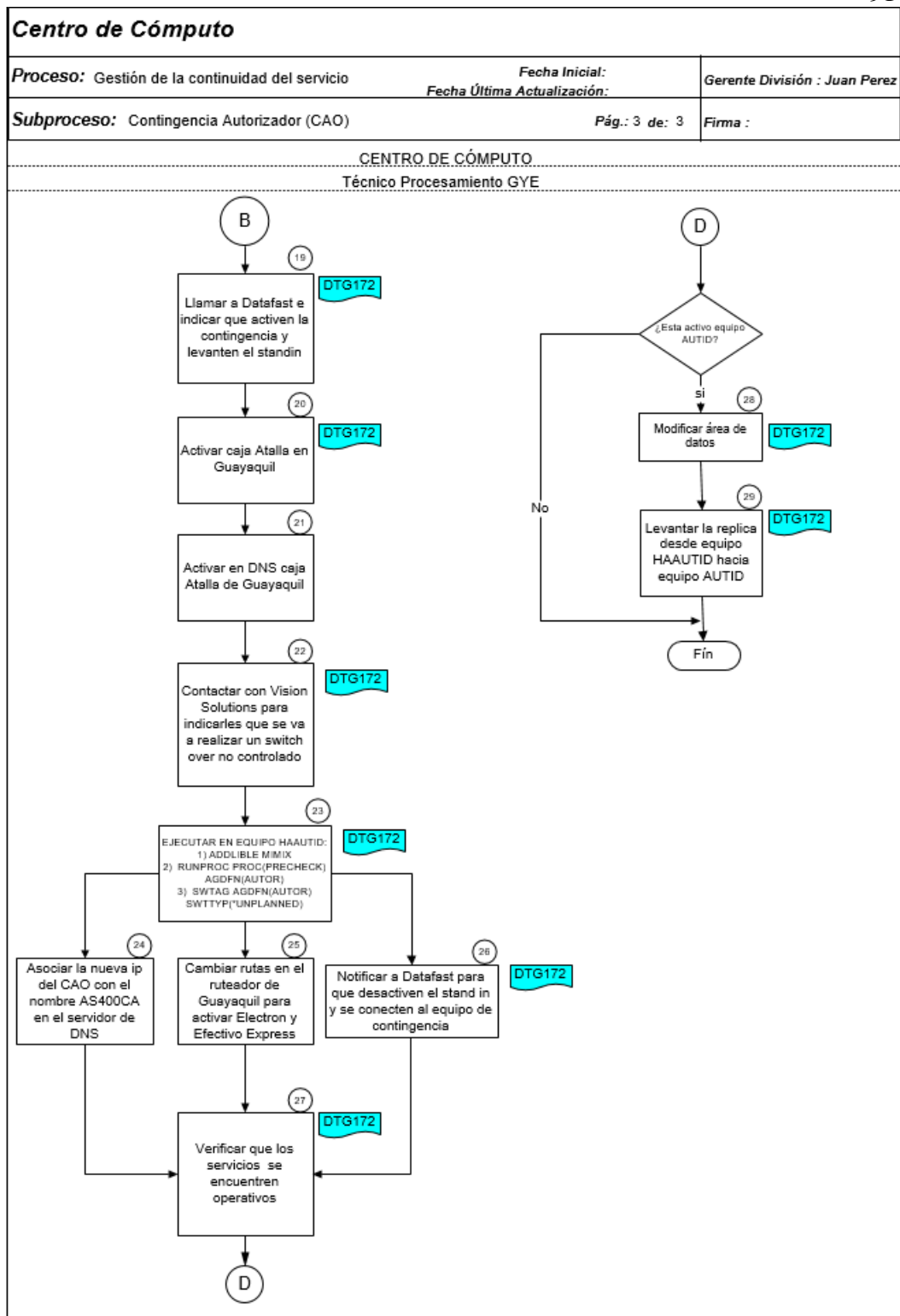


Figura 50. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Contingencia Autorizador

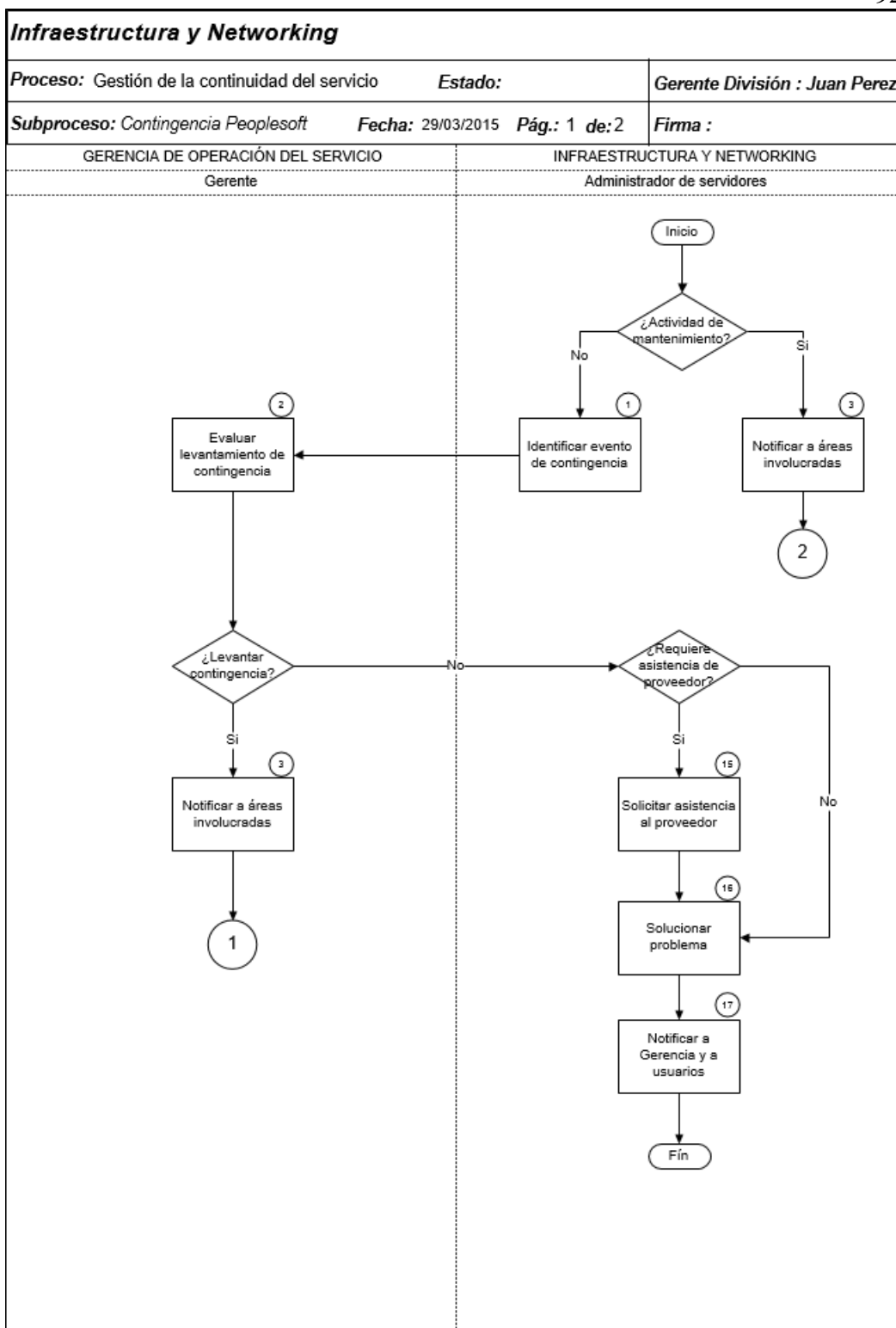


Figura 51. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Contingencia Peoplesoft

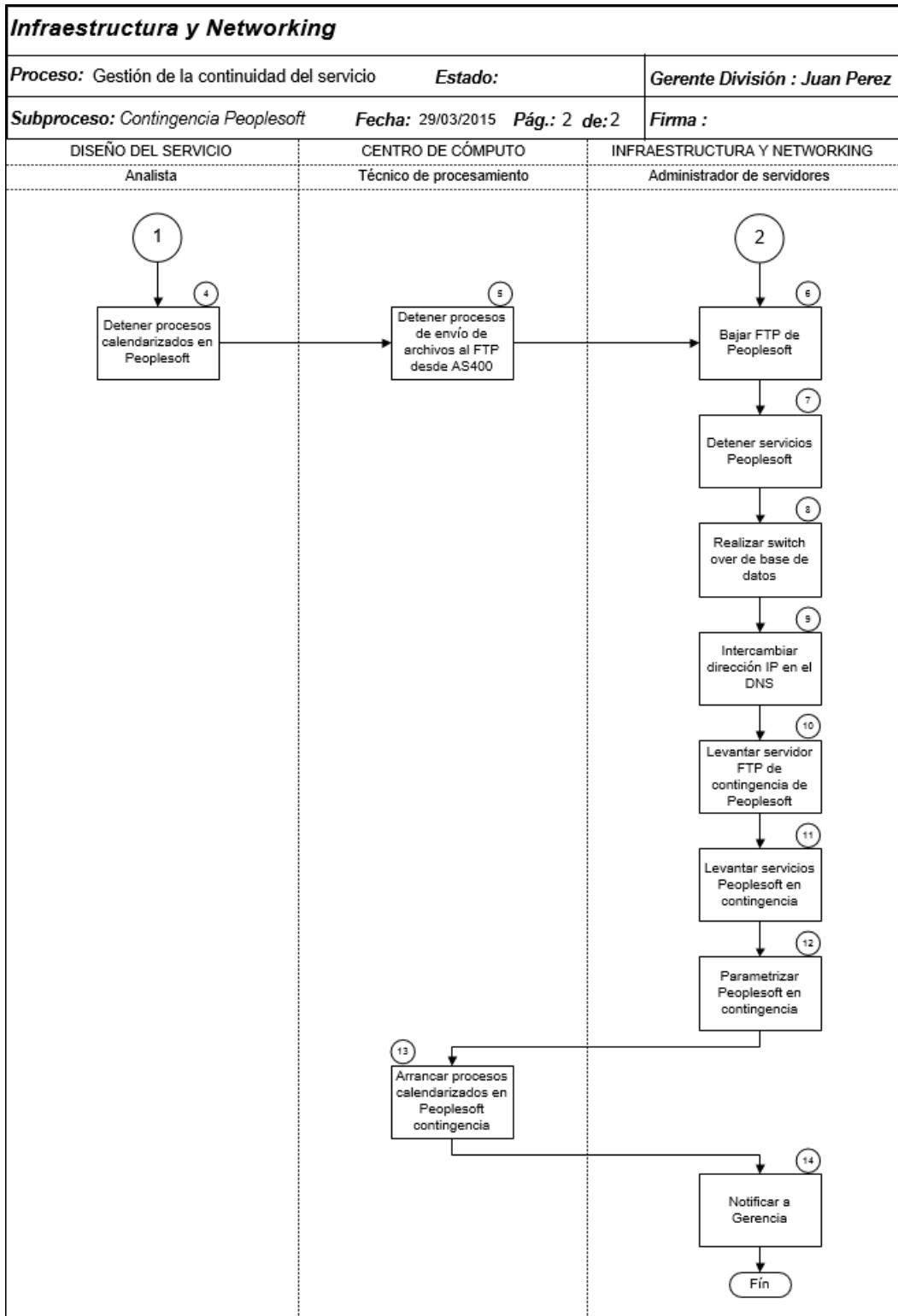


Figura 52. Proceso: Garantizar la seguridad de los sistemas  
Subproceso: Contingencia Peoplesoft

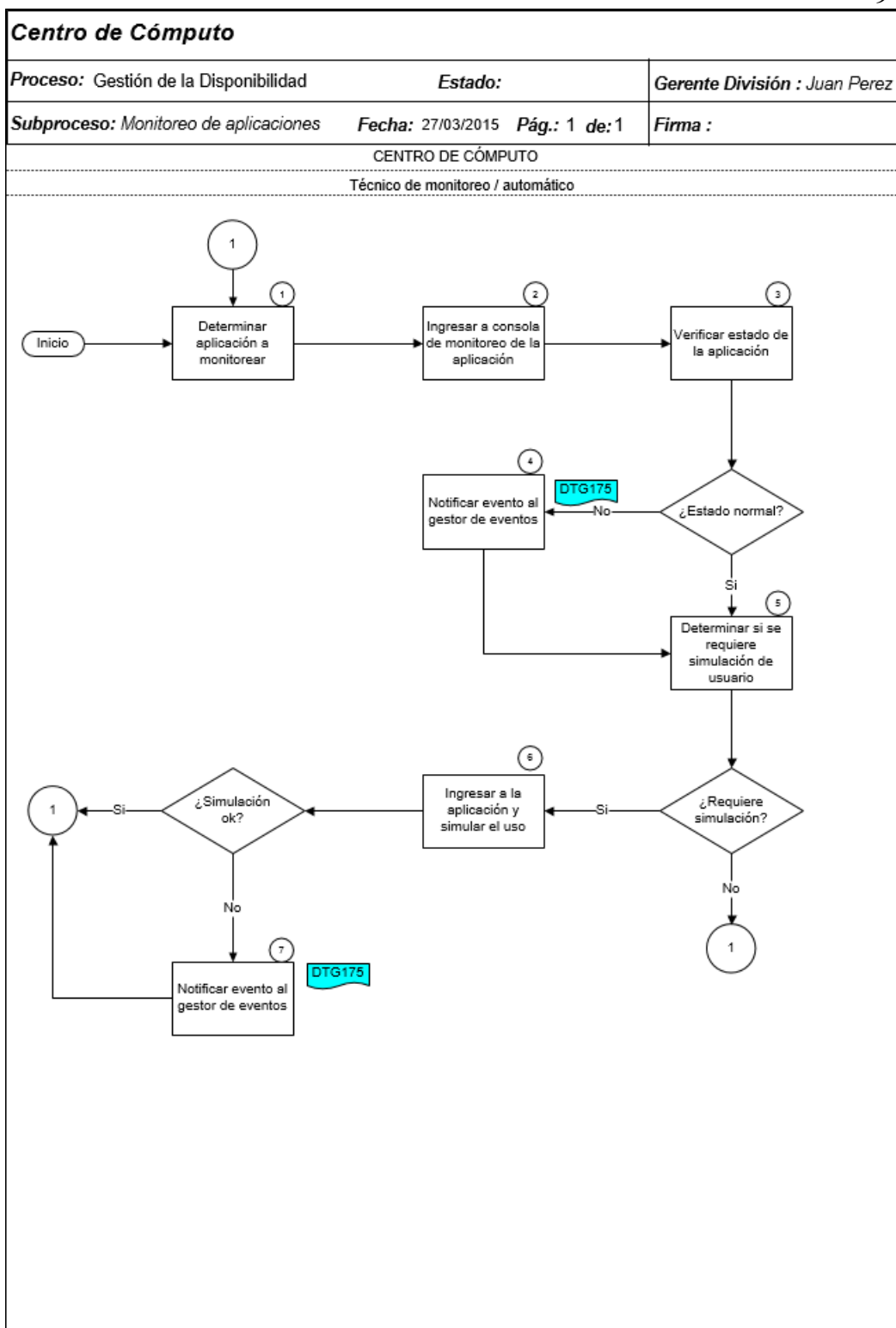


Figura 53. Proceso: Gestión de la disponibilidad  
Subproceso: Monitoreo de aplicaciones

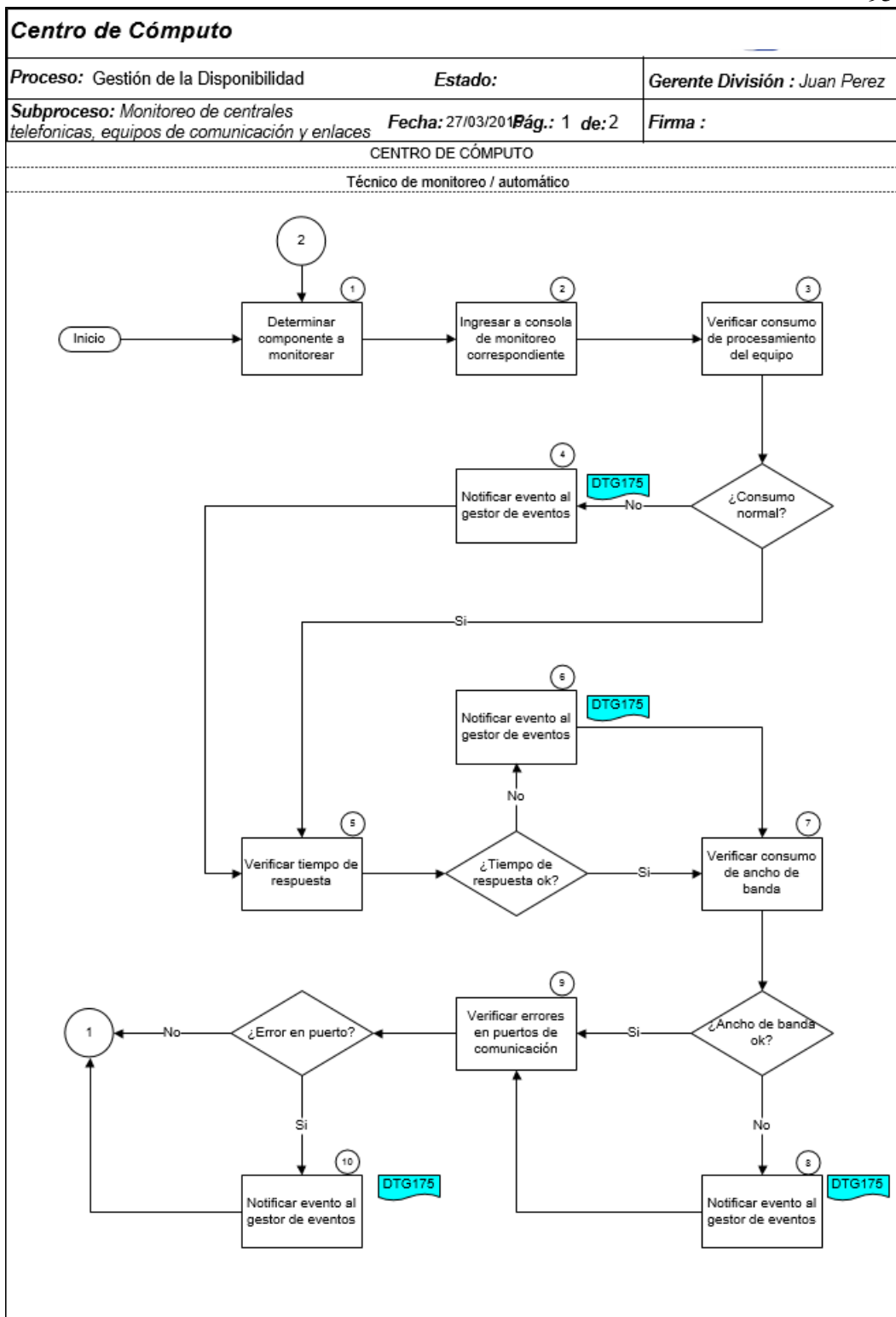


Figura 54. Proceso: Gestión de la disponibilidad  
 Subproceso: Monitoreo de centrales telefónicas, equipos de comunicación y enlaces

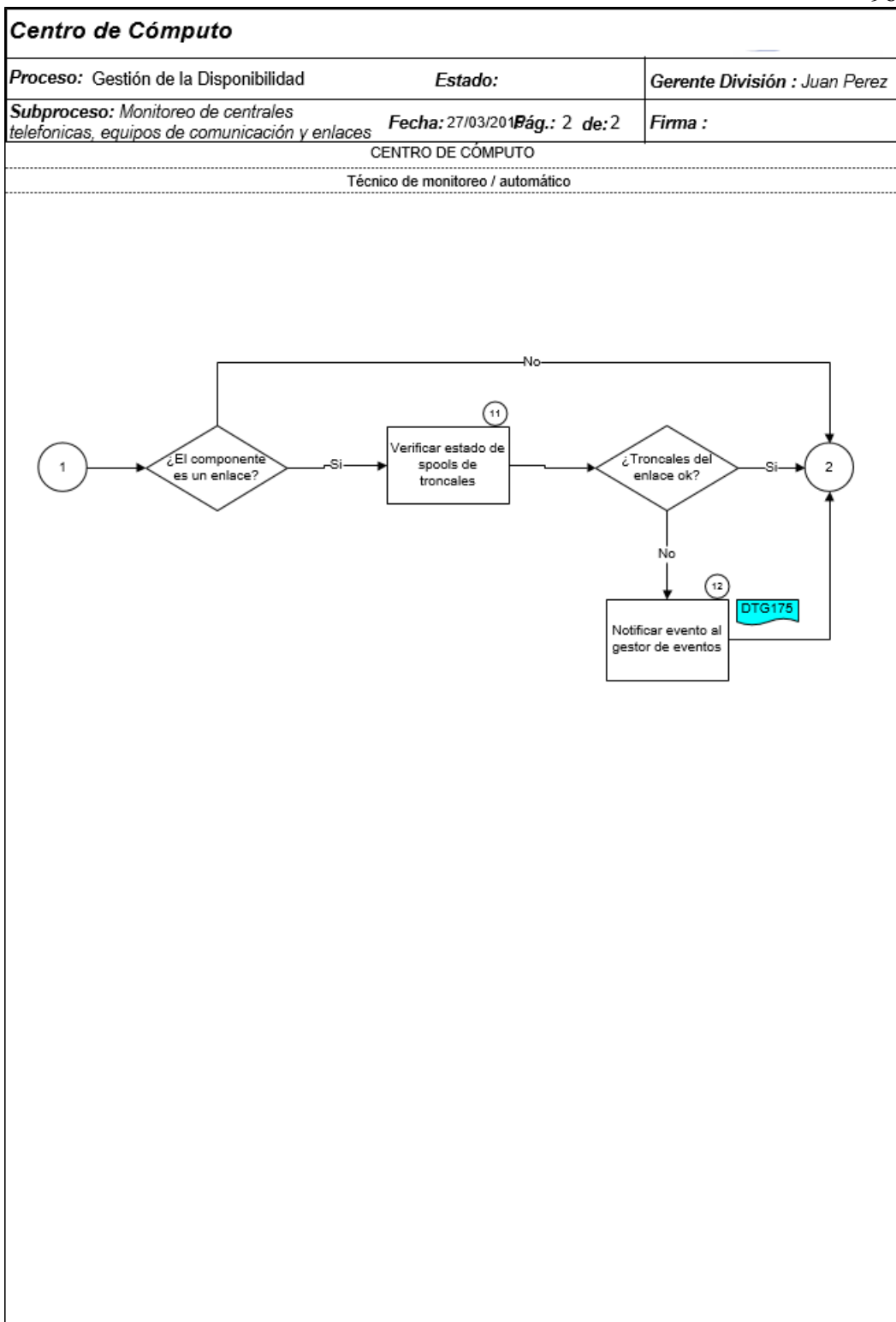


Figura 55. Proceso: Gestión de la disponibilidad  
 Subproceso: Monitoreo de centrales telefónicas, equipos de comunicación y enlaces

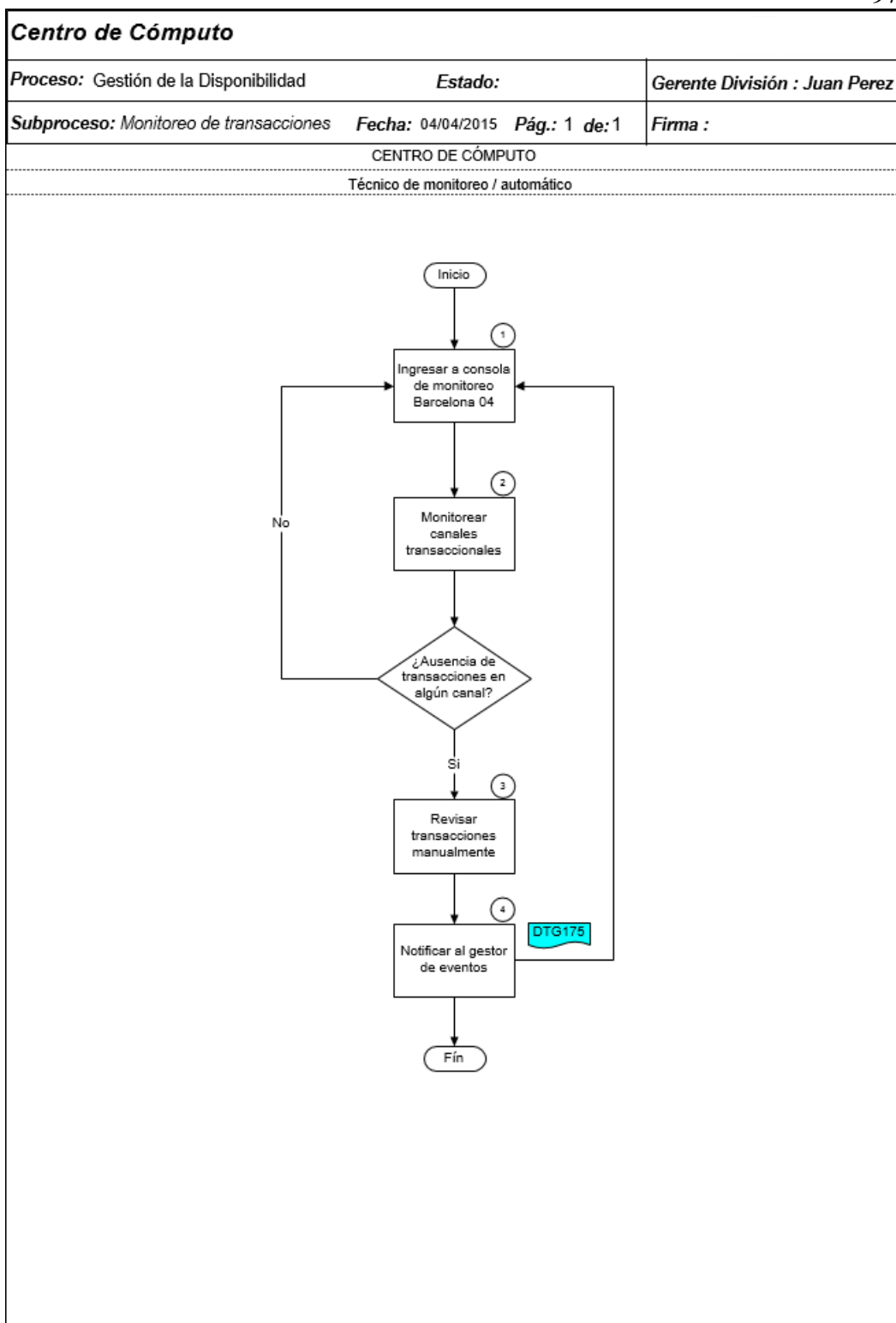


Figura 56. Proceso: Gestión de la disponibilidad  
Subproceso: Monitoreo de transacciones



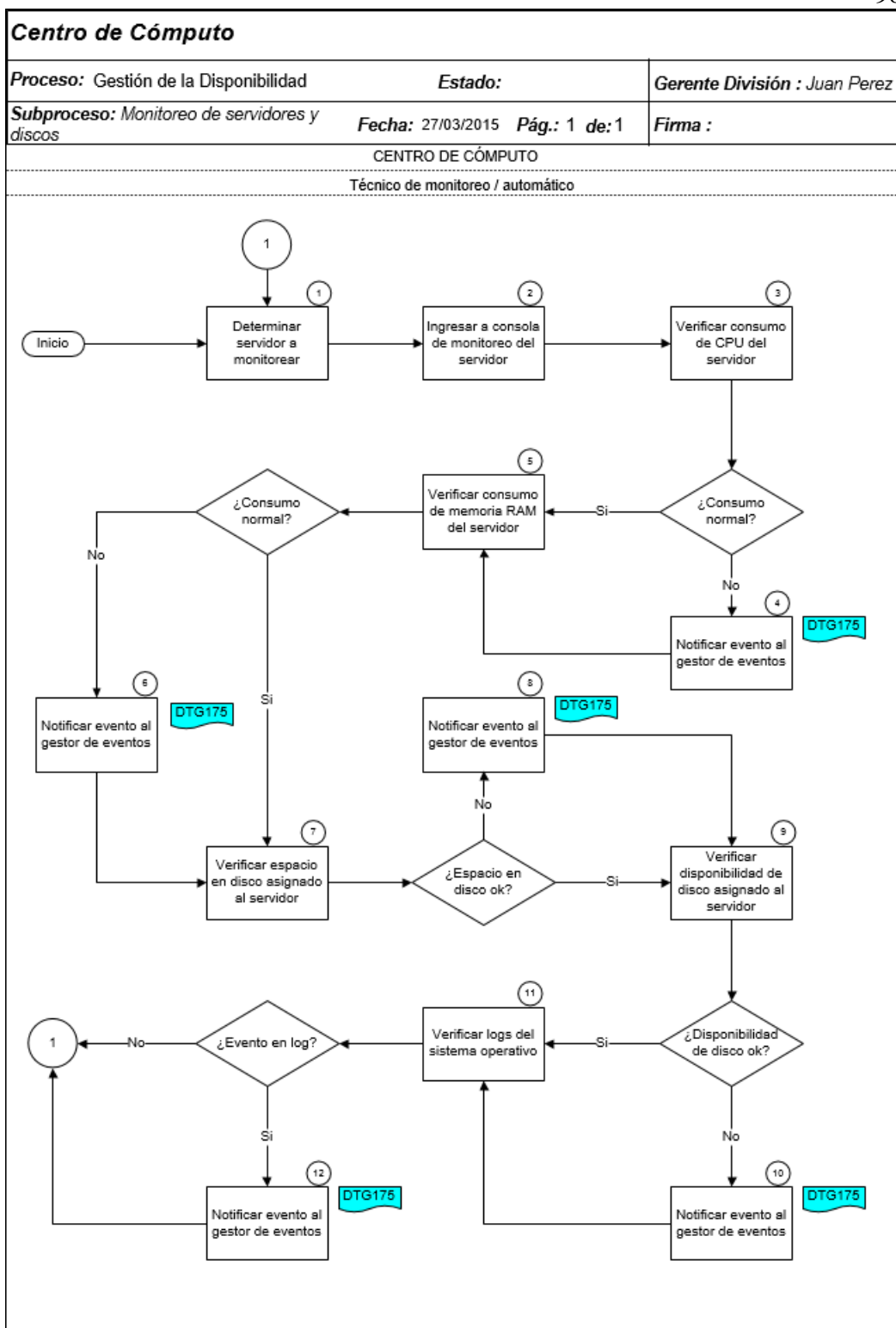


Figura 57. Proceso: Gestión de la disponibilidad  
Subproceso: Monitoreo de servidores y discos

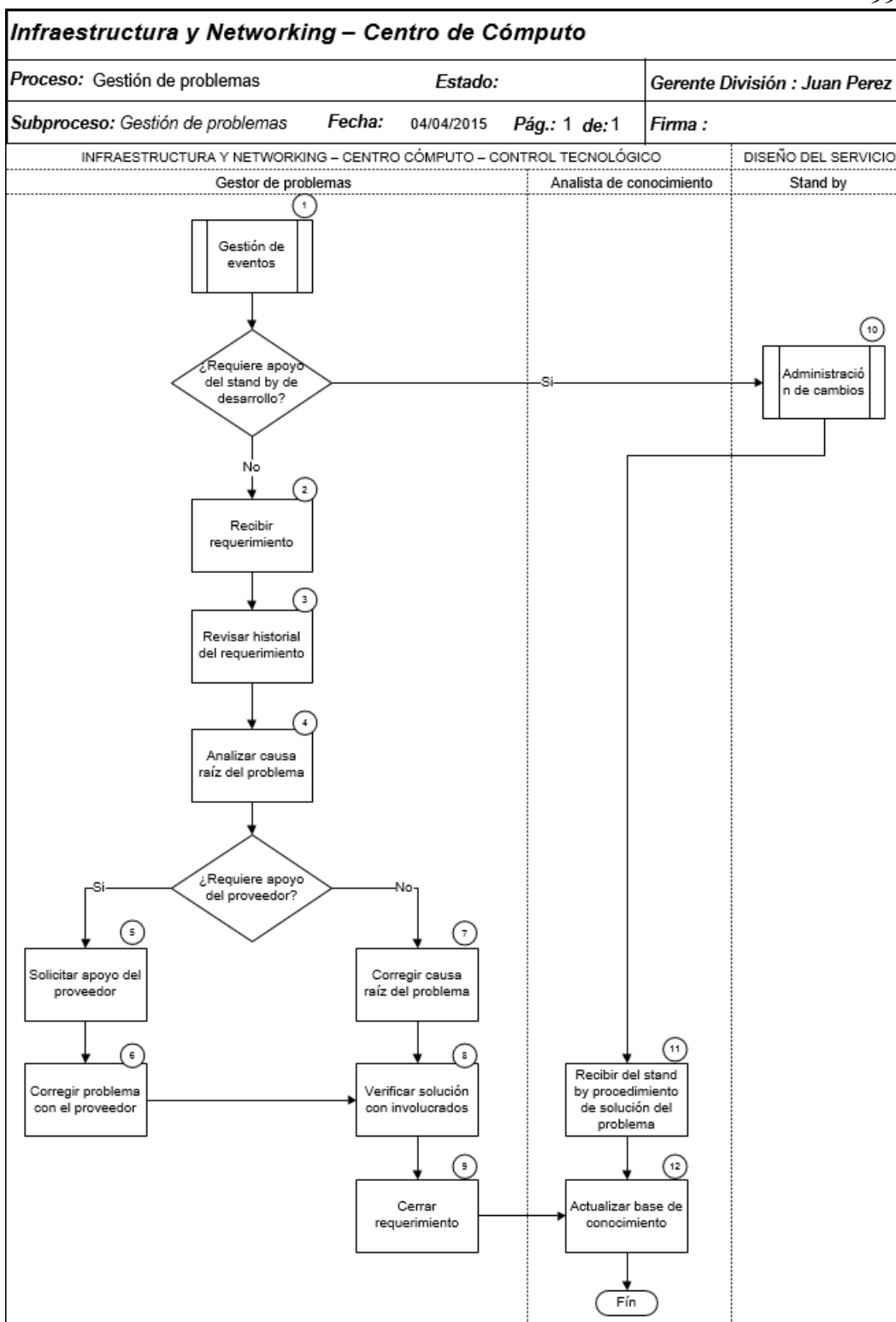


Figura 58. Proceso Gestión de problemas  
Subproceso Gestión de problemas

#### 4.3. Procesos detallados

##### 4.3.1. Proceso: Administración de datos

###### 4.3.1.1. Subproceso: Ciclo de vida de bases de datos

	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Crear Base de Datos	El Administrador de datos, recibe un requerimiento a través de la Herramienta de Service Desk para la Creación de la Base de Datos sea en SQL Server u Oracle, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.	Creación de DB SQL Server 2008 Creación de DB Oracle	Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk Consola Administración SQL Server, Oracle	Requerimiento recibido en Herramienta de Service Desk con la Solicitud de creación DB y formulario de control de cambios debidamente firmado.	DB Creada y cierre del requerimiento en la Herramienta de Service Desk, inventario actualizado	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls inventario bds SQL server al 20101123	Todas las solicitudes se deben canalizar a través del Service Desk	
2	Configurar Base de Datos	El Administrador de datos, recibe un requerimiento a través de la Herramienta de Service Desk para la Configuración de Base de Datos sea en SQL Server u Oracle, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.	AD_8_Creación de usuarios en SQL Server 2008 Políticas de gestión de BD CRM AD_20_Manual para crear un usuario de base de datos de solo lectura	Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk Consola Administración SQL Server, Oracle	Requerimiento recibido en Herramienta de Service Desk con la Solicitud de configuración de la DB y formulario de control de cambios debidamente firmado.	DB Configurada y cierre del requerimiento en la Herramienta de Service Desk.	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		
3	Activar Base de Datos	El Administrador de datos, recibe un requerimiento a través de la Herramienta de Service Desk para la Activación de Base de Datos solo en SQL Server, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.  SQL Server 2008  Primero abrir el SQL Server Management Studio Luego en el árbol buscar DataBases y hacer click derecho seleccionando Tasks -> Bring Online.		Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk Consola Administración SQL Server, Oracle	Requerimiento recibido en Herramienta de Service Desk con la Solicitud de Activación de la DB y formulario de control de cambios debidamente firmado.	DB Activa y cierre del requerimiento en la Herramienta de Service Desk. Actualizar Inventario de DB	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls inventario bds SQL server al 20101123		

CONTINÚA →

4	Administrar espacio en disco	<p>El Administrador de Base de Datos ingresa a la consola de Administración de Base de Datos (Oracle o SQL Server) en una forma periódica (2 veces a la semana) para analizar si necesitan liberación de espacio de las DB para de esta manera mantener siempre disponible espacio en los disco que utilizan las diferentes bases de datos.</p> <p>Var manuales adjuntos.</p> <p>Luego de terminar el requerimiento el Administrador de datos procede a actualizar el inventario de Base de Datos.</p>	<p>AD_9_12_Manual para borrar archive logs BD CRM producción</p> <p>AD_9_12_Manual para borrar archive logs +ASM prod CRM</p> <p>AD_9_12_Manual para borrar DMP antiguos serv desarrollo CRM</p> <p>AD_4_Manual (Procedimiento) PARA REDUCIR LAS BASES DE DATOS SQL SERVER</p>	Administrador de datos - Infraestructura y Networking	Consola Administración SQL Server, Oracle	Necesidad de Administrar el espacio en disco que ocupan las Bases de Datos. Inventario de Base de Datos.	El Analista de Base de Datos actualiza el Inventario de disco ocupado por las Bases de Datos			
5	Tunning de Base de Datos	<p>El Administrador de Base de Datos Ingresa a la consola de Administración de Base de Datos (Oracle o SQL Server) en una forma periódica (2 veces a la semana) para analizar si necesitan que se les realice un Tunning para mejorar el rendimiento de las mismas.</p> <p>Los afinamientos más comunes son:</p> <ul style="list-style-type: none"> <li>- Medición del rendimiento de la base de datos</li> <li>- Optimización del diseño físico de la base de datos</li> <li>- Optimización de Consultas</li> <li>- Refactorización de cursores en consultas</li> <li>- Optimización de la estrategia de indexación</li> </ul>	<p>AD_9_12_Manual como crear índices en tablas de CRM</p> <p>AD_9_12_Manual para copiar manualmente archive logs hacia bpd standby</p>	Administrador de datos - Infraestructura y Networking	Consola Administración SQL Server, Oracle	Necesidad de optimizar los tiempos de respuesta de las diferentes Bases de Datos. Inventario de Base de Datos	El Analista de datos entrega la DB afinada			
6	Desactivar Base de Datos	<p>El Administrador de datos, recibe un requerimiento a través de la Herramienta de Service Desk para la Desactivación de Base de Datos solo en SQL Server, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.</p> <p>SQL Server 2008 Primero abrir el SQL Server Management Studio Luego en el árbol buscar DataBases y hacer click derecho seleccionando Tasks -&gt; Take Offline.</p> <p>Luego de terminar el requerimiento el Administrador de datos procede a actualizar el inventario de Base de Datos.</p>		Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk  Consola Administración SQL Server, Oracle	Requerimiento recibido en Herramienta de Service Desk con la Solicitud de Desactivación de la DB y formulario de control de cambios debidamente firmado.	DB desconectada y cierre del requerimiento en la Herramienta de Service Desk, actualizar inventario.	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls  inventario bds SQL server al 20101123		

CONTINÚA →

7	Eliminar Base de Datos	El Administrador de datos, recibe un requerimiento a través de la Herramienta de Service Desk para la eliminación de la Base de Datos sea en SQL Server u Oracle, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.		Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk Consola Administración SQL Server, Oracle	Requerimiento recibido en Herramienta de Service Desk con la Solicitud de Eliminación de la DB y formulario de control de cambios debidamente firmado.	DB eliminada y cierre del requerimiento en la Herramienta de Service Desk, actualizar inventario.	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls inventario bds SQL server al 20101123		
---	------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	-------------------------------------------------------	--------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------	--	--

4.3.1.2. Subproceso: Soporte a bases de datos

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir requerimiento	El Jefe de servidores y administración de datos, recibe un requerimiento de Base de Datos sea en SQL Server u Oracle, a través de la Herramienta de Service Desk, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.		Jefe de servidores y administración de datos - Infraestructura y Networking	Herramienta de Service Desk	Requerimiento en Herramienta de Service Desk junto al formulario de control de cambios.	Requerimiento recibido mediante Herramienta de Service Desk	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls	Todos los requerimientos deben ser canalizados a través de la Herramienta de Service Desk.	
2	Verificar factibilidad junto con DBA	El Jefe de servidores y administración de datos junto al Administrador de datos, proceden al análisis de factibilidad, es decir analizan el impacto del requerimiento a ser ejecutado.  Dentro de dicho impacto se analiza: La afectación que pueden tener las tablas o DB en general, espacio en disco que pueden generar, afectación a los servicios que preste dicha base de datos y horario en el que se desea realizar la afectación.		Jefe de servidores y administración de datos - Infraestructura y Networking  Administrador de Datos - Infraestructura y Networking		Requerimiento asignado en Herramienta de Service Desk con formulario de control de cambios.	Dictamen de Factibilidad			
3	Notificar motivo a solicitante y cerrar requerimiento	En el caso de que el requerimiento no sea factible de ser cumplido, el Jefe de servidores y administración de datos emite un informe al usuario solicitante vía mail indicando por qué no pudo ser atendido el requerimiento y procede a cerrar el requerimiento en la Herramienta de Service Desk.		Jefe de servidores y administración de datos - Infraestructura y Networking		Dictamen de Factibilidad	Informe de factibilidad vía mail y requerimiento cerrado en Herramienta de Service Desk			
4	Asignar requerimiento a analista de datos	Si el requerimiento fue aprobado, el Jefe de servidores y administración de datos verifica la carga de los Analistas de Datos y procede a la re-asignación del requerimiento a través de la Herramienta de Service Desk, para que el mismo sea atendido.		Jefe de servidores y administración de datos - Infraestructura y Networking	Herramienta de Service Desk	Dictamen de Factibilidad	Asignación de requerimiento a Analista de Datos a través de la Herramienta de Service Desk	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		La Herramienta de Service Desk debe contar con un flujo de trabajo predefinido de manera que se pueda escalar el requerimiento.
5	Recibir requerimiento	El Administrador de Datos recibe el requerimiento debidamente aprobado a través de la Herramienta de Service Desk.		Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk	Requerimiento asignado en Herramienta de Service Desk con formulario de control de cambios.	Requerimiento recibido en Herramienta de Service Desk con formulario de control de cambios.			

CONTINÚA →

6	Crear tabla destino	En caso de que el requerimiento sea un movimiento de datos, el Administrador de Datos, recibe un script enviado por desarrollo el cual contiene los parámetros y campos para la Creación de la Tabla Destino y el nombre de la Base de Datos sea en SQL Server u Oracle, en la cual se va a realizar la afectación.		Administrador de datos - Infraestructura y Networking	Consola Administración SQL Server, Y para Oracle SQL Plus	Script enviado por desarrollo para crear la tabla y el nombre de la base de datos en el que se va a crear dicha tabla.	Tabla creada	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		
7	Definir campos a mover	El Administrador de Datos, recibe un script enviado por desarrollo el cual contiene los parámetros y campos que van a ser movidos y el nombre de la Base de Datos o tablas origen y destino, sea en SQL Server u Oracle, en la cual se va a realizar las afectación.		Administrador de datos - Infraestructura y Networking	Consola Administración SQL Server, Y para Oracle SQL Plus	Script enviado por desarrollo el cual contiene los campos a mover, la tabla y el nombre de la base de datos en el que se va a realizar la afectación.	Campos movidos	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		
8	Copiar datos a tabla destino	El Administrador de Datos, recibe un script enviado por desarrollo el cual contiene los parámetros y campos que van a ser copiados y el nombre de la Base de Datos o tablas origen y destino, sea en SQL Server u Oracle, en la cual se va a realizar las afectación.		Administrador de datos - Infraestructura y Networking	Consola Administración SQL Server, Y para Oracle SQL Plus	Script enviado por desarrollo el cual contiene los parámetros para copiar los datos, nombre de tabla o tablas y el nombre de la Base de Datos origen y destino en el que se va a realizar la afectación.	Datos copiados	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		
9	Notificar a solicitante	Una vez que se ha concluido el requerimiento se procede a notificar al solicitante vía mail o telefónicamente.		Administrador de datos - Infraestructura y Networking	Mail, Teléfono	Notificación de Requerimiento concluido	Requerimiento Concluido			
10	Verificar requerimiento con solicitante	Una vez que se ha concluido el requerimiento se procede a notificar al solicitante vía mail o telefónicamente para que realice la validación y verificación de la consistencia de los datos afectados.		Administrador de datos - Infraestructura y Networking	Mail, Teléfono	Notificación de Validación del Requerimiento	Requerimiento Validado			

CONTINÚA →

11	Actualizar campos solicitados	En caso de que el requerimiento sea una actualización de datos, el Administrador de Datos, recibe un script enviado por desarrollo el cual contiene los parámetros y campos que van a ser actualizados y el nombre de la Base de Datos o tablas a ser actualizados, sea en SQL Server u Oracle, en la cual se va a realizar las afectación.		Administrador de datos - Infraestructura y Networking	Consola Administración SQL Server, Y para Oracle SQL Plus	script enviado por desarrollo para Actualizar los campos el nombre de la tabla Base de Datos en el que se va a realizar la actualización	Campos actualizados.	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		
12	Notificar a solicitante	Una vez que se ha concluido el requerimiento se procede a notificar al solicitante vía mail o telefónicamente.		Administrador de datos - Infraestructura y Networking	Mail, Teléfono	Notificación de Requerimiento concluido	Requerimiento Concluido			
13	Verificar requerimiento con solicitante	Una vez que se ha concluido el requerimiento se procede a notificar al solicitante vía mail o telefónicamente para que realice la validación y verificación de la consistencia de los datos afectados.		Administrador de datos - Infraestructura y Networking	Mail, Teléfono	Notificación de Validación del Requerimiento	Requerimiento Validado			
14	Cerrar requerimiento	Una vez que se ha concluido y verificado el requerimiento se procede a cerrar el mismo en la Herramienta de Service Desk		Administrador de datos - Infraestructura y Networking	Herramienta de Service Desk	Requerimiento Concluido	Requerimiento cerrado en Herramienta de Service Desk			



4.3.2. Proceso: Administración de la configuración

4.3.2.1. Subproceso: Configuración de hardware

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir equipo del proveedor	Si el equipo es nuevo, en Networking se reciben los servidores o partes de los mismos, en Telefonía y Comunicaciones se reciben equipos y partes, verificando que todo lo que el proveedor está entregando sea lo que se encuentra descrito en la factura entregada por el mismo.  Si el equipo o parte corresponde a la plataforma AS400 la recepción lo realiza el Centro de Computo		Administrador de servidores Infraestructura y Networking Técnico de procesamiento Centro de Computo		Factura de compra de equipos, servidores o partes emitida por el proveedor	Equipo Recibidos y registrados en los respectivos archivos de Excel donde se lleva el inventario	Registro en inventario de servidores en Excel  Registro en inventario de PC's en Excel	Los requerimientos de configuración de hardware deben ser canalizados a través de Service Desk	Se recomienda el uso de una herramienta de gestión de activos para formalizar el registro de activos
		Si el equipo es nuevo, en el caso de PC' s el departamento de Administrativa hace la entrega de los equipos al área de Service Desk y coloca un label con los seriales respectivos en el CPU, Monitor, Teclado y Mouse respectivamente.		Analista de segunda línea de Service Desk		Listado de Pc's, monitores, teclados y mouse con sus respectivos números seriales		Los requerimientos de servidores son ejecutados por el área de Infraestructura y Networking. Los requerimientos de PCs son ejecutados por el área de Service Desk.		
2	Acompañar a proveedor durante la configuración	Para el caso de servidores y AS400, se acompaña al proveedor todo el tiempo que dura la configuración de los equipos para adquirir conocimientos sobre el tema y facilitar al proveedor el ambiente requerido para la configuración de los mismos.		Administrador de servidores Infraestructura y Networking Técnico de procesamiento Centro de Computo		Equipo entregado por el proveedor	El proveedor entrega el Equipo Configurado			
3	Verificar configuración	Cuando se configura con el proveedor se realizan conjuntamente las pruebas necesarias para certificar que el equipo se encuentre funcional y configurado en su totalidad y se emite un reporte al supervisor de Infraestructura y Networking indicando el estado del mismo. Cuando no se necesita del apoyo del proveedor, dicha verificación de la configuración se hace internamente y se emite un reporte de configuración.		Administrador de servidores Infraestructura y Networking Técnico de procesamiento Centro de Computo		El proveedor entrega el Equipo Configurado	Configuración verificada. Informe del estado de configuración del servidor, equipo o parte.	Reporte Equipo Funcional		
4	Contactar al proveedor	Cuando el equipo no es nuevo y necesita apoyo del proveedor se le contacta al mismo vía telefónica o vía email para solicitar la asistencia y el soporte requerido.		Administrador de servidores Infraestructura y Networking Técnico de procesamiento Centro de Computo		Necesidad de apoyo del proveedor	Confirmación vía mail o telefónica del proveedor para el respectivo apoyo solicitado			

CONTINÚA →

5	Configurar red	En el caso de PCs, en las propiedades del adaptador de RED se procede a fijar la IP estática de acuerdo a la VLAN a la que pertenezca y los DNS's		Analista de segunda línea de Service Desk		Se recibe el equipo para fijar la IP y DNS respectivos	Se entrega el equipo con la tarjeta de Red Configurada, la IP asignada y la MAC ADDRESS de la misma		Todo PC asignado a los funcionarios debe tener asignada y registrada una dirección IP fija, En caso de mover físicamente el PC, se debe notificar al área de Infraestructura y Networking para que se realicen las respectivas configuraciones.	
6	Configurar tarjeta de video	En el caso de PCs, se procede a la instalación de los respectivos drivers de video que el fabricante proporcione para su óptimo funcionamiento.		Analista de segunda línea de Service Desk		Se recibe el equipo a configurar la tarjeta de video	Se entrega el equipo configurados los drivers de video			
7	Configurar periféricos	En el caso de PCs, se procede a verificar la configuración y buen funcionamiento de los diferentes periféricos que utilizan las mismas (Monitor, teclado y mouse).		Analista de segunda línea de Service Desk		se reciben los periféricos (Monitor, teclado y mouse) y el equipo para configurarlos	Se entrega el equipo con los respectivos Periféricos Configurados			
8	Configuración de recursos de hardware (AS400)	En la plataforma AS400, de acuerdo a las necesidades de procesamiento y uso de recursos de los servidores, se asigna recursos de memoria, procesador y disco. Para la memoria y procesador se tiene la posibilidad de mover estos recursos entre servidores (particiones) , dependiendo de las necesidades de procesamiento		Técnico de procesamiento Centro de Computo	AS400	Necesidades de procesamiento	Movimiento de recursos de hardware entre particiones del equipo AS400			

4.3.2.2. Subproceso: Configuración de sistema operativo y software

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir requerimiento	El Jefe de servidores y administración de datos Infraestructura y Networking (servidores), el analista de segunda línea de Service Desk (PCs) o el Jefe de procesamiento del Centro de Cómputo (AS400) recibe un requerimiento de configuración de software a través de la herramienta de Service Desk indicando el equipo a configurar y los aplicativos a instalar.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Solicitud Requerimiento en herramienta de Service Desk	Requerimiento recibido en herramienta de Service Desk	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls	Todas las solicitudes de configuración deben venir a través de la herramienta de Service Desk	
2	Verificar factibilidad	Se procede al análisis de factibilidad, es decir analiza la disponibilidad de licencias del producto a instalar, si cumple con los estándares de la empresa y si existe la disponibilidad de un equipo para realizar dicha instalación, para de esta manera cumplir el respectivo requerimiento.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Requerimiento recibido en herramienta de Service Desk	Dictamen de Factibilidad		Solo se permite la instalación de los aplicativos validados por la Gerencia de TI. Ver listado de aplicativos permitidos.	
3	Notificar motivo a solicitante, cierre del requerimiento.	Si no es factible el requerimiento se emite un informe vía email al usuario del porque no pudo ser atendido el requerimiento y se procede al cierre del requerimiento a través de la herramienta de Service Desk.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Dictamen de Factibilidad	informe de factibilidad y cierre del requerimiento en la herramienta de Service Desk		Los requerimientos de servidores son ejecutados por el área de Infraestructura y Networking. Los requerimientos de PCs son ejecutados por el área de Service Desk. Los requerimientos de AS400 son ejecutados por el área de Centro de Cómputo.	

CONTINÚA →

4	Asignar requerimiento a técnico	Si el requerimiento fue aprobado, el Jefe de servidores y administración de datos Infraestructura y Networking verifica la carga de los Técnicos y procede a re-asignar el requerimiento a través de la herramienta de Service Desk a un Administrador de servidores para que el mismo sea atendido. En el caso de PCs, el requerimiento permanece en el analista de segunda línea de Service Desk. En el caso de AS400 el requerimiento permanece en el Jefe de procesamiento quien se encargara de contactar al proveedor.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Asignación de requerimiento mediante la Herramienta de Service Desk	Requerimiento asignado mediante herramienta			
5	Determinar sistema operativo a instalar	Si el requerimiento fue la instalación de un Sistema Operativo, se determina el Sistema Operativo que requiere ser instalado según el equipo y la solicitud. Con esto se procede a la obtención de los respectivos instaladores. Para los casos en donde exista un contrato con proveedor o se requiere su apoyo, se procede a contactar al proveedor para que realice el requerimiento solicitado.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Requerimiento asignado a técnico en herramienta de Service Desk	Sistema operativo a instalar y obtenido de instaladores del Sistema Operativo a instalar			
6	Instalar sistema operativo	En la plataforma AS400, la instalación de sistema operativo la realiza el proveedor del equipo, con el acompañamiento del personal del Centro de Computo		Jefe de procesamiento de Centro de Cómputo		Necesidad de instalación o actualización del sistema operativo	Servidor con sistema operativo instalado			
		Una vez obtenidos los instaladores se procede a la instalación del respectivo Sistema operativo (LINUX, WINDOWS, AIX)	AC_6_Manual Instalación RedHat 6 AC_2_Instalacion Windows Server 2008	Técnico de servidores Infraestructura y Networking Analista de segunda línea de Service Desk	Software del Sistema Operativo a instalar y manual de instalación del mismo	Equipo con Sistema Operativo Instalado	El sistema operativo debe estar instalado en una partición distinta a la de los programas			
7	Instalar componentes base	Se procede a la instalación de los componentes base de acuerdo al sistema operativo instalado.  Windows: Framework, Herramientas administrativas del servidor.  Linux: Cliente telnet		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Equipo con Sistema Operativo Instalado	Componentes base instaladas según Sistema Operativo y manual de instalación del mismo.			
8	Configurar puertos básicos	Se procede a la configuración de los puertos de acuerdo al requerimiento especificado. Windows: puerto 3389 para el escritorio remoto. Linux y AIX: SSH		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Configurar puertos básicos según Sistema Operativo.	Puertos Configurados según Sistema Operativo			

CONTINÚA →

9	Instalar antivirus (Windows)	Se procede a instalar el Antivirus solo en sistema operativo es Windows		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Equipo configurado y si es Windows se debe instalar antivirus	Equipo con Antivirus Instalado		Todos los Servidores o PC's deben tener instalado el antivirus.	
10	Cerrar requerimiento	Una vez ejecutado el requerimiento, se procede a cerrar el requerimiento en la herramienta de Service Desk.		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Equipo configurado y listo para ser usado	Cierre del requerimiento, entrega del equipo preparado al usuario solicitante			
11	Determinar aplicativo a instalar	Si en el requerimiento se especifica que es necesario instalar algún aplicativo en particular se procede a buscar los instaladores necesarios para cumplir con el requerimiento.		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk	Herramienta de Service Desk	Requerimiento con el aplicativo a instalar mediante la Herramienta de Service Desk	Aplicativo a instalar identificado y obtención de los instaladores del mismo.	Ver pestaña de Aplicativos permitidos en servidores	Todo aplicativo adicional al Sistema Operativo debe ser instalado en una partición diferente a la del Sistema Operativo	
12	Instalar aplicativo	En el caso de la plataforma AS400, se realiza la instalación de los aplicativos permitidos (ver lista de aplicativos permitidos), para lo cual es necesario contar con el soporte del proveedor del software y el análisis de los prerrequisitos antes de la instalación		Jefe de procesamiento de Centro de Cómputo	AS400 Windows Aix	Necesidad de instalación o actualización de aplicativos plataforma AS400	Aplicativo instalado o actualizado			
		En el caso servidores y PCs, se procede a la instalación del respectivo aplicativo según requerimiento (ver pestaña de aplicativos permitidos en servidores).		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Aplicativo a instalar identificado y obtención de los instaladores del mismo.	Equipo con aplicativo Instalado	Ver pestaña de Aplicativos permitidos en servidores		
13	Configurar aplicación y componentes según solicitud	En el equipo que se instaló el aplicativo se procede a configurar el aplicativo y los componentes solicitados en el requerimiento.		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Equipo con aplicativo Instalado	Equipo con Aplicativo Configurado	Ver pestaña de Aplicativos permitidos en servidores		
14	Gestión de accesos	Control Tecnológico asignara los respectivos permisos de acceso al equipo como a los diferentes aplicativos instalados en el mismo		Analista de accesos de Control Tecnológico		Solicitud de acceso según aplicativo a instalar	Acceso habilitado en aplicativo solicitado			

CONTINÚA →

15	Verificar configuración con el usuario	Se procede a realizar las respectivas validaciones del aplicativo y accesos al mismo.		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Equipo, Aplicativo y permisos Configurados	Check de funcionamiento de Aplicativo Verificado			
----	----------------------------------------	---------------------------------------------------------------------------------------	--	--------------------------------------------------------------------------------------------------------------------------------------------------------	--	--------------------------------------------	--------------------------------------------------	--	--	--

4.3.2.3. Subproceso: Mantenimiento de redes LAN

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Identificar tipo de mantenimiento	Identificar el tipo de mantenimiento que se va a realizar en la red LAN (Disponibilidad de puntos de red, Configuración de VLAN's, Cableado estructurado).		Administrador de redes Infraestructura y Networking		Necesidad de mantenimiento en red LAN	Tipo de mantenimiento de red LAN identificado			
2	Recibir requerimiento	Si el tipo de mantenimiento es sobre disponibilidad de puntos de red se debe recibir un requerimiento a través de la herramienta de Service Desk indicando la ubicación del punto.		Administrador de redes Infraestructura y Networking	Herramienta de Service Desk	Requerimiento en herramienta de Service Desk	Requerimiento recibido en herramienta de Service Desk			
3	Verificar ubicación y disponibilidad de punto	Se procede a verificar la existencia de disponibilidad de punto tanto en los switch como físicamente en el puesto a habilitar el mismo.		Administrador de redes Infraestructura y Networking		Requerimiento recibido en herramienta de Service Desk	Verificación de la disponibilidad y ubicación del punto de red solicitado			
4	Habilitar punto	Se procede a la activación y permisos del punto de red en los diferentes routers, switch. Para que quede completamente funcional el mismo.		Administrador de redes Infraestructura y Networking		Verificación de la disponibilidad y ubicación del punto de red solicitado	Punto de red habilitado			
5	Notificar al usuario y cerrar requerimiento	Una vez habilitado y comprobado el funcionamiento del punto de red, se procede a notificar al usuario que el punto de red ha sido activado y se cierra el requerimiento.		Administrador de redes Infraestructura y Networking	Herramienta de Service Desk	Punto de red habilitado	Requerimiento cerrado en la herramienta de Service Desk			
6	Notificar motivo a supervisor	En caso de encontrar un inconveniente se procede a notificar al supervisor de Networking el porque no se puede realizar dicho requerimiento y se escala el requerimiento a través de la herramienta de Service Desk.		Administrador de redes Infraestructura y Networking	Herramienta de Service Desk	Verificación de la disponibilidad y ubicación del punto de red solicitado	Requerimiento escalado a Supervisor a través de la herramienta de Service Desk			La herramienta de Service Desk debe ser capaz de escalar requerimientos según flujos de trabajo predefinidos.
7	Analizar factibilidad	El jefe de redes y comunicaciones revisa el informe y analiza la factibilidad de proceder con el requerimiento. Analiza costos de la implementación, equipos necesarios y tiempo de respuesta al requerimiento.		Jefe de redes y comunicaciones Infraestructura y Networking		Requerimiento escalado a Supervisor a través de la herramienta de Service Desk	Dictamen de factibilidad			
8	Notificar motivo a solicitante	Se notifica al solicitante que no se puede atender el requerimiento indicando los motivos asociados y se procede a cerrar el requerimiento en la herramienta de Service Desk.		Jefe de redes y comunicaciones Infraestructura y Networking		Dictamen de factibilidad	Notificación al usuario los motivos de rechazo de la solicitud y cerrar el requerimiento.			

CONTINÚA →

9	Solicitar instalación física	En caso de requerir una instalación física, el jefe de redes y comunicaciones de Infraestructura y Networking, mediante mail con orden de instalación física, solicita al área Administrativa que se realice la instalación física del punto de red.		Jefe de redes y comunicaciones Infraestructura y Networking		Dictamen de factibilidad	Orden de instalación de punto nuevo al Área de Administrativo	REQUERIMIENTO DE COMPRA DE MATERIALES Y EQUIPOS		
10	Notificar a técnico para proceder con requerimiento.	Una vez ejecutada la solicitud de compra de equipos o de instalación física por parte del área de administrativo, el jefe de redes y comunicaciones reasigna el requerimiento al técnico para que continúe con la habilitación del punto de red solicitado.		Jefe de redes y comunicaciones Infraestructura y Networking		Orden de compra ejecutada por el área Administrativa	Requerimiento reasignado al técnico en la herramienta de Service Desk			
11	Solicitar orden compra de equipos	En caso de requerir la compra de equipos, el jefe de redes y comunicaciones de Infraestructura y Networking, mediante la respectiva orden de compra solicita al área Administrativa que se realice la compra de los equipos requeridos.		Jefe de redes y comunicaciones Infraestructura y Networking		Dictamen de factibilidad	Orden de compra de equipos emitida al Área Administrativa	REQUERIMIENTO DE COMPRA DE MATERIALES Y EQUIPOS		
12	Identificar tipo de VLAN requerida	Para determinar el tipo de VLAN a crear se debe identificar si va a ser vista por las otras VLAN's o no.  VLAN's pueden ser creadas de 2 tipos: Vlan's Ruteables, que son las que pueden ser vistas por las otras Vlan's existentes, y Vlan's no Ruteables las cuales no pueden ser vistas por las demás Vlan's.		Administrador de redes Infraestructura y Networking		Tipo de mantenimiento de red LAN identificado	VLAN a crear identificada			
13	Crear VLAN	Una vez identificada la VLAN que se va a crear, se procede con la respectiva creación:  Se ingresa vía Putty a la configuración de los equipos Cisco en el cual se procede a la creación de la VLAN, especificando los siguientes datos: número de VLAN, nombre de VLAN, tipo de VLAN, se procede a activar la misma y se activan los permisos de accesibilidad dependiendo si es una VLAN Ruteable o no ruteable.		Administrador de redes Infraestructura y Networking		VLAN a crear identificada	VLAN creada según solicitud junto con Informe VLAN creada.			
14	Registrar VLAN en mapa de direcciones IP	Una vez creada y verificada la VLAN, se procede al Registro en archivo de mapa de IP's, en el cual se registran: Número de Vlan y nombre de la misma, fecha y motivo de creación.		Administrador de redes Infraestructura y Networking	Herramienta de Service Desk	VLAN creada	Cierre de requerimiento y notificación de VLAN creada	Inventario Vlan		Se debe adicionar una columna con la fecha de creación y el motivo de su creación al mapa de direcciones IP para las VLANS creadas

CONTINÚA →



15	Revisar físicamente cableado estructurado	La revisión física del cableado estructurado, se la realiza una vez por año, en la cual se va recorriendo todo el cableado estructurado componente por componente. Y que cumpla el protocolo de categoría 5, 6A o 7A según la categoría que se encuentre instalada.		Administrador de redes Infraestructura y Networking		Tipo de mantenimiento de red LAN identificado	Cableado estructurado revisado según protocolo de red categoría 5, 6A o 7A según la categoría que se encuentre instalada.			
16	Identificar problemas	Se pueden identificar problemas tales como: cables pelados, patch cord deteriorados, cajetines de red en mal estado, hilos de red desconectados, entre los más comunes.		Administrador de redes Infraestructura y Networking		Cableado estructurado revisado según protocolo de red categoría 5, 6A o 7A según la categoría que se encuentre instalada.	Problemas en el cableado estructurado Identificados			
17	Corregir problemas	Una vez que fueron identificados dichos problemas en el Cableado Estructurado, se procede a la corrección de los problemas encontrados, en caso de no existir en stock los componentes necesarios se llenan las órdenes de compra respectiva de materiales y se la pasa al Área Administrativa para que adquieran los componentes y se procede a la corrección de dichos problemas.		Administrador de redes Infraestructura y Networking		Problemas en el cableado estructurado Identificados	Corrección de errores en el Cableado Estructurado			

4.3.2.4. Subproceso: Mantenimiento de redes WAN

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir requerimiento de GST	El Sub Gerente de Infraestructura y Networking recibe la solicitud de requerimiento de nueva WAN		Sub Gerente de Infraestructura y Networking		Requerimiento de nueva WAN	Revisión requerimiento nueva WAN			
2	Analizar factibilidad	El Sub Gerente de Infraestructura y Networking analiza la factibilidad del Requerimiento, es decir analiza la disponibilidad de equipos y tiempo de implementación de la misma.		Sub Gerente de Infraestructura y Networking		Revisión requerimiento nueva WAN	Dictamen de factibilidad			
3	Realizar diseño	El administrador de redes de Infraestructura y Networking junto al proveedor realiza el diseño de la nueva WAN requerida, realizan el diseño con equipos propios o equipos del proveedor.		Administrador de redes Infraestructura y Networking - Proveedor		Dictamen de factibilidad	Diseño de WAN			
4	Realizar cotización del diseño	Se envía al proveedor el documento con el diseño de la nueva red WAN para que este realice la cotización de la misma		Proveedor		Diseño de WAN	Solicitud de Cotización nueva red WAN			
5	Aprobar cotización	El Sub Gerente de Infraestructura y Networking recibe la cotización de la nueva red WAN enviada por el proveedor y realiza la Aprobación de la misma.		Sub Gerente de Infraestructura y Networking		Cotización red WAN enviada por el proveedor	Cotización nueva red WAN aprobada			
6	Implantar diseño	Una vez aprobada la cotización para la nueva red WAN solicitada, se procede implementación de la misma		Administrador de redes Infraestructura y Networking - Proveedor		Cotización WAN aprobada	Informe de la Implementación red WAN			
7	Verificar implantación	Una vez implementada la nueva red WAN el administrador de redes de Infraestructura y Networking junto al Proveedor procede a realizar las diferentes pruebas de verificación de conexión en la red WAN.		Administrador de redes Infraestructura y Networking - Proveedor		Informe de la Implementación red WAN	Certificación de la implementación			
8	Asignar requerimiento a técnico	Una vez pasadas las pruebas de funcionamiento de la red WAN instalada y verificada, se recibe un requerimiento a través de la herramienta de Service Desk indicando que se le ha asignado un requerimiento.		Sub Gerente de Infraestructura y Networking	Herramienta de Service Desk	Requerimiento recibido en herramienta de Service Desk	Requerimiento asignado en herramienta de Service Desk			
9	Establecer niveles de seguridad	Una vez asignado el respectivo requerimiento se procede con la Configuración y aseguramiento perimetral de seguridad a la red WAN instalada, es decir se proceden a dar los permisos en los diferentes componentes de la red LAN hacia las diferentes aplicaciones para la cual fue solicitada la red WAN.		Administrador de redes Infraestructura y Networking		Requerimiento asignado en herramienta de Service Desk	Seguridades perimetrales de la red WAN establecidas.			

CONTINÚA →

10	Cerrar requerimiento	Una vez instalada y configurada toda la red WAN nueva se procede a la entrega de un informe al Sub Gerente de Infraestructura y Networking en el cual se especifican los permisos solicitados hacia las aplicaciones que fueron especificadas en el requerimiento de la creación de la red WAN y el cierre de requerimiento asignado.		Administrador de redes Infraestructura y Networking	Herramienta de Service Desk	Requerimiento asignado en herramienta de Service Desk	Informe del estado de la red WAN dirigido al Sub Gerente de Infraestructura y Networking, cierre requerimiento.	Inventario Equipos Cisco Inventario Enlaces Inventario Nat		
----	----------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	-----------------------------------------------------------	--------------------------------	----------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------	--	--

4.3.3. Proceso: Administración de la mesa de servicio y los incidentes

4.3.3.1. Subproceso: Soporte a usuarios en Service Desk

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir requerimiento vía mail o telefónico	Los analistas de primera línea de Service Desk reciben los requerimientos de 2 maneras. Sea vía telefónica mediante la ext. 4911. O vía email a través del correo: helpdesk_tecnologia@Dinersclub.com.ec		Analista de primera línea de Service Desk	Teléfono email	Requerimiento vía telefónica o vía email	Requerimiento Recibido			
2	Abrir registro en herramienta con información del requerimiento	El Analista de primera línea de Service Desk, procede a abrir la Consola de la Herramienta de Service Desk, Escoge nueva Incidencia Selecciona la Empresa Selecciona el Cliente (usuario que está solicitando el requerimiento) Llena el campo notas con una explicación detallada del requerimiento Escoge el impacto, la prioridad, tipo de incidencia y la fuente reportada, el Grupo asignado (Quito o GYE)		Analista de primera línea de Service Desk	Herramienta de Service Desk	Requerimiento Recibido	Requerimiento Abierto en Herramienta de Service Desk			
3	Categorizar el requerimiento de acuerdo a tipificación	En la misma Consola de la Herramienta de Service Desk al momento de crear el requerimiento se procede a poner la Categorización del requerimiento de acuerdo a la tipificación existente y escogiendo la que más se apegue a la naturaleza del requerimiento.  Ver pestaña de Tipificación de requerimientos.	Ver pestaña de tipificación de requerimientos.	Analista de primera línea de Service Desk	Herramienta de Service Desk	Requerimiento Abierto en Herramienta de Service Desk	Requerimiento Categorizado en Herramienta de Service Desk			
4	Generar número de requerimiento y notificar al usuario	Una vez que se han llenado todas las especificaciones necesarias para la generación del requerimiento se genera un número de requerimiento en forma automática y al guardar el requerimiento instantáneamente se dispara un email al usuario indicándole el número de requerimiento y el técnico asignado para resolver el mismo. En caso de tener un flujo predefinido, la herramienta asigna el solucionador automáticamente y envía un email indicándole que se le ha asignado un nuevo requerimiento.		Analista de primera línea de Service Desk	Herramienta de Service Desk	Requerimiento Categorizado en Herramienta de Service Desk	Requerimiento generado en Herramienta de Service Desk  Email enviado al usuario con el número de requerimiento y nombre de Técnico asignado para resolver el requerimiento.			

CONTINÚA →

5	Revisar base de conocimiento en la herramienta	El analista de primera línea procede a revisar en la base de conocimiento de Service Desk para ver si existe un procedimiento de solución del requerimiento.		Analista de primera línea de Service Desk	Base de conocimiento de la herramienta de Service Desk	Requerimiento asignado en Herramienta de Service Desk	Base de conocimientos Revisada			Se debe ingresar toda la información de los requerimientos ya resueltos a la Herramienta de Service Desk para que sea más fácil de consultar y resolver los requerimientos en una forma más eficiente.
6	Analizar requerimiento	Una vez revisada la base de conocimientos el Analista de primera línea de Service Desk procede a analizar si puede resolver el requerimiento teniendo en cuenta los tipos de requerimientos que él está autorizado a resolver.		Analista de primera línea de Service Desk		Requerimiento asignado en Herramienta de Service Desk	Requerimiento Analizado		Toda información de resolución o intento de resolución realizada por cualquiera de los entes solucionadores debe ser registrada en la herramienta de Service Desk con el ánimo de dejar trazabilidad del procedimiento de resolución para futura consulta.	
7	Resolver requerimiento	Una vez que el Analista de primera línea de Service Desk haya revisado la base de conocimiento y analizado el requerimiento en caso de poder solucionarlo procede con la solución del requerimiento. Toda la información de resolución debe ser registrada en la herramienta de Service Desk.  Ver pestaña de Tipificación de requerimientos.	Ver pestaña de Tipificación de requerimientos.	Analista de primera línea de Service Desk		Requerimiento asignado en Herramienta de Service Desk	Requerimiento resuelto.			
8	Cerrar requerimiento y notificar al usuario	Una vez resuelto el incidente, se procede a cerrar el requerimiento asignado en la herramienta de Service Desk. La Herramienta de Service Desk dispara un email automático al usuario que solicitó el requerimiento, indicándole al mismo que el requerimiento ha sido atendido.		Analista de primera línea de Service Desk	Herramienta de Service Desk	Requerimiento Resuelto	Requerimiento cerrado en Herramienta de Service Desk			

CONTINÚA →

9	Escalar el requerimiento en la herramienta	Si el Analista de primera línea de Service Desk no puede solucionar el requerimiento procede a ingresar a la herramienta de Service Desk y escalar el requerimiento al Analista de segunda línea de Service Desk con menor carga de requerimientos para que este proceda a la solución del mismo.		Analista de primera línea de Service Desk	Herramienta de Service Desk	Requerimiento Analizado	Requerimiento Re - asignado a Técnico 2 de Service Desk			
10	Recibir requerimiento en la herramienta	Una vez que se ha escalado el requerimiento el Analista de segunda línea de Service Desk recibe un correo con el número de requerimiento asignado. Procede a ingresar a la Herramienta de Service Desk. Escoge la opción de Consola de Gestión de Incidencias, en la cual se le despliegan todos los requerimientos asignados. Escoge el número de incidente y procede a revisarlo.		Analista de segunda línea de Service Desk	Herramienta de Service Desk	Requerimiento asignado en Herramienta de Service Desk	Requerimiento recibido en Herramienta de Service Desk			
11	Revisar base de conocimiento en la herramienta	El Analista de segunda línea procede a revisar en la base de conocimiento de Service Desk para ver si existe un procedimiento de solución del requerimiento.		Analista de segunda línea de Service Desk	Herramienta de Service Desk	Requerimiento recibido en Herramienta de Service Desk	Base de conocimientos Revisada			
12	Analizar requerimiento	Una vez revisada la base de conocimientos el Analista de segunda línea de Service Desk procede a analizar si puede resolver el requerimiento teniendo en cuenta los tipos de requerimientos que él está autorizado a resolver.		Analista de segunda línea de Service Desk	Herramienta de Service Desk	Base de conocimientos Revisada	Requerimiento Analizado			
13	Escalar el requerimiento a área solucionadora	Si el Analista de segunda línea de Service Desk no puede solucionar el requerimiento procede a ingresar a la herramienta de Service Desk y escala el requerimiento al área solucionadora respectiva.		Analista de segunda línea de Service Desk	Herramienta de Service Desk	Requerimiento Analizado	Requerimiento escalado al Área Solucionadora respectiva			
14	Resolver requerimiento	En caso de encontrar un procedimiento de solución para el requerimiento solicitado, el Analista de segunda línea procede a seguir dicho procedimiento y resolver el requerimiento. Toda la información de resolución debe ser registrada en la herramienta de Service Desk.		Analista de segunda línea de Service Desk		Requerimiento Analizado	Requerimiento resuelto.			
15	Cerrar requerimiento y notificar al usuario	Una vez resuelto el incidente, se procede a cerrar el requerimiento asignado en la herramienta de Service Desk. La Herramienta de Service Desk dispara un email automático al usuario que solicitó el requerimiento, indicándole al mismo que el requerimiento ha sido atendido.		Analista de segunda línea de Service Desk	Herramienta de Service Desk	Requerimiento Resuelto	Requerimiento cerrado en Herramienta de Service Desk			

4.3.4. Proceso: Administración de operaciones

4.3.4.1. Subproceso: Procesamiento de transacciones y disponibilidad de la información

#	Actividad	Descripción	Manuales de Detalle	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos
1	Ejecuta cierre de operaciones desde el Autorizador hacia el Gestor	Desde el menú del operador en el equipo CAO se ejecuta la opción de cierre de operaciones al finalizar se despliega el número de registros que se van a transmitir al equipo Gestor.  En el equipo Gestor se ejecuta la opción de cierre la cual recibe los archivos transmitidos en el paso anterior, se compara el número de registros y se registra en la bitácora		Técnico de procesamiento Centro de Computo	AS400	Actividad planificada en bitácora	Cierre de operaciones ejecutado	El proceso se ejecuta en los horarios definidos	
2	Ejecuta procesos de Avances en Efectivo en ATM	Se debe esperar que los archivos con información de ATM sean transmitidos por el banco, a continuación para la afectación en el sistema se ejecuta la opción desde el menú del operador	Procedimiento de avances en efectivo ATM	Técnico de procesamiento Centro de Computo	AS400	Cierre de operaciones ejecutado	Proceso de avances en ATM ejecutado	Se debe esperar que el banco transmita los archivos	
3	Notifica vía correo la finalización del proceso de avances	Notifica al área de facturación para que realice el traslado de la boleta generada	Procedimiento de avances en efectivo ATM	Técnico de procesamiento Centro de Computo	Correo	Proceso de avances en ATM ejecutado	Notificación al departamento de Facturación		
4	Ejecuta traslado de boleta	El departamento de facturación ejecuta el traslado de boleta para la afectación en el sistema de los movimientos de avances en efectivo por ATM		Facturación	AS400	Notificación al departamento de Facturación	Movimientos de ATM actualizados en el sistema		
5	Notifica vía correo la finalización de los procesos	El departamento de facturación ejecuta sus procesos internos como la afectación de pagos, ajustes y capturas los cuales van a procesarse en el sistema con la ejecución del cierre batch		Facturación	AS400	Movimientos ingresados	Finalización de los procesos del departamento de Facturación		
6	Realiza la carga de los spools al sistema de Gestión Documental	Los reportes generados se cargan al sistema de gestión documental y se registra el número de páginas generadas en la bitácora de procesos	Procedimiento de avances en efectivo ATM	Técnico de procesamiento Centro de Computo	AS400	Proceso de avances en ATM ejecutado	Reportes cargados al sistema		
7	Recibe notificación para el inicio de los procesos batch	Reciben mail de Facturación indicando el Ok del ingreso de todos los movimientos y ejecuta bitácora de consolidación, donde divide los movimientos de consumo tanto en corrientes como en diferido	Procedimiento ejecución procesos diarios	Técnico de procesamiento Centro de Computo	Correo	Notificación del departamento de Facturación de la finalización de sus procesos	Confirmación para inicio de la ejecución de los procesos batch	Facturación debe finalizar sus procesos hasta las 23:30	
8	Ejecuta bitácora de Consolidación	Se cuenta con una bitácora electrónica en donde están ingresados todos los programas que deben ejecutarse, el proceso de consolidación se somete para las marcas registradas. El operador confirma el arranque del proceso de consolidación y a continuación se van ejecutando todos los programas en forma secuencial	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Confirmación para inicio de la ejecución de los procesos batch	Proceso de consolidación iniciado		

CONTINÚA →

9	Ejecuta bitácora Diaria	Posterior a la finalización de la bitácora de consolidación, el operador ejecuta la bitácora electrónica de tipo DIARIO, la cual tiene las mismas características que la anterior pero con programas diferentes, en donde se realiza el procesamiento para todas las entidades que se maneja.	Procedimiento ejecución procesos diarios para todas las marcas.	Técnico de procesamiento Centro de Computo	AS400	Proceso de consolidación finalizado	Proceso diario iniciado		
10	Monitorea que los trabajos sometidos se ejecuten correctamente	Con la herramienta Barcelona04, se monitorea de forma automática la ejecución de cada uno de los programas que son sometidos desde las bitácoras electrónicas		Técnico de procesamiento Centro de Computo	AS400	Ejecución de los procesos batch	Ejecución de programas monitoreado		
11	Recibe notificación automática vía correo del programa con error	En el evento en que se presente un error en la ejecución de los programas, la herramienta envía una notificación por correo al correo del operador, indicando el mensaje de error	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	Correo	Error en la ejecución de los programas	Evento notificado al operador		
12	Notifica el problema al gestor de problemas	Se notifica el incidente al gestor de problemas contactándolo telefónicamente para indicarle el mensaje de error, adicionalmente se abre un requerimiento para la gestión del problema. En caso de que el problema no se solucione en los tiempos establecidos, se escala a los niveles de gerencia		Técnico de procesamiento Centro de Computo	Herramienta de Service Desk	Evento notificado al operador	Evento notificado al gestor de problemas		
13	Recibe confirmación para continuar con los procesos batch	El analista determina el error y corrige el problema, dando la confirmación para continuar con los procesos		Gestor de Problemas	Herramienta de Service Desk AS400	Evento notificado al gestor de problemas	Evento solucionado y confirmación para la continuación de los procesos		
14	Verifica la finalización de los programas ejecutados	Al finalizar la ejecución de las bitácoras, se revisa la finalización de todas las entidades, las cuales deben tener el status de finalizado, también se revisa que no se encuentre ningún trabajo ejecutándose en el subsistema QBATCH. Los tiempos de inicio y finalización se registra en la bitácora de procesos	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Bitácora de procesos finalizado	Revisión de la finalización de los procesos		
15	Verificar archivos de control	Revisa los archivos de INTERESES SAFCTRP y de CONTROL GENF10 en todas las entidades, se verifica que este actualizado siempre a la fecha del último proceso ejecutado	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Revisión de la finalización de los procesos	Revisión de los archivos de control		
16	Verifica generación de reportes	Mediante el comando WRKSPLF en el equipo Gestor, se verifica que se hayan generado todos los reportes del proceso batch en base al listado de la bitácora en donde se registra el número de páginas por cada reporte	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Revisión de los archivos de control	Revisión de los reportes generados		
17	Carga los reportes generados al sistema de Gestión Documental	Todos los reportes que constan en la bitácora de procesos son cargados al sistema de gestión documental, para lo cual se direccionan a la cola en donde se tiene configurado el paso al sistema Ondemand	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Revisión de los reportes generados	Reportes del proceso batch cargados al sistema de gestión documental		
18	Ejecuta opción para la generación de archivos de control solicitados por entidades asociadas	Desde el menú del operador en el equipo Gestor para las entidades externas se ejecuta la opción que generan los archivos de procesamiento de bancos asociados	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Revisión de la finalización de los procesos	Archivos de entidades asociadas generados		

CONTINÚA →



19	Transmisión de archivos generados	Desde el menú del operador se realiza la transmisión de los archivos generados, para lo cual se cuenta con una aplicación en donde previamente se define los nombres de los archivos y la ruta de destino. Al finalizar la transmisión el operador verifica que se haya transmitido correctamente en el log del programa, esta información la adjunta en el correo de las novedades del turno	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Archivos de entidades asociadas generados	Verificación de la transmisión de los archivos		
20	Verifica que se ejecute programa para la carga batch en el equipo AUTORIZADOR	Una vez que se termina la ejecución del programa de carga batch en el equipo Gestor, se realiza la transmisión de la información al equipo Autorizador, por lo que se verifica que el programa que actualiza los datos se ejecute en el equipo Autorizador para todas las entidades	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Finalización del programa de carga batch en el Gestor	Verificación de la ejecución del programa de carga batch en el Autorizador		
21	Verificación de los archivos de control de carga batch	Se realiza el control de Carga Batch en el equipo Gestor desde el menú del operador en donde el estado debe estar en terminado. En el equipo autorizador se verifica el reporte generado desde la opción del CAO Grafico para consultar registros errados o diferencia en registros		Técnico de procesamiento Centro de Computo	AS400	Finalización del programa de carga batch en el Autorizador	Verificación de la carga batch en los equipos Autorizador y Gestor		
22	Recibe notificación automática vía correo de diferencias de registros entre Gestor y Autorizador	En el caso de que se presente algún incidente, con el software de monitoreo Barcelona, se tiene configurado una alerta que envía por correo una notificación al operador para alertarle sobre diferencias presentadas en el número de registros transmitidos desde el Gestor hacia el Autorizador en el proceso de carga batch		Técnico de procesamiento Centro de Computo	AS400	Diferencia de registros transmitidos entre Gestor y Autorizador	Notificación sobre diferencias al operador		
23	Notifica el incidente al gestor de problemas	Cuando se presenta el evento de error se notifica al gestor de problemas para la corrección de la inconsistencia, abriendo un requerimiento		Técnico de procesamiento Centro de Computo	AS400	Notificación sobre diferencias al operador	Problema resuelto por analista en stand by		
24	Verifica la transmisión de los archivos enviados al sistema de cobranzas	Desde el menú del operador se ingresa a la opción de transmisión de archivos, para verificar que los archivos enviados al sistema de cobranzas se hayan depositado correctamente. Se cuenta con un monitoreo automático que alerta al operador en el caso de que la transmisión haya fallado, en este evento se notifica al gestor de problemas		Técnico de procesamiento Centro de Computo	AS400	Proceso batch finalizado	Verificación de la transmisión de los archivos		
25	Ejecuta proceso de liquidación a establecimientos	En base a las fechas de pago que son remitidas por el departamento de facturación, se ejecuta proceso de liquidación a establecimientos para generar los pagos a comercios. Desde la opción del operador se ingresa la fecha de liquidación que corresponda para que se ejecute el programa	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Verificación de la carga batch en los equipos Autorizador y Gestor	Ejecución del proceso de liquidación de pagos a establecimientos		
26	Verifica generación de reportes	Revisa reportes de resúmenes generados para comprobar que se hayan generado los pagos para cada fecha liquidada.	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Ejecución del proceso de liquidación de pagos a establecimientos	Verificación de los reportes de resumen		

CONTINÚA →

27	Verifica archivo de control LIQUE30P	Mediante una consulta a la base de datos en el equipo Gestor, se verifica el archivo LIQUE30P en el cual deben constar las fechas de pago afectadas en el sistema	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Verificación de los reportes de resumen	Archivo de control LIQE30P revisado		
28	Direcciona spools de cheques generados a cola de impresión	Los reportes con formato de cheques se direccionan a la cola de impresión con el comando CHGOUTQ, los cuales son impresos por el departamento de Back Office	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Archivo de control LIQE30P revisado	Spools de cheques direccionados a la cola de impresión		
29	Carga de reportes contables al sistema de Gestión Documental	Todos los reportes que constan en la bitácora de procesos son cargados al sistema de gestión documental, para lo cual se direccionan a la cola en donde se tiene configurado el paso al sistema Ondemand. Adicionalmente se transmite los archivos de comprobantes y anexos a la empresa de impresión.	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Archivo de control LIQE30P revisado	Carga de reportes y transmisión de archivos para impresión		
30	Verifica que haya finalizado programa que actualiza los movimientos de la consulta web	En el servidor SRWEB se ejecuta un proceso bat que actualiza la información de movimientos de socios que consultan desde el portal web	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Finalización de programa que actualiza movimientos web en el Gestor	Consulta de movimientos de clientes actualizado en el portal web		
31	Ejecuta opción para la generación de archivos para banco Pichincha	Desde la opción del menú del operador, se ejecutan la generación de archivos que son transmitidos al banco	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Bitácora de procesos	Generación de archivos ejecutado	Los archivos se transmiten hasta las 14:00	
32	Verifica que la transmisión de archivos finalizó correctamente	Desde el menú del operador se realiza la transmisión de los archivos generados, para lo cual se cuenta con una aplicación en donde previamente se define los nombres de los archivos y la ruta de destino. Al finalizar la transmisión el operador verifica que se haya transmitido correctamente en el log del programa, esta información la adjunta en el correo de las novedades del turno	Procedimiento ejecución procesos diarios.	Técnico de procesamiento Centro de Computo	AS400	Generación de archivos finalizado	Verificación de la transmisión de los archivos		
33	Ejecuta bitácora de Facturación	Se tiene establecido un calendario de facturación mensual para todas las entidades que se procesa, en los días en que se tiene el ciclo de facturación el operador ejecuta la bitácora electrónica de tipo FACTURACIÓN la cual tiene las mismas características que las anteriores pero con programas diferentes, en donde se realiza el procesamiento para todas las marcas	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Fecha corresponde a ciclo de facturación	Bitácora de facturación iniciada		
34	Realiza el cuadro de reportes TURP013, contra el FAC0310A	Se tiene un punto de pare de la bitácora , en el momento en que el proceso actualiza la generación de movimientos facturados se generan dos reportes: TURPE013: RESUMEN GENERAL DEL MOVIMIENTO A FACTURAR y FAC0310A: LIQUIDACIÓN  Con esta información se realiza un cuadro entre los dos reportes como punto de control, en el caso de que no se tengan novedades se continua con la ejecución del proceso	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Punto de pare en la generación de liquidación de movimientos facturados	Cuadro de movimientos verificado		

CONTINÚA →

35	Reporta incidentes del proceso de facturación	En el caso en que se presente algún error en la ejecución de los programas o novedades en el cuadro, se notifica el problema al analista en stand by contactándolo telefónicamente para indicarle el mensaje de error, se completa la actividad abriendo un requerimiento e informando al Subgerente del Centro de Computo. El analista determina el error y corrige el problema, dando la confirmación para continuar con los procesos		Técnico de procesamiento Centro de Computo	Herramienta de Service Desk	Evento notificado al operador	Evento notificado al analista en stand by		
36	Transmite archivos de muestras de estados de cuenta a la empresa de Impresión	En el momento en que se genera las muestras de estados de cuenta, se convierte a un archivo de texto con el software Symtrax, y se remite a la empresa que da los servicios de impresión, con una notificación del detalle de los archivos. Las muestras generadas son un grupo de estados de cuenta que el usuario ingresa en el sistema para realizar los controles correspondientes	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Muestras de estados de cuenta generados	Archivo de muestras de estados de cuenta enviado		
37	Carga los reportes de facturación al sistema Documenta	Todos los reportes que constan en la bitácora de procesos son cargados al sistema de gestión documental, para lo cual se direccionan a la cola en donde se tiene configurado el paso al sistema Ondemand, en base a estos reportes se realiza el control de la facturación por parte de Control Interno	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Archivo de muestras de estados de cuenta enviado	Reportes cargados al sistema de gestión documental		
38	Recibe el OK de la revisión realizada por Control Interno	El proceso de ejecución se detiene en un punto de espera, mientras el departamento de Control Interno revisa la información generada para certificar que la actualización de los datos no tiene inconsistencias. En el caso de que se presente alguna observación se comunica a Desarrollo para el reproceso de estados de cuenta. En el caso de que todo este correcto, Control Interno da el visto bueno con firmas de responsabilidad en la bitácora de procesos.	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Punto de pare para la revisión de Control Interno	Confirmación para continuar con la ejecución del proceso		
39	Transmite archivos de estados de cuenta	Para las entidades Visa y MasterCard se realiza la transmisión de los archivos de estados de cuenta personales y corporativos, los cuales se depositan en el servidor FTP del banco Pichincha dese la opción del menú del operador	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Generación del archivo de estados de cuenta	Verificación de la transmisión de los archivos		
40	Envía los archivos de estados de cuenta a la empresa de impresión con notificación por correo	Cuando se tiene el Ok de Control Interno se envían los archivos de estados de cuenta, para lo cual se convierte a un archivo de texto con el software Symtrax, y se remite a la empresa que da los servicios de impresión, con una notificación del detalle de los archivos.	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Ok de la revisión de Control Interno	Archivos de estados de cuenta transmitidos para la impresión		

CONTINÚA →

41	Verifica la finalización de los programas ejecutados y registra los tiempos de los procesos en la bitácora	Al finalizar la ejecución de las bitácoras, se revisa la finalización de todas las entidades, las cuales deben tener el status de finalizado, también se revisa que no se encuentre ningún trabajo ejecutándose en el subsistema QBATCH. Los tiempos de inicio y finalización se registra en la bitácora de procesos	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Finalización de la bitácora electrónica de facturación	Revisión de la finalización de los procesos		
42	Carga los archivos de estados de cuenta al Sistema de Gestión Documental	Todos los reportes que constan en la bitácora de procesos de facturación son cargados al sistema de gestión documental, para lo cual se direccionan a la cola en donde se tiene configurado el paso al sistema Ondemand, a continuación se liberan los spools con la opción 6.	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Ok de la revisión de Control Interno	Estados de cuenta cargados al sistema de gestión documental para la consulta de usuarios		
43	Verifica que haya finalizado programa que actualiza los movimientos de la consulta web	El operador verifica que haya finalizado la ejecución del programa TODO1 de facturación, el cual genera los movimientos para la web, a continuación se ingresa al servidor SRVWEB y ejecuta el bat que realiza la carga de la información al portal web	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Finalización del programa para la generación de movimientos web	Movimientos de socios cargados en el portal web para la consulta		
44	Ejecuta proceso de renovaciones para estudio en el ciclo 30	Únicamente en el ciclo 30, desde el menú del operador se ejecuta la opción para la generación de renovaciones de estudio, el proceso genera los reportes que son transmitidos al departamento de Crédito para el análisis de las tarjetas que serán renovadas	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Finalización de la bitácora electrónica de facturación	Proceso de renovaciones para estudio ejecutado y transmisión de reportes al departamento de Crédito		CONTINÚA →
45	Respaldar archivos generados en la facturación	Cuando se completa la ejecución de toda la bitácora de facturación, se realiza el respaldo de la librería *BACKUP de acuerdo a la entidad que se está procesando, se registra el número de objetos salvados y la secuencia lógica de la cinta donde se realizó el respaldo	PRO_CC_MANUAL DE PROCESOS FACTURACION	Técnico de procesamiento Centro de Computo	AS400	Finalización de la bitácora electrónica de facturación	Respaldo obtenido del proceso de facturación		

4.3.4.2. Subproceso: Servicio de back up

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos
1	Inicializar la cinta	En el caso de que el respaldo sea ejecutado en la plataforma AS400 de los equipos de Producción de Ecuador se debe ingresar la cinta diaria entregada por Control Tecnológico en la librería de respaldos, mediante la interfaz gráfica se debe ubicar la cinta en el drive asignado a las particiones de producción.  Mediante el comando INZTAP se debe preparar la cinta para el respaldo, el comando elimina la información anterior y etiqueta de forma lógica a la cinta para iniciar el backup		Técnico de procesamiento Centro de Computo	AS400	Cinta de respaldo entregada por Control Tecnológico	Cinta inicializada		
2	Ejecutar backup del servidor CAO	A las 22:00 antes del inicio de los procesos diarios se ejecuta el respaldo del equipo autorizador de producción mediante el siguiente comando CALL QGPL/SALVACAO, el cual salva las librerías previamente definidas para este servidor	PRO_CC_PROCEDIMIENTO DE RESPALDOS DEL SISTEMA AS400-825 CAO	Técnico de procesamiento Centro de Computo	AS400	Cinta inicializada	Respaldo ejecutado equipo Cao		
3	Verificar finalización de la bitácora diaria para cada marca	En el caso de que el respaldo del equipo CAO se haya completado satisfactoriamente y que corresponda a un backup diario, es decir de lunes a viernes, se debe verificar que haya finalizado la ejecución de los cierres diarios de todas las entidades para todas las marcas.		Técnico de procesamiento Centro de Computo	AS400	Proceso diario finalizado	Finalización del proceso diario verificado		
4	Ejecutar backup del servidor Gestor	El backup se obtiene de forma secuencial conforme va finalizando la ejecución de los cierres batch, la obtención del respaldo se lo realiza mediante la opción definida en el menú del operador, en donde se parametriza las librerías que deben salvarse por cada ambiente.	PRO_CC_PROCEDIMIENTO DE RESPALDOS DEL SISTEMA AS400-825 GESTOR	Técnico de procesamiento Centro de Computo	AS400	Finalización del proceso diario verificado	Respaldo ejecutado equipo Gestor		
5	Realizar backup del ambiente de contabilidad	En el caso de que el respaldo del equipo Gestor se haya completado satisfactoriamente y una vez que haya finalizado el proceso de liquidación a establecimientos de la marca 1, se ejecuta el respaldo del ambiente de Contabilidad desde la opción definida en el menú del operador en donde se parametrizar las librerías que deben ser salvadas	PRO_CC_PROCEDIMIENTO DE RESPALDOS DEL SISTEMA AS400-825 GESTOR	Técnico de procesamiento Centro de Computo	AS400	Respaldo ejecutado equipo Gestor	Respaldo ambiente de contabilidad Gestor		
6	Entregar cintas al supervisor	En el caso de que el respaldo haya finalizado correctamente, la cinta se entrega al supervisor adjuntando el display con la información contenida en el respaldo, esta actividad se aplica para los siguientes equipos: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta equipos Gestor y CAO producción Perú 3) Cinta equipo DESARID, ambiente desarrollo 4) Cinta equipo F170, ambiente desarrollo 5) Cinta base de datos software Tivoli, ambiente de producción para plataformas distintas al AS400.		Técnico de procesamiento Centro de Computo	AS400 Tivoli	Cintas con respaldos ejecutados	Cintas entregadas al Supervisor		
7	Verificar que la información haya sido respaldada completa	Se realiza una validación de los respaldos obtenidos mediante una revisión de los display de las cintas en las que se verifica que las librerías respaldadas estén completas, esta actividad se aplica para los siguientes equipos: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta equipos Gestor y CAO producción Perú 3) Cinta equipo DESARID, ambiente desarrollo 4) Cinta equipo F170, ambiente desarrollo		Jefe de procesamiento Centro de Computo	Herramienta de requerimientos	Cintas entregadas al Supervisor	Respaldo verificado		

CONTINÚA →

8	Ejecutar backup de librerías no respaldadas	En el caso en que se constate que el respaldo esté incompleto, se procede a realizar un respaldo de las librerías que no fueron salvadas en el proceso, esta actividad se aplica para los siguientes equipos: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta equipos Gestor y CAO producción Perú 3) Cinta equipo DESARID, ambiente desarrollo 4) Cinta equipo F170, ambiente desarrollo		Técnico de procesamiento Centro de Computo	AS400	Respaldo incompleto	Respaldo ejecutado		
9	Ejecutar duplicado de la cinta diaria	Para el caso en que no se encontraron novedades en la verificación y las cintas corresponden a la plataforma AS400 de los equipos de producción Gestor y Autorizador tanto de Ecuador como Perú, se procede con la obtención de los duplicados de las cintas mediante el comando DUPTAP		Técnico de procesamiento Centro de Computo	AS400	Respaldo verificado	Cinta duplicada		
10	Realizar memo de entrega detallando cada cinta que será entregada	Se elabora un acta de entrega recepción en donde se detallan todas las cintas que son entregadas a Control Tecnológico.		Jefe de procesamiento Centro de Computo	Windows	Respaldo verificado Cinta duplicada	Acta realizada		
11	Entrega cintas y memos al área de Seguridad	Mediante el acta firmada por el Centro de Computo y Control Tecnológico se hace entrega formal de las siguientes cintas en forma diaria: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta duplicada equipos de producción Ecuador 3) Cinta equipos Gestor y CAO producción Perú 4) Cinta duplicada equipos de producción Perú 5) Cinta equipo DESARID, ambiente desarrollo 6) Cinta equipo F170, ambiente desarrollo 7) Cinta base de datos software Tivoli Los días lunes se entrega adicional a las diarias las siguientes cintas, que corresponden a los respaldos semanales: 8) Cinta de los equipos de pruebas de Ecuador y Perú PRUEBASID y TESTPE 9) Cinta duplicada de los respaldos obtenidos mediante Tivoli	PRO_CC_PROCEDIMIENTO DE RESPALDOS DEL SISTEMA AS400-825 GESTOR	Jefe de procesamiento Centro de Computo		Acta realizada	Cintas entregadas a Control Tecnológico		
12	Recibir memo firmado y archivar	Como medio de constatación una copia del acta firmada se entrega al Centro de Computo y Control Tecnológico		Jefe de procesamiento Centro de Computo		Cintas entregadas a Control Tecnológico	Acta de recepción firmada		
13	Verificar que haya terminado los procesos Diarios	Para el caso de que se realice un respaldo del equipo Gestor de Ecuador de forma semanal o mensual se debe verificar que los procesos batch hayan finalizado para todas las marcas y entidades		Técnico de procesamiento Centro de Computo	AS400	Proceso diario finalizado	Finalización del proceso diario verificado		
14	Realizar backup semanal del ambiente del servidor Gestor	El respaldo se lo ejecuta mediante el comando SAVLIB con el parámetro ALLUSR, es decir se respaldan todas las librerías de usuario del sistema	PRO_CC_PROCEDIMIENTO DE RESPALDOS DEL SISTEMA AS400-825 GESTOR	Técnico de procesamiento Centro de Computo	AS400	Finalización del proceso diario verificado	Respaldo ejecutado equipo Gestor		

CONTINÚA →

15	Realizar backup mensual del ambiente del servidor Gestor	El respaldo mensual corresponde al primer día de cada mes, el cual se obtiene por ambientes si se ejecuta en días laborables o salvando todas las librerías de usuario (ALLISR) si se ejecuta el fin de semana	PRO_CC_PROCEDIMIENTO DE RESPALDOS DEL SISTEMA AS400-825 GESTOR	Técnico de procesamiento Centro de Computo	AS400	Finalización del proceso diario verificado	Respaldo ejecutado equipo Gestor		
16	Entregar cintas al supervisor	En el caso de que el respaldo semanal o mensual se haya obtenido correctamente se entregan las cintas al supervisor para su validación siguiendo el proceso descrito anteriormente.		Técnico de procesamiento Centro de Computo		Cintas con respaldos ejecutados	Cintas entregadas al Supervisor		
17	Verificar que no estén usuarios en el sistema	Para el caso en que el respaldo corresponde a la plataforma As400 de los ambientes de no producción, antes de ejecutar el respaldo se verifica que no existan usuarios en el sistema para evitar bloqueos en el proceso.	PRO_CC_PROCEDIMIENTO DE RESPALDOS DE LOS SISTEMAS DE PRUEBAS Y DESARROLLO	Técnico de procesamiento Centro de Computo	AS400	Bitácora de procesos	Ambiente listo para respaldo		
18	Realizar backup diario, semanal y mensual (pruebas y desarrollo)	Los respaldos se obtienen tomando en cuenta las siguientes consideraciones: 1) Se debe inicializar las cintas 2) Para el equipo DESARID de forma diaria se salvan programas con el comando CALL QGPL/SALVADESA. También se salvan los objetos y documento de usuario (IFS y DLO), para lo cual se ejecuta el siguiente comando CALL PROD/SAVIFSDLO. 3) Para el equipo F170 se salva de forma diaria todas las librerías con el parámetro ALLUSR 4) Para los equipos TESTPE y PRUEBASID, el respaldo se lo ejecuta de forma semanal mediante el parámetro ALLUSR	PRO_CC_PROCEDIMIENTO DE RESPALDOS DE LOS SISTEMAS DE PRUEBAS Y DESARROLLO	Técnico de procesamiento Centro de Computo	AS400	Ambiente listo para respaldo	Respaldo equipos ejecutado		
19	Entregar cintas al supervisor	En el caso de que el respaldo se haya obtenido correctamente se entregan las cintas al supervisor para su validación siguiendo el proceso descrito anteriormente.		Técnico de procesamiento Centro de Computo		Cintas con respaldos ejecutados	Cintas entregadas al Supervisor		
20	Verificar que los procesos diarios en Perú hayan finalizado	Antes de la ejecución del respaldo se debe verificar que haya finalizado la ejecución de los cierres diarios del cierre batch de Perú		Técnico de procesamiento Centro de Computo	AS400	Proceso diario finalizado	Finalización del proceso diario verificado		
21	Inicializar la cinta	En el caso de que el respaldo sea ejecutado en la plataforma AS400 de los equipos de Producción de Perú se debe ingresar la cinta diaria entregada por Control Tecnológico en la librería de respaldos, mediante la interfaz gráfica se debe ubicar la cinta en el drive asignado a las particiones de producción.  Mediante el comando INZTAP se debe preparar la cinta para el respaldo, el comando elimina la información anterior y etiqueta de forma lógica a la cinta para iniciar el backup		Técnico de procesamiento Centro de Computo	AS400	Finalización del proceso diario verificado	Cinta preparada para respaldo		

CONTINÚA →

22	Ejecutar backup para servidor Gestor Perú	El respaldo se lo ejecuta en el equipo Gestor de Perú, mediante el comando SAVLIB con el parámetro ALLUSR, es decir se respaldan todas las librerías de usuario del sistema		Técnico de procesamiento Centro de Computo	AS400	Cinta preparada para respaldo	Respaldo ejecutado		
23	Ejecutar backup Para servidor CAO Perú	El respaldo se lo ejecuta en el equipo Autorizador de Perú mediante el comando SAVLIB con el parámetro ALLUSR, es decir se respaldan todas las librerías de usuario del sistema		Técnico de procesamiento Centro de Computo	AS400	Cinta preparada para respaldo	Respaldo ejecutado		
24	Entregar cintas al supervisor	En el caso de que el respaldo se haya obtenido correctamente se entregan las cintas al supervisor para su validación siguiendo el proceso descrito anteriormente.		Técnico de procesamiento Centro de Computo		Cintas con respaldos ejecutados	Cintas entregadas al Supervisor		
25	Activar dispositivo	En el caso en que se presente un error en cualquier tipo de los resoplados de la plataforma AS400, el primer paso es revisar si el dispositivo configurado para las cintas se encuentra activo, mediante el comando wrkcfgsts *dev tap*, de presentarse esta novedad es necesario activar el dispositivo		Técnico de procesamiento Centro de Computo	AS400	Error en dispositivo	Dispositivo activado		
26	Cambiar backup al dispositivo activo	Otro tipo de error puede relacionarse con el direccionamiento del respaldo a un dispositivo que no está activo, en este caso se debe cambiar la cinta o desde el comando para salvar apuntar al dispositivo activo		Técnico de procesamiento Centro de Computo	Librería de respaldos	Error cinta no encontrada	Cinta ingresada en dispositivo activo		
27	Ingresar cinta en el drive correspondiente	En el caso de que el error se presente debido a que la cinta no esté ingresada en el drive, la solución es ubicar la cinta en el drive activo desde la interfaz gráfica de la librería de respaldos		Técnico de procesamiento Centro de Computo	Librería de respaldos	Error cinta no encontrada	Cinta ingresada en dispositivo activo		
28	Notificar al proveedor para revisión de la librería	Si el error se debe a un fallo de hardware en la librería de respaldos, se debe abrir una llamada de soporte al proveedor indicado la serie del equipo y el mensaje de error que se despliega al realizar el respaldo, se genera un número de caso para realizar el seguimiento del problema		Técnico de procesamiento Centro de Computo		Error de librería de respaldos	Caso de soporte abierto con proveedor		
29	Hacer seguimiento al proveedor	En el caso de que no se dé una solución por el proveedor en los tiempos definidos, el supervisor realiza un seguimiento con el número de caso abierto		Jefe de procesamiento Centro de Computo		Caso de soporte abierto con proveedor	Soporte gestionado		
30	Volver a ejecutar backup	Cuando se han corregido todos los tipos de errores, se debe volver a ejecutar el respaldo que corresponda siguiendo el procedimiento descrito anteriormente	pro_cc_procedimiento de respaldos del sistema as400-825 cao pro_cc_procedimiento de respaldos del sistema as400-825 gestor pro_cc_procedimiento de respaldos de los sistemas de pruebas y desarrollo	Técnico de procesamiento Centro de Computo	AS400	Errores solucionados	Respaldos ejecutados		
31	Verificar en bitácora tipo de backup personal a realizar	En el caso de que el respaldo sea ejecutado mediante la herramienta Tivoli y corresponda a los backup de equipos personales se debe verificar que los equipos se encuentren encendidos para que se conecten mediante el agente Tivoli		Técnico de procesamiento Centro de Computo	Tivoli	Bitácora de procesos	Verificación completada para ejecutar los respaldos personales		

CONTINÚA →



32	Ejecutar backup personal en TSM	Para la ejecución del respaldo se debe conectar al servidor Tivoli y ejecutar la opción configurada para el efecto, la frecuencia de los backup es la siguiente: 1) Miércoles equipo de Presidencia 2) Jueves equipo de Gerencia de Operaciones	procedimiento para sacar backup de los personales	Técnico de procesamiento Centro de Computo	Tivoli	Verificación completada para ejecutar los respaldos personales	Respaldo ejecutado		
33	Determinar información que se requiere respaldar	En el caso de que el respaldo sea ejecutado mediante la herramienta Tivoli y corresponda a los backup de tipo diario o semanal, es necesario configurar en la herramienta para adicionar los servidores que se van a respaldar, esta actividad se lo realiza una sola vez y mediante Tivoli se respalda lo siguiente: 1.- Servidores Windows: archivos carpetas y bases de datos. 2.- Servidores Aix: file systems		Jefe de procesamiento Centro de Computo	Tivoli	Requerimiento de respaldo	Configuración ejecutada		
34	Ejecutar backup incremental	Los respaldos se ejecutan de forma automática en base a la calendarización definida en la herramienta Tivoli. Para los respaldos diarios se tiene una configuración de tipo incremental en donde se salva las modificaciones que se hayan realizado en los archivos. Para los respaldos semanales se tiene una configuración de tipo full backup, en donde se respalda todos los archivos, esto aplica para las bases de datos SQL. El tiempo de retención de los respaldos es de 30 días	procedimiento para sacar backup base de datos sql procedimiento para sacar backup de archivos o carpetas	Técnico de procesamiento Centro de Computo	Tivoli	Calendarizador Tivoli	Respaldo ejecutado		
35	Ejecutar backup según calendario definido	En el caso de que el respaldo sea ejecutado mediante la herramienta Tivoli y corresponda a los backup de tipo mensual, es necesario verificar en la herramienta que el tipo de respaldo corresponda a full backup		Jefe de procesamiento Centro de Computo	Tivoli	Calendarizador Tivoli	Configuración revisada		
36	Ejecutar backup completo	Los respaldos se ejecutan de forma automática en base a la calendarización definida en la herramienta Tivoli. Para los respaldos mensuales se tiene una configuración de tipo full backup, en donde se respalda todos los archivos Las cintas mensuales no se vuelven a reutilizar	procedimiento para sacar backup base de datos sql	Técnico de procesamiento Centro de Computo	Tivoli	Calendarizador Tivoli	Respaldo ejecutado		
37	Verificar ejecución correcta de backups	La revisión de los respaldos ejecutados automáticamente se realiza a través del aplicativo Tivoli con el comando QEVENT en donde se verifica que los respaldos hayan finalizado satisfactoriamente		Técnico de procesamiento Centro de Computo	Tivoli	Respaldo ejecutado	Respaldo obtenido verificado		
38	Realizar copia del backup	En el caso en que el respaldo se haya completado satisfactoriamente se realiza un duplicado de las cintas, para lo cual se ejecuta el comando que realiza la copia desde la herramienta Tivoli		Técnico de procesamiento Centro de Computo	Tivoli	Respaldo obtenido verificado	Cinta duplicada		
39	Enviar cintas al área de Seguridad	Se realiza la misma actividad descrita para la plataforma AS400, en el acta de entrega recepción se adicionan las cintas que se respaldan con Tivoli		Técnico de procesamiento Centro de Computo	Tivoli	Acta realizada	Cintas entregadas a Control Tecnológico		
40	Recibir memo firmado y archivar	Como medio de constatación una copia del acta firmada se entrega al Centro de Computo y Control Tecnológico		Técnico de procesamiento Centro de Computo		Cintas entregadas a Control Tecnológico	Acta de recepción firmada		
41	Informar novedades presentadas al supervisor	En el caso de que se presenten novedades en la verificación de los respaldos ejecutados, se notifica al supervisor los errores encontrados y que no se pueden resolver por el Técnico del Centro de Computo		Técnico de procesamiento Centro de Computo		Errores detectados	Notificación de error a Supervisor		

CONTINÚA →

42	Verificar cual servidor no fue respaldado	Para verificar el error reportado en el respaldo, se ingresa en el aplicativo Tivoli para determinar el servidor en donde se presentó el fallo		Jefe de procesamiento Centro de Computo	Tivoli	Notificación de error a Supervisor	Servidor en donde se presentó el error identificado		
43	Revisar logs dentro de servidor	Para ingresar al servidor en donde se detectó el error se solicita al área de Networking los datos de acceso y se revisa el archivo de log generado por la aplicación TSM para tomar las medidas correctivas		Jefe de procesamiento Centro de Computo		Identificar Servidor del error	Problema identificado		
44	Verificar que los servicios dentro del servidor estén levantados.	En el servidor donde se presentó el error se verifica que los servicios que utiliza la aplicación Tivoli se encuentren activos, de ser el caso se los reinicia		Jefe de procesamiento Centro de Computo	Tivoli	Problema identificado	Error corregido		
45	Ejecutar nuevamente el backup	Cuando se han corregido todos los tipos de errores, se debe volver a ejecutar el respaldo que corresponda siguiendo el procedimiento descrito anteriormente		Técnico de procesamiento Centro de Computo	Tivoli	Error corregido	Respaldo ejecutado		

4.3.4.3. Subproceso: Servicio de recovery

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos
1	Ubicar cinta de respaldo	Para identificar la cinta desde donde se debe recuperar la información se tienen tres posibilidades:  1) Si el respaldo fue obtenido en la plataforma AS400, las cintas deben ser proporcionadas por Control Tecnológico quienes recuperan la cinta desde la bóveda local o solicitando a la empresa contratada para la custodia externa. 2) Si el respaldo fue obtenido mediante el software Tivoli, el Centro de Computo dispone de las cintas de los últimos 30 días las cuales se encuentran en la librería de respaldo, en este caso no es necesario que se entreguen las cintas. 3) Si el respaldo fue obtenido mediante el software Tivoli, y la solicitud de restauración corresponde a una fecha posterior a los 30 días, la cinta debe ser proporcionada por Control Tecnológico.		Técnico de procesamiento de Centro de Computo	AS400	Solicitud de respaldo a través de la herramienta de Service Desk	Cinta localizada		
2	Solicitud de respaldos	Proceso de Control Tecnológico en donde se solicitan las cintas custodiadas ya sea local o externamente.		Analista de Control Tecnológico		Solicitud de respaldo a través de la herramienta de Service Desk	Cinta entregada a Centro de Cómputo		
3	Verificar que archivos solicitados existan en el sistema	Para verificar que los archivos indicados en el formulario de solicitud de respaldos sean correctos, en el AS400 se busca el objeto con el comando wrkobj. Para los respaldos obtenidos con Tivoli, se ingresa en la aplicación y se realiza una búsqueda del archivo. En el caso de que no se encuentre el archivo, se le notifica al usuario para que verifique si esta correcta la información del formulario.		Técnico de procesamiento de Centro de Computo	AS400	Formulario solicitud de respaldos Cinta para restauración	Archivos solicitados verificados		
4	Restaurar la información solicitada	Para el ambiente AS400, se ingresa la cinta histórica en la librería de respaldos y se restauran los objetos solicitados mediante el comando RSTOBJ, los archivos deben ser restaurados en la librería RESPALDOS del equipo AS400. Una vez restaurada la información se da autoridad al objeto para que pueda ser accedido por el usuario	pro_cc_procedimiento de restauración as400	Técnico de procesamiento de Centro de Computo	AS400	Archivos solicitados verificados	Restauración de los archivos solicitados ejecutado	Los archivos deben restaurarse en la librería RESPALDOS	
		Para el ambiente Tivoli se ingresa la cinta histórica en la librería de respaldos y se ingresa en la aplicación desde donde se selecciona el archivo a restaurar y la carpeta destino. Para el caso de base de datos, se selecciona la base que se debe restaurar y desde la opción Restore Database se recupera la información solicitada	pro_cc_procedimiento de restauración tsm procedimiento para restaurar base de datos sql.	Técnico de procesamiento de Centro de Computo	Tivoli	Archivos solicitados verificados	Restauración de los archivos solicitados ejecutado		

CONTINÚA →

5	Notificar a usuario que la información ha sido recuperada	Si el proceso de restauración finalizó de forma satisfactoria, se comunica al usuario solicitante por correo que la información fue restaurada, indicándole la ruta de destino de los archivos	pro_cc_procedimiento de restauración tsm para restaurar base de datos sql pro_cc_procedimiento de restauración as400	Técnico de procesamiento de Centro de Computo	AS400	Archivos restaurados correctamente	Notificación a usuario sobre la correcta restauración de la información		
6	Devolver la cinta al área de seguridad	Si el proceso de restauración finalizó de forma satisfactoria, se entrega las cintas y el formulario de respaldos al área de Control Tecnológico	pro_cc_procedimiento de restauración as400	Técnico de procesamiento de Centro de Computo	AS400	Notificación a usuario sobre la correcta restauración de la información	Cintras entregadas a Control Tecnológico		
7	Notificar a usuario que la información no ha sido recuperada	En el caso de que no se haya recuperado la información solicitada, se le comunica al usuario para evaluar la posibilidad de recuperar la información desde otra cinta		Técnico de procesamiento de Centro de Computo	AS400 Tivoli	Información no recuperada	Notificación a usuario, para evaluar si se puede recuperar la información desde otra cinta		
8	Cerrar requerimiento	Una vez realizada la operación de recovery, se procede a cerrar el requerimiento en la herramienta de Service Desk.		Técnico de procesamiento de Centro de Computo	Herramienta de Service Desk	Notificación a usuario sobre la correcta restauración de la información	Requerimiento cerrado en la herramienta de Service Desk		
9	Custodia de respaldo	Una vez realizada la operación de recovery, se procede a devolver la cinta de respaldo al área de Control Tecnológico para su almacenamiento y custodia.		Técnico de procesamiento de Centro de Computo		Requerimiento cerrado en la herramienta de Service Desk	Cinta devuelta a Control Tecnológico		

4.3.4.4. Subproceso: Depuración de archivos

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Acceder a cada equipo a depurar	De acuerdo al monitoreo que se realice del equipo y la política establecida se determina cuales quipos se deben depurar.		Técnico de procesamiento - Centro de Cómputo		Necesidad de depuración de espacio en disco	Equipos a depurar identificados			
2	Generar reporte en Excel de archivos a depurar	El técnico de procesamiento ejecuta los comandos en batch para obtener el listado de los objetos a depurar que se encuentran en las librerías de desarrollo y pruebas.		Técnico de procesamiento - Centro de Cómputo		Equipos a depurar identificados	Reporte de archivos a depurar			
3	Enviar reporte de depuración a dueños de archivos	El técnico de procesamiento envía el reporte de archivos a depurar a todos los dueños de dichos a archivos como advertencia de que estos serán depurados de no recibir una orden de no depuración.		Técnico de procesamiento - Centro de Cómputo		Reporte de archivos a depurar	Mail con reporte de archivos a depurar a todos los dueños de archivo			
4	Verificar archivos a depurar	Los dueños de archivos verifican que los archivos listados en el reporte puedan en efecto ser depurados y que su depuración no causará traumatismos a la operación.		Dueños de archivos - Diseño y Entrega del Servicio		Mail con reporte de archivos a depurar a todos los dueños de archivo	Reporte de archivos a depurar verificado por los dueños respectivos			
5	Solicitar no depuración de archivos a conservar	En caso de que el dueño de algún archivo requiera la no depuración de un archivo, este debe solicitarlo por medio de correo electrónico tan pronto tenga conocimiento al técnico de procesamiento del Centro de Cómputo o de lo contrario el archivo será depurado.		Dueños de archivos - Diseño y Entrega del Servicio		Reporte de archivos a depurar verificado por los dueños respectivos	Mail de solicitud de no depuración indicando los archivos a conservar		Los archivos cuya permanencia no sea solicitada una semana después de su notificación de depuración, serán depurados automáticamente.	
6	Generar nuevo reporte en Excel de archivos a depurar	El técnico de procesamiento ejecuta los comandos en batch para obtener el listado de los objetos a depurar que se encuentran en las librerías de desarrollo, pruebas, pre-producción y producción excluyendo los archivos a los cuales se les solicitó su permanencia.		Técnico de procesamiento - Centro de Cómputo		Mail de solicitud de no depuración indicando los archivos a conservar	Nuevo reporte de archivos a depurar			

CONTINÚA →

7	Comparar reportes para verificar los archivos a depurar	El técnico de procesamiento compara los dos reportes de depuración para asegurar que los archivos cuya permanencia fue solicitada hayan sido excluidos de la nueva lista de depuración.		Técnico de procesamiento - Centro de Cómputo		Nuevo reporte de archivos a depurar	Nuevo reporte de archivos a depurar verificado			
8	Backup	Previa a la depuración de los archivos, el técnico de procesamiento debe asegurar que dichos archivos hayan sido respaldados o de lo contrario realizar el back up correspondiente.		Técnico de procesamiento - Centro de Cómputo		Nuevo reporte de archivos a depurar verificado	Back up de los archivos a depurar			
9	Depurar archivos	Por medio de una herramienta automatizada el técnico de procesamiento selecciona los archivos a depurar y depura las librerías correspondientes a los ambientes de desarrollo y pruebas. Adicionalmente, corre la herramienta de depuración de los ambientes de preproducción y producción en donde se tiene previamente automatizada la depuración periódica de archivos.		Técnico de procesamiento - Centro de Cómputo		Back up de los archivos a depurar	Archivos depurados			El área de Diseño y Entrega del Servicio debe entregar la herramienta de automatización para poder depurar los archivos de librerías de los ambientes de desarrollo y pruebas. En caso contrario, la depuración de archivos para librerías de los ambientes de pruebas y desarrollo permanecerá a cargo del área de Diseño y Entrega del Servicio.
10	Informar archivos depurados a dueños de archivos	El técnico de procesamiento confirma por medio de correo electrónico a los dueños de archivos que dichos archivos fueron depurados exitosamente.		Técnico de procesamiento - Centro de Cómputo		Archivos depurados	Correo electrónico de conformación de depuración a los dueños de archivos.			

4.3.4.5. Subproceso: Soporte a usuarios

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos
1	Recibir y generar requerimiento	El área de Service Desk, recibe la solicitud del usuario vía mail o teléfono y la asigna al Supervisor del Centro de Cómputo según tipologías predefinidas a través de la herramienta de Service Desk.		Analista de primera línea Service Desk	Herramienta de Service Desk	Solicitud de soporte enviada por mail o teléfono al área de Service Desk	Requerimiento asignado a Supervisor de Centro de Cómputo	Todos los requerimientos deben ser canalizados a través de Service Desk	La herramienta de Service Desk debe tener la capacidad de workflow y escalamiento para manejar tipologías predefinidas de manera automática.
2	Verificar factibilidad del requerimiento	El requerimiento es revisado por el Supervisor, quien determina si el requerimiento es factible teniendo en cuenta que puede ser necesario la intervención de otra área para la ejecución y en cuyo caso solicitaría el apoyo de dicha área a través de Service Desk.		Jefe de procesamiento / monitoreo Centro de Cómputo	Herramienta de Service Desk	Requerimiento asignado a Supervisor de Centro de Cómputo	Factibilidad del requerimiento verificada por Supervisor		
3	Asignar analista al requerimiento	En el caso que el requerimiento se lo puede ejecutar por el Centro de Cómputo, se asigna al técnico del Centro de Cómputo mediante la herramienta de Service Desk. Se debe considerar la carga de los técnicos disponibles y los conocimientos necesarios para la atención del requerimiento. En caso de que el requerimiento se deba ejecutar otra área se debe solicitar otro requerimiento a través de Service Desk de manera que se ejecute el requerimiento de forma paralela por las aéreas ejecutoras.		Jefe de procesamiento / monitoreo Centro de Cómputo	Herramienta de Service Desk	Factibilidad del requerimiento verificada por Supervisor	Requerimiento asignado a Técnico de Centro de Cómputo a través de la herramienta de Service Desk		
4	Ejecutar requerimiento según solicitud	El requerimiento es ejecutado en base a la solicitud recibida. Ver detalle de tipificaciones en documento adjunto: Listado de tipificaciones de Centro de Cómputo.	Ver detalle de tipificaciones en documento adjunto: Listado de tipificaciones de Centro de Cómputo.	Técnico de procesamiento / monitoreo Centro de Cómputo		Requerimiento asignado a Técnico de Centro de Cómputo a través de la herramienta de Service Desk	Requerimiento ejecutado		
5	Notificar al usuario que el requerimiento se ha completado	Mediante correo o vía telefónica se le notifica al usuario que el requerimiento fue ejecutado y se verifica si cumplió con lo esperado.		Técnico de procesamiento / monitoreo Centro de Cómputo		Requerimiento ejecutado	Notificación y verificación con el usuario de la ejecución del requerimiento		
6	Cerrar el requerimiento	Una vez terminado y verificado el requerimiento, el técnico de Centro de Cómputo cierra el requerimiento en la herramienta de Service Desk.		Técnico de procesamiento / monitoreo Centro de Cómputo	Herramienta de Service Desk	Notificación y verificación con el usuario de la ejecución del requerimiento	Requerimiento finalizado en la herramienta		
7	Notificar al usuario indicando los motivos	En caso de que no sea factible la ejecución del requerimiento, el Supervisor de Centro de Cómputo notifica al usuario vía mail o telefónicamente indicando las razones por las cuales no se puede procesar la solicitud.		Jefe de procesamiento / monitoreo Centro de Cómputo	Herramienta de Service Desk	Factibilidad del requerimiento verificada por Supervisor	Notificación de rechazo a usuario solicitante vía mail o telefónicamente.		

4.3.5. Proceso: Administración del desempeño y la capacidad

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos
1	Gestión de la disponibilidad	El proceso de Gestión de la disponibilidad entrega información valiosa para determinar la capacidad de la infraestructura de TI. Las herramientas de monitoreo entregan mediciones de indicadores de desempeño (KPIs) que son evaluados posteriormente por las gerencias Centro de Cómputo e Infraestructura y Networking.		Proceso automático Técnico de monitoreo	Barcelona 04	Equipos de monitoreo configurados	VARIABLES de monitoreo medidas		Software de Monitoreo
2	Calcular KPIs de desempeño de infraestructura de TI	El técnico recibe las mediciones de los equipos de monitoreo y calcula los KPIs de desempeño de infraestructura que se hayan definido. Entre estos se encuentran: consumo en disco, consumo de memoria RAM, consumo de CPU (para servidores centrales y distribuidos), ancho de banda para los equipos de comunicación y la disponibilidad de los sistemas.		Técnico de monitoreo Centro de Cómputo		VARIABLES de monitoreo medidas	KPIs de infraestructura calculados	Los KPIs calculados a partir de la información medida por las herramientas de monitoreo deben estar definidos previamente.	
3	Redactar informe de KPIs y enviarlo a la Gerencia del área	Una vez calculados los KPIs, el técnico elabora un informe con los KPIs calculados e indicando los comentarios pertinentes respecto a los valores obtenidos. Posteriormente, lo entrega al Gerente del área para su revisión y análisis. Este informe se debe realizar mensualmente.		Técnico de monitoreo Centro de Cómputo		KPIs de infraestructura calculados	Informe de KPIs enviado al Gerente del área	El informe de capacidad se debe realizar mensualmente.	
4	Comparar medición de KPIs contra umbrales definidos	Los KPIs medidos se comparan contra los umbrales de alerta predefinidos para cada uno de ellos con el ánimo de identificar de manera oportuna problemas de capacidad de infraestructura.		Gerente del área Infraestructura y Networking, Centro de Cómputo		Informe de KPIs enviado al Gerente del área	KPIs comparados contra sus umbrales respectivos	Los umbrales de alerta para cada uno de los KPIs deben estar definidos previamente.	
5	Comparar desempeño actual contra desempeño proyectado	Los KPIs medidos ilustran la capacidad actual de la infraestructura instalada. Estos KPIs se deben contrastar contra la capacidad proyectada para cada uno de ellos que se encuentra estipulada en el plan de capacidad para el año en curso. De esta manera se logra un análisis proactivo y depurado mensualmente de la capacidad instalada y de su futuro crecimiento.		Gerente del área Infraestructura y Networking, Centro de Cómputo		Informe de KPIs enviado al Gerente del área	Capacidad actual contrastada contra capacidad proyectada	El plan de capacidad se debe realizar anualmente en donde se proyecte la capacidad futura para el año y se planeen los aumentos de capacidad requeridos. Aquí se incluyen los KPIs y los ANS pertinentes y se definen los umbrales de alerta de los KPIs.	
6	Determinar aumento en capacidad	En caso de que las mediciones indiquen que la capacidad actual de algún recurso no es suficiente, se debe determinar qué aumento en capacidad se requiere para suplir la demanda actual de dicho recurso.		Gerente del área Infraestructura y Networking, Centro de Cómputo		KPIs comparados contra de capacidad actual contra capacidad proyectada	Aumento de capacidad en recurso determinado		
7	Aprobar aumento en capacidad	Los aumentos de capacidad en un recurso determinado que no estén estipulados en el plan de capacidad, deben ser aprobados por la gerencia de tecnología. Se debe verificar la viabilidad y el presupuesto requerido antes de aprobar dicho aumento.		Gerente de Tecnología		Aumento de capacidad en recurso determinado	Aumento aprobado		

CONTINÚA →



8	Aumentar capacidad	Se procede a aumentar la capacidad de los recursos necesario según el plan de capacidad o según la aprobación respectiva en caso contrario. El gerente de cada área debe gestionar la compra de los recursos requeridos apoyándose en el área de administrativo y siguiendo los lineamientos de compra de la organización.		Gerente del área Infraestructura y Networking, Centro de Cómputo		Aumento de capacidad en recurso determinado	Aumento en capacidad del recurso requerido instalado		
9	Revisar proyección de capacidad futura	La capacidad proyectada de los recursos de infraestructura se debe revisar y ajustar periódicamente con el ánimo de refinar la proyección del año en curso y de esa manera poder predecir con mayor certeza los aumentos futuros de capacidad. Esto reduce la probabilidad de pérdida de disponibilidad del servicio y la afectación al negocio.		Gerente del área Infraestructura y Networking, Centro de Cómputo		Aumento en capacidad del recurso requerido instalado	Proyección de capacidad futura revisada y ajustada (si aplica)		
10	Revisar ANS actuales y proponer nuevos si aplica	Los ANS de disponibilidad del servicio son función de la capacidad instalada y por lo tanto deben ser revisados cada vez que la capacidad cambie para determinar si es necesario ajustarlos o crear ANS nuevos.		Gerente del área Infraestructura y Networking, Centro de Cómputo		Proyección de capacidad futura revisada y ajustada (si aplica)	ANS actuales revisados y ajustados (si aplica)		
11	Actualizar plan de capacidad	Una vez revisada la proyección de capacidad futura y los ANS correspondientes, se procede a ajustar el plan de capacidad del año en curso reflejando los cambios realizados y las proyecciones ajustadas.		Gerente del área Infraestructura y Networking, Centro de Cómputo		ANS actuales revisados y ajustados (si aplica)	Plan de capacidad actualizado		
12	Aprobar plan de capacidad	En los casos en donde el plan de capacidad cambie, el gerente de tecnología debe revisar y aprobar dichos cambios.		Gerente de Tecnología		Plan de capacidad actualizado	Plan de capacidad actualizado y aprobado		

4.3.6. Proceso: Administración del ambiente físico

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos
1	Determinar componente a monitorear	Los aplicativos de monitoreo y el técnico de centro de cómputo están monitoreando permanentemente los componentes críticos del centro de cómputo entre los cuales se encuentran: la temperatura y humedad del aire, sistemas de potencia, filtraciones de líquidos, error humano y acceso del personal, humo o incendios y contaminantes del aire.		Técnico de Centro de Cómputo	Registro digital o analógico de temperatura, humedad, sistema de potencia, filtraciones de líquidos, error humano y acceso del personal, humo o incendios o contaminantes del aire	Necesidad de controlar el ambiente físico del centro de cómputo	Componentes a monitorear identificados	El monitoreo de componentes debe ser permanente y sin interrupciones para garantizar la seguridad física del centro de cómputo.	Sensores y Registro digital o analógico instalados en puntos de la sala de cómputo para temperatura, humedad, sistema de potencia, filtraciones de líquidos, error humano y acceso del personal, humo o incendios o contaminantes del aire
2	Revisar sensores de temperatura y sistema de aire acondicionado	Para monitorear la temperatura del aire se deben revisar los sensores de temperatura del aire en la sala, el rack y los equipos. De igual manera se debe revisar el correcto funcionamiento del sistema de aire acondicionado.		Área de Administrativo / automático	Sensores de temperatura y sistema de aire acondicionado	Componentes a monitorear identificados	Valores registrados de temperatura y sistema de aire acondicionado		
3	Revisar sensores de humedad	Para monitorear la humedad del aire se deben revisar los sensores de humedad relativa de la sala y del rack a una temperatura determinada.		Área de Administrativo / automático	Sensores de humedad	Componentes a monitorear identificados	Valores registrados de humedad		
4	Revisar niveles de tensión y corriente en UPS	Para monitorear los sistemas de potencia se debe revisar la calidad de la energía entregada por las unidades UPS verificando los niveles de tensión y corriente.		Área de Administrativo / automático	UPS	Componentes a monitorear identificados	Valores de Corriente y Voltaje a la salida del UPS		
5	Revisar nivel de combustible de la planta eléctrica	Adicionalmente, para monitorear los sistemas de potencia se debe revisar también el correcto funcionamiento de la planta de respaldo eléctrico. Para ello se debe monitorear regularmente los niveles de combustible y realizar simulacros periódicos de uso de la planta eléctrica.		Área de Administrativo / automático	Planta eléctrica	Componentes a monitorear identificados	Valores de Voltaje y Corriente a la salida de la Planta eléctrica y nivel de combustible	El nivel de combustible de la planta eléctrica se debe verificar semanalmente. Los simulacros de funcionamiento deben llevarse a cabo por lo menos dos veces al año.	
6	Revisar sensores de filtraciones bajo piso falso	Para monitorear las filtraciones de líquidos se deben revisar los sensores de filtraciones de líquidos ubicados bajo el piso falso para identificar filtraciones de agua o refrigerante.		Área de Administrativo / automático	Sensores de filtraciones	Componentes a monitorear identificados	Valores registrados de filtraciones		

CONTINÚA →

7	Revisar sensores de apertura de puertas de acceso	Para monitorear el error humano y el acceso del personal se deben monitorear los sensores de apertura de puertas para identificar ingresos al Centro de Cómputo.		Área de Administrativo / automático	Sensores de apertura de puertas de acceso	Componentes a monitorear identificados	Estado de apertura de puertas de acceso		
8	Revisar cámaras de video y sensores de movimiento	Adicionalmente, para monitorear el error humano y el acceso del personal se deben monitorear las cámaras de video y los sensores de movimiento para identificar daños involuntarios del personal o ingresos forzados al Centro de Cómputo.		Área de Administrativo / automático	Cámaras de video y sensores de movimiento	Componentes a monitorear identificados	Imágenes y valores registrados de movimiento		
9	Ejecutar política de control de acceso físico al centro de cómputo	Adicionalmente, para monitorear el error humano y el acceso del personal se debe verificar la ejecución de la política de control de acceso físico al Centro de Cómputo para controlar los accesos no autorizados y prevenir incidentes de seguridad física.	PROCEDIMIENTO DE SEGURIDADES CENTRO DE CÓMPUTO	Técnico de Centro de Cómputo	Bitácora de Registro de accesos del personal autorizado	Listado de accesos del personal autorizado al Centro de Cómputo	Valoración del cumplimiento de la política de control de acceso físico al Centro de Cómputo		
10	Revisar sensores de humo	Para monitorear el humo o el riesgo de incendio se deben monitorear los sensores de humo para determinar con suficiente anticipación cualquier incendio en equipos eléctricos o materiales.		Área de Administrativo / automático	Sensores de humo	Componentes a monitorear identificados	Valores registrados de humo		
11	Revisar sensores de polvo / químicos en el aire	Para monitorear los contaminantes en el aire se deben monitorear los sensores de polvo o químicos suspendidos en el aire como hidrógeno de las baterías y partículas como polvo.		Área de Administrativo / automático	Sensores de polvo / químicos en el aire	Componentes a monitorear identificados	Valores registrados de partículas de polvo / químicos en el aire monitoreados		
12	Notificar al proveedor del equipo	En caso de recibir una alarma de alguno de los equipos o actividades de monitoreo, se debe notificar al proveedor del equipo para su corrección.		Técnico de Centro de Cómputo / automático	Sistema de Alarmas y Protección	Evento que supera umbral definido o falla del equipo	Señal visual o sonora de advertencia o alarma		

4.3.7. Proceso: Adquisición y mantenimiento de la infraestructura de TI

4.3.7.1. Subproceso: Mantenimiento de hardware

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir Requerimiento	En el caso de que el mantenimiento sea correctivo el Jefe de servidores y administración de datos de y administración de datos de Infraestructura y Networking (servidores), el analista de primera línea de Service Desk (PCs) o el Jefe de procesamiento del Centro de Cómputo (AS400) recibe un requerimiento de mantenimiento a través de la herramienta de Service Desk en donde se especifique que tipo de mantenimiento		Jefe de servidores y administración de datos Infraestructura y Networking Jefe de procesamiento del Centro de Cómputo	Herramienta de Service Desk	Requerimiento vía email o vía telefónica	Requerimiento recibido en herramienta de Service Desk		Todos los requerimientos deben ser canalizados a través de la herramienta de Service Desk.	
2	Asignar requerimiento a técnico	En el caso de servidores el requerimiento se asigna, mediante la herramienta de Service Desk, al Administrador de servidores de Infraestructura y Networking. En el caso de PCs, el requerimiento se asigna al Analista de segunda línea de Service Desk. En el caso de AS400, el requerimiento se asigna al técnico de procesamiento del Centro de Cómputo.		Jefe de servidores y administración de datos Infraestructura y Networking Jefe de procesamiento del Centro de Cómputo	Herramienta de Service Desk	Requerimiento recibido en herramienta de Service Desk	Requerimiento asignado.		Los requerimientos de servidores son ejecutados por el área de Infraestructura y Networking. Los requerimientos de PCs son ejecutados por el área de Service Desk. Los requerimientos de AS400 son ejecutados por el área de Centro de Cómputo.	
3	Identificar daño reportado	Una vez que ha sido asignado el respectivo requerimiento el técnico procede a revisar físicamente el equipo para identificar el tipo de problema que presenta. En el caso de servidores pueden presentarse alarmas de disco, procesador, memorias y mother board. Para el caso de PC's pueden tener problemas de teclado, mouse, monitor, disco, memoria, procesador.		Técnico de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Requerimiento asignado.	Daño Identificado.			
		En el caso de la plataforma AS400, los problemas son detectados mediante la herramienta de monitoreo Barcelona o por mensajes críticos que envía el sistema operativo a la consola del Técnico del Centro de Computo.		Técnico de procesamiento Centro de Computo	AS400 Barcelona	Requerimiento asignado.	Daño Identificado.			

CONTINÚA →

4	Solicitar garantía del equipo	Una vez identificado el tipo de daño reportado se procede a verificar en el inventario de equipos si el mismo se encuentra en garantía o no. Si el equipo se encuentra en garantía se procede a solicitar al proveedor la garantía del mismo, dicha garantía se la hace vía telefónica o vía mail.		Técnico de servidores Infraestructura y Networking Analista de segunda línea de Service Desk		Daño Identificado.	Garantía solicitada			
		En la plataforma AS400, se reporta el problema a la línea de soporte del proveedor del servidor, en donde se asigna un número de caso para la gestión del incidente. El técnico asignado revisa y evalúa el daño y de ser necesario solicita el reemplazo de la parte afectada, si es necesario una maquina dedicada se coordina el reemplazo del hardware. Una vez que se soluciona el problema, se firma con el proveedor la hoja de trabajo en donde se especifican las horas empleadas en la actividad.		Técnico de procesamiento Centro de Computo Jefe de procesamiento Centro de Computo		Daño Identificado.	Garantía solicitada			
5	Recibir equipo con daño corregido por proveedor	El proveedor procede a entregar el equipo con el daño corregido.		Técnico de servidores Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento Centro de Computo		Equipo con garantía solicitada	Equipo con daños solucionados.			
6	Repara daño localmente	En el caso de PCs, si el daño del equipo puede ser solucionado localmente se procede a la resolución del mismo.		Analista de segunda línea de Service Desk		Equipo con problema	Equipo con daños solucionados.			
7	Solicitar repuesto	Para el caso de PC's que no están en garantía y que requieren de un repuesto se procede a solicitar al Área de Service Desk el repuesto necesario para cumplir con el requerimiento asignado.		Analista de segunda línea de Service Desk		Solicitar repuesto	Repuesto solicitado			
8	Solicitar compra	En caso de que no exista en stock la parte solicitada para corregir el daño reportado, se procede a llenar la respectiva orden de compra de la parte o equipo, debidamente autorizada, para entregar dicha orden de compra al <b>Departamento Administrativo</b> para que realice la respectiva compra.		Sub gerente de Service Desk		Orden de compra para entregar al Departamento Administrativo	Orden de compra llenada y entregada al Departamento Administrativo	requerimiento de compra de materiales y equipos formulario-equipos-nuevos		
9	Recibir repuesto nuevo	Se recibe por parte del Departamento Administrativo el equipo o parte solicitada, se verifica que sea la correcta y que este en buen estado.		Sub gerente de Service Desk		Recepción equipo o parte nueva	Equipo o parte nueva recibida y verificada			

CONTINÚA →

10	Entregar repuesto a técnico	Una vez que se ha recibido el equipo o parte por parte del Departamento de Administrativo y ha sido verificada su funcionalidad, se procede a entregar la parte o equipo al Analista de segunda línea de Service Desk para que continúe con la ejecución del requerimiento.		Sub gerente de Service Desk		Recepción equipo o parte nueva	Equipo o parte nueva recibida			
11	Registrar repuesto en inventario	Una vez reciba la parte o equipo solicitada procede al respectivo registro del mismo en el archivo de inventario en el cual se registra la parte y el número de serie.		Analista de segunda línea de Service Desk		Equipo o parte nueva recibida	Equipo o parte registrada en inventario.	Inventario de PC's de Servidores de Movimiento de Equipos o partes		
12	Recibir repuesto	El analista de segunda línea de Service Desk recibe la parte o equipo para que proceda con la solución del daño reportado.		Analista de segunda línea de Service Desk		Equipo o parte registrada en inventario.	Equipo o parte recibido			
13	Verificar planificación de mantenimientos	En el caso de que el mantenimiento sea Preventivo, se debe analizar el impacto de este mantenimiento y verificar que exista la planificación adecuada, se pueden presentar 2 casos: Para el caso de Servidores, el Jefe de servidores y administración de datos de Infraestructura y Networking, procede a analizar y verificar la factibilidad de realizar dicho mantenimiento, tomando en cuenta el impacto en los aplicativos, la hora de menos impacto hacia el usuario y el tiempo de afectación hacia el usuario.  Para el caso de PC's, el analista de primera línea Service Desk verifica con los usuarios la disponibilidad de tiempo de los usuarios para facilitar los equipos y el tiempo que se necesitaría para realizar dicho mantenimiento.		Jefe de servidores y administración de datos de Infraestructura y Networking Analista de primera línea de Service Desk		Planificación de mantenimiento	Planificación de Mantenimiento verificada y analizada			
		Para la plataforma AS400, en el caso de que el mantenimiento sea preventivo, se debe analizar el impacto mediante un plan de actividades, en el que se considera la activación de contingencia puesto que se necesita maquina dedicada, por lo que es necesario contar con la autorización de la Gerencia de Tecnología. Con la autorización aprobada se coordina con el proveedor, quien realiza las actividades de mantenimiento en los equipos con plataforma AS400, en el año se planifica dos mantenimientos.		Jefe de procesamiento de Centro de Computo Sub Gerente de Centro de Computo		Planificación de mantenimiento	Planificación de Mantenimiento verificada y analizada			

CONTINÚA →

14	Agendar mantenimiento con el usuario	Una vez que se ha verificado la factibilidad de hacer el mantenimiento se procede a agendar en conjunto con los usuarios la fecha y hora en la que se realizara dicho mantenimiento con el fin de que el usuario reciba el menor impacto posible.		Jefe de servidores y administración de datos de Infraestructura y Networking Analista de primera línea de Service Desk		Planificación de mantenimiento y factibilidad aprobadas	Agendamiento del mantenimiento con el usuario			
15	Asignar requerimiento a técnico	En el caso de mantenimiento preventivo a PCs, el analista de primera línea de Service Desk asigna un requerimiento al Analista de segunda línea de Service Desk para que ejecute dicho mantenimiento		Analista de primera línea de Service Desk		Agendamiento del mantenimiento con el usuario	Requerimiento asignado.			
16	Recibir equipo	En el caso de PCs, el Analista de segunda línea de Service Desk procede a dirigirse al puesto físico a recibir por parte del usuario el equipo al que se le va a realizar el mantenimiento planificado.		Analista de segunda línea de Service Desk		Recibir equipo para mantenimiento	Equipo para mantenimiento recibido			
17	Realizar limpieza interna y externa	Una vez que el Analista de segunda línea de Service Desk recibe el equipo procede a realizar la respectiva limpieza tanto interna como externa del equipo. En la parte interna sopletea y en la parte externa procede a limpiar con los utensilios de limpieza asignados para este propósito.		Analista de segunda línea de Service Desk		Recibir materiales para realizar la limpieza interna y externa del Equipo	Equipo limpiado interna y externamente.			
18	Realizar diagnóstico de CPU, memoria y discos	Una vez realizada la limpieza tanto externa como interna el Técnico procede a realizar un diagnóstico del buen funcionamiento del CPU, memorias y discos.		Analista de segunda línea de Service Desk		Recibir equipo limpio	Equipo revisado CPU, memoria y discos.			
19	Revisar conexiones eléctricas y de red	Se procede a la revisión física tanto de las conexiones eléctricas como de red, se revisan cables y cajetines.		Analista de segunda línea de Service Desk		Identificar las conexiones eléctricas y de red a revisar	conexiones eléctricas y de red a revisadas			
20	Revisar periféricos	Se procede a la revisión y buen funcionamiento de los periféricos que tiene el PC. Se verifica el monitor, mouse y teclado.		Analista de segunda línea de Service Desk		Identificar periféricos a revisar	Periféricos revisados			CONTINÚA →
21	Entregar equipo al usuario	En el caso de PCs, una vez realizado el mantenimiento se procede a la entrega del equipo al usuario y se realiza la verificación del equipo y sus aplicativos en compañía del usuario.		Analista de segunda línea de Service Desk		Equipo realizado mantenimiento	Equipo entregado al Usuario			
22	Cerrar requerimiento	Una vez se ha realizado el mantenimiento, se procede a dar por concluido el requerimiento y se cierra el mismo en la herramienta de Service Desk.		Analista de segunda línea de Service Desk	Herramienta de Service Desk	Equipo entregado al Usuario	Cierre del requerimiento en la Herramienta de Service Desk			

4.3.7.2. Subproceso: Mantenimiento de software

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Recibir requerimiento	El Jefe de servidores y administración de datos Infraestructura y Networking (servidores), el analista de segunda línea de Service Desk (PCs) o el Jefe de procesamiento del Centro de Cómputo (AS400) recibe un requerimiento de mantenimiento de software a través de la herramienta de Service Desk, junto con el respectivo formulario de control de cambios con las respectivas firmas de autorización.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Requerimiento asignado en herramienta de Service Desk junto al formulario de control de cambios.	Requerimiento recibido	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls	Los requerimientos de mantenimiento de software deben ser canalizados a través de Service Desk	
2	Verificar factibilidad	Se procede al análisis de factibilidad analizando si la actualización cumple con los estándares de la empresa y se revisa el impacto del requerimiento a ser ejecutado. Dentro de dicho impacto se analiza: La afectación que pueden tener dichas actualizaciones en general, el espacio en disco que pueden generar, la afectación a los servicios que preste dicho software y el horario en el que se desea realizar la afectación.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Requerimiento recibido	Dictamen de Factibilidad		Los requerimientos de servidores son ejecutados por el área de Infraestructura y Networking. Los requerimientos de PCs son ejecutados por el área de Service Desk. Los requerimientos de AS400 son ejecutados por el área de Centro de Cómputo.	
3	Notificar motivo a solicitante	En el caso de que el requerimiento no sea factible, se emite un informe al usuario solicitante indicando por qué no pudo ser atendido el requerimiento y se procede a cerrar el requerimiento en la herramienta de Service Desk.		Jefe de Servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Dictamen de Factibilidad	Informe de factibilidad y requerimiento cerrado en la herramienta de Service Desk.			

CONTINÚA →



4	Asignar requerimiento a técnico	Si el requerimiento fue aprobado, el Jefe de servidores y administración de datos de Infraestructura y Networking verifica la carga de los Técnicos y procede a re-asignar el requerimiento a través de la herramienta de Service Desk a un administrador de servidores para que el mismo sea atendido. En el caso de PCs, el requerimiento permanece en el analista de segunda línea de Service Desk. En el caso de AS400 el requerimiento permanece en el Jefe de procesamiento quien se encargara de contactar al proveedor.		Jefe de servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Re - asignación de requerimiento en herramienta de Service Desk	Requerimiento asignado en herramienta de Service Desk con formulario de control de cambios.	FORMULARIO PARA CONTROL DE CAMBIOS_v3.xls		
5	Identificar tipo de mantenimiento	Se procede a identificar el tipo de mantenimiento a realizar identificando si es una instalación nueva, una actualización o una configuración de un aplicativo.		Jefe de servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Requerimiento asignado en herramienta de Service Desk con formulario de control de cambios.	Mantenimiento Identificado			
6	Identificar SW a instalar	SI el requerimiento es de Instalación de un aplicativo se procede a la identificación del software del aplicativo. Ver listado de aplicativos permitidos en la empresa. Para los casos en donde exista un contrato con proveedor o se requiere su apoyo, se procede a contactar al proveedor para que realice el requerimiento solicitado.		Jefe de servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Mantenimiento Identificado y Formulario de control de cambios.	Software Identificado	Listado de aplicativos permitidos	Solo se permite la instalación de los aplicativos que figuran en el listado de aplicativos permitidos en Diners	
7	Obtener e instalar el SW	Una vez que se ha identificado el aplicativo a instalar se procede a la obtención de los instaladores, ya sea en el almacén de instaladores o se procede a bajarlos o solicitarles al proveedor del aplicativo		Jefe de servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Software Identificado	Software Actualizado			
8	Identificar SW a configurar	SI el requerimiento es de configuración de software se procede a la identificación del software y la identificación de los manuales del software a configurar. Ver listado de aplicativos permitidos en la empresa. Para los casos en donde exista un contrato con proveedor o se requiere su apoyo, se procede a contactar al proveedor para que realice el requerimiento solicitado.		Jefe de servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Mantenimiento Identificado y Formulario de control de cambios.	Software Identificado	aplicativos permitidos		

CONTINÚA →

9	Realizar configuración según solicitud	Una vez identificado el Software a configurar e identificado el respectivo manual se procede a la configuración de acuerdo a los parámetros indicados en el manual o recomendados por el proveedor del Software. Ver listado de aplicativos permitidos en la empresa.		Jefe de servidores Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Software manuales Identificados y	Software Actualizado			
10	Identificar SW a actualizar	SI el requerimiento es de actualización de software se procede a la identificación del Sistema Operativo a parchar (Control Tecnológico emite un informe de vulnerabilidades detectadas que deben ser corregidas). Sistemas Operativos: Windows Linux AIX VMWARE AS400  Para los casos en donde exista un contrato con proveedor o se requiere su apoyo, se procede a contactar al proveedor para que realice el requerimiento solicitado.		Jefe de servidores y administración de datos Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Mantenimiento Identificado, Formulario de control de cambios e informe de Control Tecnológico sobre vulnerabilidades	Software actualizar a identificado			
11	Obtener e instalar parches o nuevas versiones	En el caso de servidores y PCs, una vez identificado el Sistema Operativo a ser parchado y teniendo en cuenta el informe emitido por Control Tecnológico, se procede a la obtención de los respectivos parches y la instalación de los mismos.		Administrador de servidores Analista de segunda línea de Service Desk		Software actualizar a identificado	Software Actualizado			
		Para la plataforma AS400, el proveedor del sistema operativo libera dos veces al año un acumulativo de arreglos (PTFS) los cuales son correcciones a los programas del sistema operativo o bajo licencia del OS/400. El jefe de procesamiento de Centro de cómputo solicita el envío de los archivos al proveedor, quien entrega la información en medio magnético para proceder con la instalación. Una vez que se ha ejecutado normalmente, se debe coordinar las siguientes actividades en los equipos en donde se puede afectar la disponibilidad de los servicios: 1.- Reinicio del sistema (IPL) para que los arreglos se apliquen en el sistema operativo. 2.- Respaldo del sistema operativo con las actualizaciones aplicadas		Técnico de procesamiento de Centro de Computo Jefe de procesamiento de Centro de Computo		Software Identificado	Software Actualizado			

CONTINÚA →

12	Notificar y verificar funcionamiento con el usuario	Una vez que se ha realizado el mantenimiento respectivo, se procede a informar al usuario vía email o vía telefónica que el requerimiento ha sido concluido para que este proceda a la verificación del buen funcionamiento del aplicativo afectado.		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo		Software Actualizado	Software verificado por el usuario			
13	Cerrar requerimiento	Una vez que el usuario ha certificado que el aplicativo se encuentra funcional se procede a cerrar el respectivo requerimiento en la herramienta de Service Desk.		Administrador de servidores Infraestructura y Networking Analista de segunda línea de Service Desk Jefe de procesamiento de Centro de Cómputo	Herramienta de Service Desk	Software verificado por el usuario y funcional al 100%	Requerimiento cerrado en la herramienta de Service Desk			

4.3.8. Proceso: Evaluación y administración los riesgos de TI

4.3.8.1. Subproceso: Evaluación y administración los riesgos de TI

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Determinar proceso de TI a recorrer	Los riesgos críticos de TI se evidencian al recorrer los procesos asociados al área de la Operación del Servicio dado que en ellos es donde se manipula directa o indirectamente la información de producción de la organización. De esta manera se deben recorrer todos los procesos asociados al área de la Operación del Servicio para asegurar la identificación de todos los riesgos potenciales.  En este orden de ideas, cada Gerente de área (Infraestructura y Networking, Centro de Cómputo y Control Tecnológico) selecciona un proceso de su área para recorrer.  Igualmente se puede aplicar el proceso a las demás áreas de TI (Diseño y Entrega del servicio, Estrategia y Planeación del Servicio)		Gerentes de cada área de la gerencia de tecnología		Procesos del área de Operación del Servicio documentados y actualizados	Proceso identificado a recorrer para identificar sus riesgos asociados.		Todos los procesos del área de Operación del Servicio deben ser recorridos para identificar riesgos potenciales por los menos una vez al año o cada vez que se realice una modificación importante a los procesos del área.	
2	Recorrer proceso de TI	Una vez seleccionado el proceso, el Gerente junto con su equipo recorre detenidamente cada actividad del proceso en búsqueda de riesgos potenciales. Es conveniente recorrer las actividades con los directos responsables de cada actividad para aprovechar su conocimiento operativo.		Gerentes de cada área de la gerencia de tecnología		Proceso identificado a recorrer para identificar sus riesgos asociados.	Proceso recorrido			
3	Identificar los riesgos del proceso	Una vez recorrido el proceso se registran en la matriz de riesgo y controles todos los riesgos identificados en el procesos detallando claramente en que consiste cada uno. Estos riesgos pueden haber ocurrido en el pasado como también pueden ser riesgos potenciales que se identifican a priori con el ánimo de anticipar su ocurrencia y mitigar su impacto. En este orden de ideas es conveniente hacer un análisis de peor escenario con el ánimo de identificar dichos riesgos potenciales.		Gerentes de cada área de la gerencia de tecnología		Proceso recorrido	Riesgos asociados al procesos identificados y registrados en la matriz de riesgos y controles	Matriz de riesgos y controles		Se debe verificar con el área de Riesgos si cuenta con un formato de Matriz de riesgos y controles. Si no se cuenta el área de riesgos debe diseñarlateniendo en cuenta los lineamientos.
4	Identificar posibles fallas que materialicen cada riesgo	Cada riesgo identificado puede materializarse debido a diferentes fallas. Se deben entonces identificar todas aquellas fallas (o al menos las principales) que pueden causar que el riesgo se materialice y estas deben quedar debidamente registradas en la matriz de riesgos y controles. Esto se debe hacer para cada uno de los riesgos identificados en el proceso.		Gerentes de cada área de la gerencia de tecnología		Riesgos asociados al procesos identificados y registrados en la matriz de riesgos y controles	Posibles fallas que materialicen los riesgos identificados y registradas en la matriz de riesgos y controles.			

CONTINÚA →

5	Asignar probabilidad a cada riesgo	Teniendo en cuenta las posibles fallas que pueden materializar el riesgo, se debe estimar la probabilidad de ocurrencia del riesgo sin tener en cuenta los controles asociados que mitiguen dicho riesgo. La probabilidad de ocurrencia debe valorarse según la siguiente escala: muy alta, alta, moderada, baja, muy baja. Esta probabilidad debe quedar registrada para cada riesgo en la matriz de riesgos y controles.		Gerentes de cada área de la gerencia de tecnología		Posibles fallas que materialicen los riesgos identificados y registradas en la matriz de riesgos y controles.	Probabilidad estimada para cada riesgo registrada en la matriz de riesgos y controles.			
6	Asignar impacto a cada riesgo	Teniendo en cuenta las posibles fallas que pueden materializar el riesgo, se debe estimar el impacto en el negocio en caso de que el riesgo se materialice sin tener en cuenta los controles asociados que mitiguen dicho riesgo. El impacto del riesgo debe valorarse según la siguiente escala: superior, mayor, importante, menor, inferior.		Gerentes de cada área de la gerencia de tecnología		Probabilidad estimada para cada riesgo registrada en la matriz de riesgos y controles.	Impacto estimado para cada riesgo registrado en la matriz de riesgos y controles.			
7	Calcular severidad inherente a cada riesgo	De acuerdo a la combinación de impacto y probabilidad estimada para cada riesgo, se calcula la severidad inherente de cada riesgo. Esta severidad resume la criticidad inherente de cada riesgo sin tener en cuenta los controles que los mitiguen. La severidad inherente puede tener los siguientes valores: extremo, alto, moderado, bajo. La tabla de combinaciones de impacto y probabilidad que equivalen a cada valor de severidad inherente debe estar definida y aprobada previamente.		Gerentes de cada área de la gerencia de tecnología Área de Riesgos		Impacto estimado para cada riesgo registrado en la matriz de riesgos y controles.	Severidad inherente de cada riesgo registrada en la matriz de riesgos y controles.		La tabla de combinaciones de impacto y probabilidad que equivalen a cada valor de severidad debe estar definida y aprobada previamente.	El área de Riesgos debe apoyar en el diligenciamiento CONTINÚA → riesgo inherente y residual dado que dicha área se especializa en esa tarea.
8	Actualizar mapa del riesgo inherente	Una vez calculada la severidad inherente de cada riesgo, se procede a mapear el riesgo en el mapa de riesgo inherente. El mapa de riesgo inherente constituye una gráfica que mide en el eje vertical la probabilidad de ocurrencia y en el eje horizontal el impacto de cada riesgo. Esto conlleva a un gráfico matriz de 5x5 en donde cada casilla representa una de las posibles combinaciones de impacto y probabilidad. Cada una de estas casillas de tener asociado un nivel de severidad inherente según la escala definida previamente. Este mapa facilita la visualización de los riesgos identificados y su severidad correspondiente.		Gerentes de cada área de la gerencia de tecnología Área de Riesgos		Severidad inherente de cada riesgo registrada en la matriz de riesgos y controles.	Mapa de riesgo inherente actualizado	Mapa de riesgo inherente		El área de Riesgos debe apoyar en la actualización del mapa de riesgo inherente y residual.
9	Identificar controles de mitigación para cada falla	Con el ánimo de mitigar las posibles fallas que pueden materializar los riesgos identificados, se deben establecer controles para cada falla detectada. Aquí se detalla el objetivo del control en las actividades que lo componen (quién, qué, cómo, dónde, cuándo). Incluye su documentación (manuales, circulares, procedimientos) y su importancia.		Gerentes de cada área de la gerencia de tecnología		Mapa de riesgo inherente actualizado	Controles identificados para cada falla identificada y debidamente registrados en la matriz de riesgos y controles			

CONTINÚA →

10	Determinar solidez de cada control individualmente	La solidez de cada control es función de una serie de variables que determinan la calidad del control. Se deben tener en cuenta las siguientes variables: Responsable del control, tipo de control (preventivo o correctivo), naturaleza del control (automático, semiautomático o manual), frecuencia, documentación (documentado o no documentado), ejecución del control (fuerte, moderada o débil). De acuerdo a una tabla de valores predefinida que tiene en cuenta las distintas combinaciones de las variables mencionadas, se calcula la solidez individual de cada control con el siguiente rango: fuerte, moderado o débil.		Gerentes de cada área de la gerencia de tecnología Área de Riesgos		Controles identificados para cada falla identificada y debidamente registrados en la matriz de riesgos y controles	Solidez individual de cada control para cada falla identificada y registrada en la matriz de riesgos y controles.		La tabla de combinaciones de las variables que componen un control y que equivalen a cada valor de solidez individual de control debe estar definida y aprobada previamente.	El área de Riesgos debe apoyar en el cálculo de la solidez de los controles así como en la definición de las tablas de valores que determinan los resultados de solidez.
11	Determinar solidez del conjunto de controles para cada riesgo	Una vez calculada la solidez de cada control que mitigan las fallas correspondientes a un riesgo determinado, se procede a calcular la solidez del conjunto de controles de dicho riesgo. Esta solidez conjunta se determina a partir de una serie de criterios que se deben definir para ponderar el efecto conjunto de mitigación del riesgo. Esto se debe realizar para cada riesgo identificado y debe quedar debidamente registrado en la matriz de riesgos y controles.		Gerentes de cada área de la gerencia de tecnología Área de Riesgos		Solidez individual de cada control para cada falla identificada y registrada en la matriz de riesgos y controles.	Solidez conjunta de los controles que mitigan cada riesgo identificado y registrada en la matriz de riesgos y controles.		Los criterios utilizados para determinar cada valor de solidez conjunta deben estar definidos y aprobados previamente.	El área de Riesgos debe apoyar en el cálculo de la solidez de los controles así como en la definición de las tablas de valores que determinan los resultados posibles de solidez.
12	Asignar nuevo impacto a cada riesgo	Teniendo en cuenta la solidez del conjunto de controles que mitigan cada riesgo identificado, se debe estimar la nueva probabilidad de ocurrencia de cada riesgo asumiendo que los controles pueden disminuir dicha probabilidad. La probabilidad de ocurrencia debe valorarse según la siguiente escala: muy alta, alta, moderada, baja, muy baja. Esta probabilidad debe quedar registrada para cada riesgo en la matriz de riesgos y controles.		Gerentes de cada área de la gerencia de tecnología		Solidez conjunta de los controles que mitigan cada riesgo identificado y registrada en la matriz de riesgos y controles.	Probabilidad estimada para cada riesgo teniendo en cuenta los controles identificados y registrada en la matriz de riesgos y controles.			
13	Asignar nueva probabilidad a cada riesgo	Teniendo en cuenta las posibles fallas que pueden materializar el riesgo, se debe estimar el impacto en el negocio en caso de que el riesgo se materialice sin tener en cuenta los controles asociados que mitiguen dicho riesgo. El impacto del riesgo debe valorarse según la siguiente escala: superior, mayor, importante, menor, inferior. Este impacto debe quedar registrado para cada riesgo en la matriz de riesgos y controles.		Gerentes de cada área de la gerencia de tecnología		Probabilidad estimada para cada riesgo teniendo en cuenta los controles identificados y registrada en la matriz de riesgos y controles.	Impacto estimado para para cada riesgo teniendo en cuenta los controles identificados y registrado en la matriz de riesgos y controles.			

CONTINÚA →

14	Calcular severidad residual de cada riesgo	De acuerdo a la combinación de impacto y probabilidad estimada teniendo en cuenta los controles identificados para cada riesgo, se calcula la severidad residual de cada riesgo. Esta severidad resume la criticidad restante de cada riesgo al aplicar los controles que los mitiguen. La severidad residual puede tener los siguientes valores: extremo, alto, moderado, bajo. La tabla de combinaciones de impacto y probabilidad que equivalen a cada valor de severidad residual debe estar definida y aprobada previamente. La severidad residual debe quedar registrada en la matriz de riesgos y controles para cada riesgo identificado.		Gerentes de cada área de la gerencia de tecnología Área de Riesgos		Impacto estimado para cada riesgo teniendo en cuenta los controles identificados y registrado en la matriz de riesgos y controles.	Severidad residual de cada riesgo registrada en la matriz de riesgos y controles.		La tabla de combinaciones de impacto y probabilidad que equivalen a cada valor de severidad residual debe estar definida y aprobada previamente.	El área de Riesgos debe apoyar en el diligenciamiento y cálculo del riesgo inherente y residual dado que dicha área se especializa en esa tarea.
15	Actualizar mapa del riesgo residual	Una vez calculada la severidad inherente de cada riesgo, se procede a mapear el riesgo en el mapa de riesgo inherente. El mapa de riesgo inherente constituye una gráfica que mide en el eje vertical la probabilidad de ocurrencia y en el eje horizontal el impacto de cada riesgo. Esto conlleva a un gráfico matriz de 5x5 en donde cada casilla representa una de las posibles combinaciones de impacto y probabilidad. Cada una de estas casillas de tener asociado un nivel de severidad inherente según la escala definida previamente. Este mapa facilita la visualización de los riesgos identificados y su severidad correspondiente.		Gerentes de cada área de la gerencia de tecnología Área de Riesgos		Severidad residual de cada riesgo registrada en la matriz de riesgos y controles.	Mapa de riesgo residual actualizado			El área de Riesgos debe apoyar en la actualización del mapa de riesgo inherente y residual dado que dicha área se especializa en esa tarea.

4.3.9. Proceso: Garantizar la seguridad de los sistemas

4.3.9.1. Subproceso: Administración de la seguridad de la información

#	Actividad	Descripción	Manuales de Detalle	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Revisión de Claves Administrativas	<p>Se tiene definido un calendario de revisión para realizar el cambio de contraseñas administrativas de los equipos de la organización, con la finalidad de identificar aquellas que deben modificarse por vencimiento de fecha de retención, o en su defecto por apertura de sobre cerrado.</p> <p>Este proceso consiste en que el analista de Control Tecnológico realiza la verificación de las contraseñas y el ingreso dual de una clave, para aquellos equipos que deben ser modificados a nivel de contraseña administrativa, se debe contactar con la contraparte responsable de los servidores, para realizar el ingreso de clave duada en los equipos que están siendo actualizados.</p>	<p>procedimiento de uso y cambios de contraseñas administrativas y emergentes.doc</p>	Analista Control Tecnológico	Sistemas en donde se ha ejecutado el cambio de clave	<p>Cronograma de revisión.</p> <p>Bitácora de inventario de claves administrativas.</p>	<p>Bitácora de inventario de claves administrativas actualizada.</p> <p>Sobre con nuevas claves duadas.</p>	<p>inventariodeclavesadministrativas.xls</p> <p>Bitácora Registro Ccomputo.xls</p> <p>formulario para claves de seguridad.xls</p> <p>documento de custodia de contraseñas administrativas.doc</p>	El calendario de revisión de claves administrativas se debe generar anualmente durante el mes de enero.	
2	Configuración de llaves de encriptación para cajas Atalla	<p>Este procedimiento se realiza por única vez en la adquisición de equipos para encriptación de transacciones, PIN (número de identificación personal) y CVV (Código verificador) de tarjetahabientes o en el caso de adquirir una nueva marca de tarjeta de crédito para difusión en el país.</p> <p>Este proceso consiste en el ingreso de algoritmos de cifrado en estándar 3DES proporcionado por las marcas internacionales VISA, MASTERCARD, DINERS, DISCOVER, para la transaccionalidad con las tarjetas otorgadas a los tarjetahabientes de forma segura. La configuración del algoritmo de cifrado se realiza en conjunto con los representantes de las áreas de Control Tecnológico (Analista), Riesgos (Oficial) y Auditoría (Auditor de Sistemas).</p>	<p>instructivo para activación de contingencia de caja atalla.doc</p> <p>procedimiento para ingreso de mfk en caja atalla.doc</p> <p>procedimiento para ingreso de llaves en caja atalla.doc</p>	<p>Analista Control Tecnológico</p> <p>Oficial de Riesgos</p> <p>Auditor de Sistemas</p> <p>Supervisor Centro Cómputo</p> <p>Técnico Networking</p>	Cajas Atalla	Componentes de cifrado de las marcas Visa, MasterCard, Diners, Discover internacional.	Claves de cifrado por marca para transaccionalidad y aseguramiento de encriptación de la transacción.	<p>Anexo 3 Acta de entrega.doc</p> <p>Anexo 1 Acta ingreso llaves ATALLA.doc</p>		

CONTINÚA →



3	Cifrado de Discos	Se tiene desarrollado un cronograma de implementación de cifrado de discos a nivel de la organización de acuerdo a la criticidad de la información que se almacena en cada estación de trabajo por áreas, adicionalmente se cuenta con un reporte entregado por el área de Riesgos para cifrar estaciones de trabajo de manera urgente por la criticidad del negocio.	inscripción de estaciones de trabajo dlp.doc  GuíaTécnicos Recuperación DLP.doc	Analista Control Tecnológico  Técnico Service Desk	McAfee DLP  Sophos	Cronograma de implementación de encripción.  Reporte del área de Riesgos para cifrado de equipos críticos.	Equipos cifrados.  Notificación de equipos cifrados vía mail al área de Riesgos.		El área de Service Desk debe entregar un informe de estado de los equipos a cifrar.	
4	Administración e impresión de sobreflex	Permite generar la información para la impresión de sobreflex de visa Banco.  Este proceso consiste en la generación de pines (código de 4 dígitos para activación de tarjeta de crédito) para imprimirse en los sobreflex que almacenarán la tarjeta de crédito que se entregará a los tarjetahabientes.  El operador del Centro de Cómputo, recibe los sobres para impresión de pines y registra en la bitácora la fecha, hora y cantidad de sobres que ha recibido del analista de Control Tecnológico y procede a imprimir los pines que se han entregado para enviarlos al área de la Datacard.	procedimiento impresión de pines dn.doc  procedimiento impresión de pines bp.doc	Gerente Control Tecnológico  Analista Control Tecnológico  Operador Centro de Cómputo	AS400 Gestor Producción  SFTP/Banco Pichincha	Requerimiento vía mail del área de Operaciones para impresión de pines.  Bases de tarjetas para impresión de pines.	Archivo generado de pines para impresión.  Entrega de sobreflex para impresión			
5	Entrega de claves para generación de pines	Permite generar claves de 4 dígitos para entregarlos a los tarjetahabientes para que realicen el cambio de contraseña en el caso de bloqueo u olvido.  Este proceso consiste en habilitar el acceso del personal autorizado del Call Center de bancos asociados y propios a la opción asignada para generar automáticamente claves para ser entregadas vía telefónica a los tarjetahabientes que por determinadas circunstancias han bloqueado o han olvidado su contraseña.		Técnico Service Desk  Analista Control Tecnológico	AS400 Gestor Producción	Requerimiento asignado en la herramienta de Service Desk.	Entrega de clave a solicitante y registro de clave en bitácora.	Usuarios Call Center Visa BP pines.xls  Asignación de PINES.xls	Cualquier requerimiento de entrega de pines debe pasar por el control de preguntas de validación de identidad para entregar la clave.	La herramienta de Service Desk debe permitir escalar los requerimientos a través de un flujo de trabajo predefinido.
6	Administración de certificados digitales	Permite realizar el cambio e instalación de certificados digitales para los servidores que se conectan con los AS400 para el aseguramiento de transacciones de compra mediante páginas web.	procedimiento y manual de usuario para la administración de certificados digitales.doc	Analista Control Tecnológico  Técnico Networking  Técnico Desarrollo	Open SSL	Inventario de registro de fechas de caducidad del certificado.	Implementación de actualización de certificado o de nuevo certificado en producción.		Se debe contar con la autorización del área de Desarrollo para proceder a la bajada del certificado y la instalación del nuevo certificado digital.	

CONTINÚA →

7	Análisis de cumplimiento PCI para comercios	<p>Permite identificar si los comercios que se asocian para transaccional con Diners-Ínterin cumplen los requisitos mínimos de seguridad definidos por la normativa PCI DES.</p> <p>En este proceso se realiza una evaluación del comercio en base a un checolista proporcionado por la organización PCI DES, para verificar si los comercios solicitantes cuentan con las seguridades adecuadas para transmisión y almacenamiento de información del tarjetahabiente. El analista de Control Tecnológico se encarga de verificar la información proporcionada mediante el checolista, basándose en una matriz de ponderación de cumplimiento. Con este trabajo se genera una evaluación del estado del comercio y esta es remitida al solicitante junto con una carta en donde se especifica si se acepta o no su vinculación en base al resultado obtenido en la calificación de cumplimiento de la normativa.</p>	<p>pci_dss.pdf</p> <p>MatrizRevisión_v1.4.xls</p>	Analista Control Tecnológico		Cuestionario de cumplimiento PCI DES para comercios.	<p>Informe de evaluación de cuestionario de cumplimiento de normativa PCI DES para comercios.</p> <p>Carta de rechazo o aceptación del cumplimiento a la normativa.</p>	pci_saq_d_v2_ES_Cuestionario.doc (cuestionario proporcionado a comercios para autoevaluación)	Sin la carta de certificación de cumplimiento de la normativa PCI DES dirigida al comercio no se puede iniciar o actualizar la relación comercial.	
---	---------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------	------------------------------	--	------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------	--

4.3.9.2. Subproceso: Monitoreo de seguridad

#	Actividad	Descripción	Manuales de Detalle	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Determinar componente a monitorear	El analista de Control Tecnológico como parte de sus funciones diarias, debe ingresar a la consola de seguridad de las herramientas que tiene bajo su cargo y realizar una revisión del estado de cumplimiento de políticas y alertas generadas en los mismos y presentarlas en el informe.	procedimiento de monitoreo de eventos de seguridad.doc	Analista Control Tecnológico Gerente Control Tecnológico	Todas la herramientas de monitoreo de seguridad	Necesidad de monitoreo de seguridad	Componente a monitorear identificado	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
2	Monitorear accesos, pasos a producción y contraseñas	El analista de Control Tecnológico, ingresa a la herramienta y genera un reporte con un corte de tiempo determinado para realizar la revisión de las alertas que se han generado en dicho periodo. Por cada una de las políticas de seguridad de control de accesos se revisa y genera datos para el informe gerencial. Transferencias: El analista ingresa a la herramienta Barcelona04, sección Política transferencias AS400, filtra los registros por todos los que aparecen en color rojo y evalúa los tipos de violación a la política, si se trata de violaciones graves genera un informe que se entrega a la gerencia de Control Tecnológico para las acciones correspondientes.	procedimiento de monitoreo de eventos de seguridad.doc	Analista Control Tecnológico	Barcelona04	Componente a monitorear identificado	Estadísticos de revisión de Barcelona04	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
3	Monitorear Vulnerabilidades en la red	El analista de Control Tecnológico ingresa a la herramienta McAfee Secure y ejecuta en la consola de administración la opción para búsqueda de vulnerabilidades en la red interna y externa. La herramienta genera un reporte que es enviado al gestor de eventos de Service Desk para que solvante los problemas identificados en caso dado. El analista de Control Tecnológico por cada punto de vulnerabilidad presentado en el reporte solicita la fecha de solución, a la que debe hacerle un seguimiento en los plazos y términos acordados para la remediación de los problemas identificados. En este seguimiento el analista también evalúa el estado de las remediaciones que deben implantarse como resultado del Ethical Hacking realizado a la red de la organización.	procedimiento de monitoreo de eventos de seguridad.doc  procedimiento y manual de usuario para revisión y remediación de vulnerabilidades.doc	Analista Control Tecnológico	McAfee Secure	Componente a monitorear identificado	Estadísticos de revisión de McAfee Secure	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
4	Monitorear accesos remotos (VPN)	El analista de Control Tecnológico debe ingresar a la consola de la herramienta VPN SSL para revisar el log de eventos tanto del equipo como de usuarios conectados, además de verificar la validez de los certificados incluidos en la conexión como factor de autenticación.  El monitoreo consiste en revisar errores de conexión, fecha de ingreso, tiempo de uso de sesión de cada uno de los usuarios registrados en el sistema VPN SSL, donde la información recopilada es procesada manualmente para presentar en el informe semanal.	estándar de configuración de doble factor v1.doc  manual de administración de vpn ssl v1.doc	Analista Control Tecnológico	Juniper VPN	Componente a monitorear identificado	Estadísticos de revisión de Juniper VPN	Formulario para Acceso VPN.xls  Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		

CONTINÚA →

5	Monitorear Detección de intrusos	<p>El analista de Control Tecnológico debe ingresar a la consola de la herramienta Site Protector IPS, en donde identificará los tipos de ataques que se han recibido a través de la red interna como externa.</p> <p>El IPS brinda seguridad perimetral a través de la red interna mediante el acceso a los servidores por la DMZ. A nivel de la red externa e internet mediante la configuración de los equipos para proteger a los Firewalls.</p> <p>El monitoreo consiste en evaluar las alertas que se presentan en la consola.</p>	manual de administración ips.doc	Analista Control Tecnológico	Site Protector IBM	Componente a monitorear identificado	Estadísticos de revisión de Site Protector	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
6	Monitorear Ataques web	<p>El analista de Control Tecnológico debe ingresar a la consola de la herramienta WAF (web application firewall), en donde identificará los diferentes tipos de ataques que han recibido los portales web para acceso de clientes mediante internet.</p> <p>Este monitoreo consiste en la evaluación de las alertas que se presentan en la consola detallar el tipo de problema y su solución.</p>	manual de usuario waf.doc	Analista Control Tecnológico	WAF	Componente a monitorear identificado	Estadísticos de revisión de WAF	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
7	Monitorear Fuga de información confidencial	<p>El gerente de Control Tecnológico ingresa a la consola de administración de McAfee en donde selecciona el appliance "Discover" y en la sección de administración selecciona el tipo de red que se va a evaluar.</p> <p>El gerente de Control Tecnológico elimina la información confidencial de los equipos identificados.</p>		Gerente Control Tecnológico	Discover McAfee DLP	Componente a monitorear identificado	Estadísticos de revisión de Discover McAfee DLP	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
8	Monitorear Periféricos	<p>El analista de Control Tecnológico ingresa a la consola de administración de la herramienta McAfee DLP e ingresa a la sección de supervisión en donde revisa el reporte de accesos a dispositivos removibles. De este reporte filtra los intentos de accesos a equipos no autorizados, así como filtra los ingresos de usuarios autorizados por tipo de dato archivos con contenido cédula. De esa información genera un reporte que es presentado a la gerencia de Control Tecnológico para su revisión y análisis.</p>	procedimiento de habilitación de puertos dlp.doc	Analista Control Tecnológico	McAfee DLP	Componente a monitorear identificado	Estadísticos de revisión de McAfee DLP	Levantamiento Incidencias Tecnología.xls  Informe semanal.ppt		
9	Verificar alarmas visuales generadas por la herramienta	<p>En las herramientas de seguridad que tienen habilitada la opción de presentación de alarmas visuales se debe ingresar diariamente y verificar todas las alarmas que tienen prioridad crítica.</p>		Analista Control Tecnológico	Las herramientas han sido detalladas en la parte superior	Estadísticos de revisión de herramientas de seguridad	Alarmas visuales verificadas			

CONTINÚA →

10	Verificar correos generados por la herramienta	Los analistas de Control Tecnológico deben revisar los correos que se receiptan de acciones de administradores que acceden a las aplicaciones y compararlas con las solicitudes de acceso entregadas a la gerencia de Control Tecnológico, en el caso en que se identifique el acceso de usuarios que no han formalizado el ingreso a los aplicativos.		Analista Control Tecnológico	Las herramientas han sido detalladas en la parte superior	Estadísticos de revisión de herramientas de seguridad	Correos de alarma verificados			
11	Verificar logs generados por la herramienta	Los analistas de Control Tecnológico deben revisar los logs de las aplicaciones y sistemas que se han cargado en la herramienta Barcelona04.		Analista Control Tecnológico		Estadísticos de revisión de herramientas de seguridad	Logs verificados			
12	Notificar al gestor de eventos	En caso de detectar un evento de seguridad, el analista debe informar el evento al área de Service Desk, quien a su vez se encarga de gestionar el evento con el gestor de eventos de Service Desk o con el área solucionadora según sea el caso.		Analista Control Tecnológico	Herramienta de Service Desk	Evento de seguridad	Notificación a Service Desk			
13	Elaborar informe semanal con novedades	Los analistas de Control Tecnológico encargados de las herramientas de seguridad, ingresan a cada uno de los aplicativos y exportan la información de monitoreo a hojas xls, para manualmente generar la información estadística que será presentada en el informe semanal.		Analista Control Tecnológico		Estadísticos de revisión de herramientas de seguridad	Informe semanal			
14	Enviar informe a Gerencia Control Tecnológico	Los analistas envían los informes al gerente de Control Tecnológico. El gerente de Control Tecnológico se encarga de consolidar la información generada por cada analista y las entrega a la gerencia de Tecnología para su revisión.		Analista y Gerente Control Tecnológico		Reportes entregados por los analistas	Informe semanal	Informe semanal.ppt		

4.3.9.3. Subproceso: Paso a producción

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Gestión de la liberación e implementación	Este proceso es ejecutado por el área de Desarrollo y comprende todo el procedimiento para la liberación de fuentes, objetos, SQLs, que dicha área realiza.	"Gestión de la Liberación e Implementación"	Área de Diseño del Servicio						
2	Recibir de Desarrollo el requerimiento de paso a producción	El gerente de Control Tecnológico recibe el requerimiento de atención para paso a producción del área de Desarrollo con la documentación necesaria para revisión y análisis.	procedimiento de control de cambio.doc	Gerente Control Tecnológico	Herramienta Service Desk.	Requerimiento creado en herramienta y documentación habilitante física y digital.	Requerimiento creado en herramienta y documentación habilitante física y digital revisadas.	formularios de traslados a pruebas y produccion_web.xls  formularios de traslados a pruebas y producción v1.xls	Sin número de requerimiento y formulario detallado específicamente no se atiende la solicitud.	Automatizar mediante un flujo workflow los formularios que requieren autorizaciones en la herramienta de Service Desk.
3	Verificar documentación de soporte aprobada	El gerente de Control Tecnológico revisa la documentación verificando principalmente que se adjunte el documento funcional en donde se detalla el motivo del paso a producción, así como el correo del área solicitante que ha identificado el problema. En el formulario de paso a producción en cambio, se revisa que se tengan las firmas de autorización de todas las personas involucradas.	procedimiento de control de cambio.doc	Gerente Control Tecnológico	Herramienta Service Desk.	Requerimiento creado en herramienta y documentación habilitante física y digital revisadas.	Verificación de firmas de autorización en documentos físicos.			
4	Devolver documentación a desarrollo notificando motivo	Si la documentación no se encuentra completa:  El supervisor de Control Tecnológico devuelve el requerimiento junto con la documentación recibida, cierra la atención del requerimiento y envía una notificación al área de Desarrollo y explica las razones por las que no se procede a atender la solicitud.		Gerente Control Tecnológico	Herramienta Service Desk.	Verificación de firmas de autorización en documentos físicos.	Documentación incompleta respecto a firmas de autorización.			La notificación debería enviarse automáticamente a través de la herramienta workflow de Service Desk.
5	Enviar requerimiento y documentación a auditor de seguridad	Si la documentación se encuentra completa:  El gerente de Control Tecnológico envía el requerimiento al auditor de seguridad a través de la herramienta de Service Desk junto con la documentación de soporte debidamente revisada.		Gerente Control Tecnológico	Herramienta Service Desk.	Verificación de firmas de autorización en documentos físicos.	Requerimiento asignado a auditor de seguridad en herramienta y documentación habilitante física y digital autorizada.			Se debe crear el perfil Auditor de Seguridad en el área de Control Tecnológico ya que actualmente no existe como rol.
6	Recibir requerimiento y documentación de paso a producción	El auditor recibe el requerimiento y la documentación de paso a producción para su análisis correspondiente.		Auditor Control Tecnológico	Herramienta Service Desk.	Requerimiento creado en herramienta y documentación habilitante física y digital autorizada.	Validación de documentos habilitantes para paso a producción y plan de implementación.			

CONTINÚA →

7	Revisar y analizar plan de la solicitud	El auditor revisa la documentación presentada y analiza cada punto del plan de implementación previa la autorización, parte de esta revisión incluye y no se limita a verificar el código fuente con la finalidad de identificar que no se inyecte código malicioso, sqls no autorizados o programas fuente que no hayan sido autorizados para el paso a producción.		Auditor Control Tecnológico	Herramienta Service Desk.	Validación de documentos habilitantes para paso a producción y plan de implementación.	Verificación de plan de implementación de código fuente.			
8	Devolver documentación a desarrollo notificando motivo	Si existen inconsistencias en la documentación recibida:  El auditor de Control Tecnológico devuelve el requerimiento al área de Desarrollo y lo cierra adjuntando un informe sobre las inconsistencias encontradas.		Auditor Control Tecnológico	Herramienta Service Desk.	Verificación de plan de implementación y prueba de código fuente.	Devolución de requerimiento y documentos habilitantes por inconsistencias encontradas.			
9	Certificar documentación de paso a producción	Si no existen inconsistencias en la documentación recibida:  El auditor de Control Tecnológico certifica que las pruebas de seguridad realizadas para los objetos, sqls, fuentes fueron aprobadas, mediante un informe de resultados.		Auditor Control Tecnológico	Herramienta Service Desk.	Verificación de plan de implementación y prueba de código fuente.	Certificación de pasos a producción vía mail.			
10	Notificar y enviar requerimiento a supervisor	El auditor de Control Tecnológico envía el requerimiento al gerente de Control Tecnológico para que se ejecute el paso a producción a través de la herramienta de Service Desk		Auditor Control Tecnológico	Herramienta Service Desk.	Certificación de pasos a producción vía mail.	Requerimiento enviado al supervisor a través de la herramienta de Service Desk			
11	Asignar requerimiento a analista de Control Tecnológico	El gerente de Control Tecnológico con la certificación del auditor asigna el requerimiento a un analista de Control Tecnológico para su atención.		Gerente Control Tecnológico	Herramienta Service Desk.	Requerimiento enviado al supervisor a través de la herramienta de Service Desk junto con documentación habilitante.	Requerimiento asignado a analista.			
12	Enviar documentación a analista de Control Tecnológico	El gerente de Control Tecnológico envía la documentación proporcionada por el área de Desarrollo junto con el informe entregado por el auditor, al analista para su atención.		Gerente Control Tecnológico		Requerimiento asignado a analista.	Entrega de documentación habilitante.			
13	Recibir el requerimiento junto con la documentación	El analista de Control Tecnológico recibe la documentación, revisa la solicitud e ingresa en los ambientes en donde se va a realizar el paso a producción, dependiendo del tipo de solicitud, ingresará como usuario administrador, notificando a todo el personal del área de Control Tecnológico sobre el uso de la clave administrador.		Analista Control Tecnológico	Herramienta Service Desk.	Entrega de documentación habilitante.	Inicialización para atención de requerimiento y preparación de ambientes en base a documentación habilitante.			

CONTINÚA →

14	Obtener respaldos según plan de paso a producción	Previa la ejecución del paso a producción solicitado, el analista genera los respaldos de los objetos o fuentes que se encuentran actualmente funcionando		Analista Control Tecnológico	Herramienta Service Desk.	Ambientes para ejecución de paso a producción. Preparación de plan de implementación.	Obtención de respaldos de ambientes sobre los que se va a pasar a producción.			
15	Ejecutar procedimiento de paso a producción según plan	El analista de Control Tecnológico debe seguir los pasos detallados en el documento plan de implementación proporcionado por el desarrollador y para cualquiera de los casos detallados a continuación realizar los siguientes pasos: Pasos desarrollo a producción.- Pasar los objetos y fuentes del ambiente de desarrollo a producción. Pasos pruebas a producción.- Pasar los objetos y fuentes del ambiente de pruebas y producción colocando las librerías de destino en el orden indicado por el área de Desarrollo.	procedimiento de traslado de desarrollo a produccion.doc  procedimiento de traslado de pruebas a produccion.doc	Analista Control Tecnológico	AS400  CRM  Aplicaciones WEB	Obtención de respaldos de ambientes sobre los que se va a pasar a producción.	Ejecución de pasos a producción de acuerdo a plan de implementación.	formularios de traslados a pruebas y produccion_web.xls  formularios de traslados a pruebas y producción v1.xls		
16	Verificar resultado del procedimiento	El analista de Control Tecnológico por cada paso a producción realizado ingresa al spool del AS400 para capturar las pantallas de resultados de los procesos ejecutados, esta información será remitida al área de Desarrollo.		Analista Control Tecnológico	AS400 CRM Aplicaciones WEB	Ejecución de pasos a producción.	Validación de resultados en cada ambiente de paso a producción.			
17	Otorgar permisos necesarios según plan	Si no existen errores en el paso a producción:  El analista de Control Tecnológico en el caso de pasos de objetos o fuentes al ambiente de producción debe dar permisos (autorizaciones) para que estos elementos puedan ser accedidos en modo consulta por los Desarrolladores.	procedimiento de traslado de desarrollo a produccion.doc	Analista Control Tecnológico	AS400  CRM  Aplicaciones WEB	Validación de resultados en cada ambiente de paso a producción.	Dar autorizaciones sobre los objetos o fuentes pasados a producción.			
18	Abortar plan de ejecución	Si existen errores en el paso a producción: El analista de Control Tecnológico suspende el paso a producción que se encuentra realizando, captura las pantallas con los errores generados por el paso a producción y elabora un informe de incidencias, para entregarlo vía mail a los participantes.		Analista Control Tecnológico	AS400  CRM  Aplicaciones WEB	Validación de resultados en cada ambiente de paso a producción.	Suspensión de paso a producción y recopilación de pantallas de error.			
19	Ejecutar roll back según plan de paso a producción	El analista de Control Tecnológico ejecuta el plan de roll back (marcha atrás), detallado en el plan de implementación, para recuperar la operatividad de las aplicaciones regresando al estado anterior.		Analista Control Tecnológico	AS400  CRM  Aplicaciones WEB	Suspensión de paso a producción y recopilación de pantallas de error.	Aplicación de rollback de documento plan de implementación.			

CONTINÚA →



20	Notificar a analista desarrollador el resultado de ejecución del paso	En el caso en que hayan existido errores durante la ejecución del paso. El analista de Control Tecnológico notifica al técnico desarrollador las incidencias ocurridas durante el paso a producción, adjuntando el informe con las capturas de pantallas. En el caso en que el paso se haya ejecutado con éxito. El analista de Control Tecnológico notifica al técnico desarrollador la ejecución satisfactoria del mismo.		Analista Control Tecnológico		Notificar el resultado del paso.	Envío de notificación de estado del paso a producción.			
21	Notificar a supervisor sobre estado de paso a producción	El analista de Control Tecnológico tanto en el caso de ejecución exitosa, como en el caso de errores notifica al gerente de Control Tecnológico sobre el estado del requerimiento asignado, detallando los problemas encontrados.		Analista Control Tecnológico		Envío de notificación de estado del paso a producción.	Mail de notificación de ejecución de paso a producción.			
22	Archivar documentación de soporte	El analista de Control Tecnológico archiva la documentación soporte con las firmas de autorización en las carpetas correspondientes que serán almacenadas en la bodega, para su posterior entrega en casos de auditoría.		Analista Control Tecnológico	Herramienta Service Desk.	Mail de notificación de ejecución de paso a producción.	Archivo de documentación habilitante en bodega.			
23	Cerrar requerimiento	El analista de Control Tecnológico cerrará el requerimiento en la herramienta de Service Desk.		Analista Control Tecnológico	Herramienta Service Desk.	Archivo de documentación habilitante en bodega.	Cierre de requerimiento en herramienta de Service Desk			

4.3.9.4. Subproceso: Solicitud de respaldos

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Recibir solicitud de respaldos	El gerente del área de Control Tecnológico, recibe el requerimiento ingresado por la herramienta de Service Desk para la solicitud de respaldos, por medio de un mail de solicitud y un formulario físico de aprobación de la Gerencia solicitante o su delegado, para asignarlos a un analista.	procedimiento de solicitud de respaldos.doc	Gerente Control Tecnológico	Herramienta Service Desk	Mail solicitud respaldos y Formulario físico enviado por la Gerencia solicitante.	Mail solicitud respaldos y Formulario físico recibido.	FORMULARIO DE SOLICITUD DE RESPALDOS.xls	Todas las solicitudes se deben canalizar a través del Service Desk.	
2	Verificar que la solicitud sea consistente y esté autorizada	El gerente de Control Tecnológico identifica el tipo de solicitud de respaldo y verifica que el formulario físico incluya las debidas aprobaciones de la Gerencia solicitante.	procedimiento de solicitud de respaldos.doc	Gerente Control Tecnológico		Mail solicitud respaldos y Formulario físico recibido.	Formulario revisado con las debidas firmas de autorización			El formulario debe automatizarse para que se adjunten las autorizaciones mediante un flujo workflow.
3	Devolver al solicitante la solicitud incompleta	En el caso en que la documentación no esté completa:  El gerente de Control Tecnológico devuelve la solicitud al área solicitante explicando en detalle las razones por las que no se tramitará su requerimiento y cierra el requerimiento.		Gerente Control Tecnológico	Herramienta Service Desk	Formulario revisado con las debidas firmas de autorización	Mail de notificación de no atención de requerimiento.			El correo de notificación se debe generar automáticamente mediante la herramienta de workflow de Service Desk.
4	Aprobar solicitud	En el caso en que la documentación se encuentre completa: El gerente de Control Tecnológico traslada el requerimiento al analista de Control Tecnológico con la documentación física autorizada.	procedimiento de solicitud de respaldos.doc	Gerente Control Tecnológico	Herramienta Service Desk	Formulario revisado con las debidas firmas de autorización	Requerimiento generado, mail solicitud respaldos y Formulario físico recibido.			
5	Asignar requerimiento a un analista	El gerente de Control Tecnológico asigna a un analista la atención de esta solicitud, basándose en la cantidad de tareas que tiene pendientes de resolución.	procedimiento de solicitud de respaldos.doc	Gerente Control Tecnológico	Herramienta Service Desk	Requerimiento generado, mail solicitud respaldos y Formulario físico recibido.	Requerimiento por atender.			
6	Identificar lugar de almacenamiento del respaldo	El analista de Control Tecnológico debe identificar el lugar donde se encuentra almacenada la cinta de respaldo solicitado, basándose en la bitácora de registro, realiza la identificación del lugar y del tipo de respaldo (diario, semanal, mensual).	procedimiento de solicitud de respaldos.doc	Analista Control Tecnológico		Requerimiento por atender.	Revisión de bitácora de custodia.	CONTROL DE CINTAS WACKENHUT.xls		
7	Obtener el respaldo del sitio de almacenamiento local	Si el respaldo se encuentra en custodia local:  El analista de Control Tecnológico, debe abrir la caja fuerte con el código de seguridad, apertura la caja fuerte y traer la cinta solicitada para entregarla al área de Centro de Cómputo para restauración.	procedimiento de solicitud de respaldos.doc	Analista Control Tecnológico		Revisión de bitácora de custodia.	Traer cinta de almacenamiento local.	CONTROL DE CINTAS WACKENHUT.xls		

CONTINÚA →

8	Solicitar el respaldo a custodia externo	Si el respaldo no se encuentra en custodia local:  El analista de Control Tecnológico debe comunicarse con su contraparte responsable en Wackenhut (custodio externo), para solicitar se entregue la caja de seguridad en donde se encuentra almacenada la cinta a ser restaurada.	procedimiento de solicitud de respaldos.doc	Analista Control Tecnológico  Proveedor Wackenhut		Revisión de bitácora de custodia.	Traer cinta de almacenamiento externo.	CONTROL DE CINTAS WACKENHUT.xls		
9	Obtener respaldo del custodio externo	El analista de Control Tecnológico debe romper la cinta de seguridad de la caja entregada por Wackenhut y extraer la cinta correspondiente a la fecha de solicitud de respaldo, para entregarla al área de Centro de Cómputo para restauración.	procedimiento de solicitud de respaldos.doc	Analista Control Tecnológico		Traer cinta de almacenamiento externo.	Preparar cinta para entrega a Centro de Cómputo.			
10	Entregar respaldo a supervisor del Centro de Computo	El analista de Control Tecnológico entregará la cinta almacenada localmente o almacenada externamente al Centro de Cómputo junto con el formulario debidamente autorizado para la correspondiente restauración. Adicionalmente, el requerimiento en Service Desk es transferido al técnico de procesamiento del Centro de Cómputo para completar el servicio de recovery.	procedimiento de solicitud de respaldos.doc	Analista Control Tecnológico		Preparar cinta para entrega a Centro de Cómputo.	Entregar cinta para restauración. Requerimiento transferido a Centro de Cómputo.			
11	Recovery	Este proceso lo ejecuta el área de Centro de Cómputo, referirse a su matriz de diseño detallado "Servicio de recovery". Ellos son quienes deben notificar la restauración de la cinta.		Técnico de procesamiento Centro de Cómputo		Entregar cinta para restauración.	Enviar notificación de restauración.			
12	Recibir, registrar y archivar respaldo recuperado	Una vez que se haya restaurado la cinta el Centro de Cómputo entregará la cinta física al analista de Control Tecnológico quien debe revisar que la cinta corresponda a la fecha de la solicitud, actualizar la bitácora de registro, indicando fecha y hora de entrega recepción de la cinta, y almacenarla en el repositorio correspondiente de acuerdo a la ubicación en la que se encontraba inicialmente.	procedimiento de solicitud de respaldos.doc	Analista Control Tecnológico		Enviar notificación de restauración.	Almacenar cinta en el repositorio correspondiente.	CONTROL DE CINTAS WACKENHUT.xls		

4.3.9.5. Subproceso: Rotación de respaldos

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Revisar el "Control de Cintas" y determinar las cintas a rotar	El analista de Control Tecnológico revisa el inventario Excel de cintas, en donde identifica la cinta que va a rotar de acuerdo al siguiente esquema: Gestor y CAO Ecuador rotación 270 días Gestor y CAO Perú rotación 270 días AS400/170 rotación 90 días AS400 Desarrollo rotación 90 días Base de Datos TSM rotación 90 días  Una vez que las cintas cumplieron ese rango de tiempo se entrega al Centro de Cómputo de manera diaria correspondiente al día.  La de la Base de Datos TSM se entrega por adelantado, esto quiere decir que la cinta del lunes y martes se entregan el lunes.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Inventario de "Control de Cintas".	Identificación de cintas a rotar por equipo.			Automatizar la identificación de la o las cintas que deben rotar.
2	Identificar lugar de almacenamiento de la cinta	El analista de Control Tecnológico una vez que establece las cintas a rotar por cada equipo, identifica el lugar en donde se encuentran almacenadas, dependiendo del tipo de cinta, localmente o con el proveedor externo.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Identificación de cintas a rotar por equipo.	Identificación de lugar de almacenamiento de cintas a rotar.			
3	Obtener la cinta del sitio de almacenamiento local	Si la cinta se encuentra en almacenamiento local:  El analista de Control Tecnológico se dirige al subsuelo del edificio matriz Dineros o al subsuelo del edificio Banco Pichincha para traer la cinta a rotar.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Identificación de lugar de almacenamiento de cintas a rotar.	Obtención de cintas a rotar.			
4	Solicitar la cinta del custodio externo	Si la cinta no se encuentra en almacenamiento local:  El analista de Control Tecnológico se contacta telefónicamente con el responsable de la custodia de las cintas en Wackenhut y solicita se entregue la caja de seguridad en donde se encuentra almacenada la cinta a rotar.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Identificación de lugar de almacenamiento de cintas a rotar.	Solicitud de caja de seguridad que contiene cintas a rotar.			
5	Obtener la cinta del custodio externo	El analista de Control Tecnológico se comunica telefónicamente con el proveedor en Wackenhut, para solicitar se proporcione la caja de seguridad en donde se encuentra almacenada la cinta que va a rotar, recibe la caja de seguridad, abre la cinta de seguridad y extrae la cinta para rotación, actualiza el registro de almacenamiento de cintas que se guarda en la caja de seguridad y envía la caja de seguridad nuevamente a custodia externa.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Solicitud de caja de seguridad que contiene cintas a rotar.	Obtención de cintas a rotar.			

CONTINÚA →

6	Entregar cinta a supervisor del Centro de Cómputo	El analista de Control Tecnológico con la o las cintas obtenidas de los diferentes repositorios de almacenamiento prepara el acta de entrega recepción y entrega tanto el acta como las cintas al Centro de Cómputo, se firma por los responsables de las dos áreas el acta, se deja una copia en el Centro de Cómputo y se almacena la copia del acta en las carpetas correspondientes.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Obtención de cintas a rotar.	Entrega de cinta física y acta de entrega recepción.	ENTREGA-RESPALDOS1.pdf		
7	Actualizar "Control de Cintas"	El analista de Control Tecnológico una vez que ha entregado las cintas y guardado su respectiva copia del acta de entrega recepción, debe actualizar el inventario de "Control de Cintas", registrando la cinta que se ha entregado para rotación al Centro de Cómputo.	procedimiento de rotación de respaldos.doc	Analista Control Tecnológico		Entrega de cinta física y acta de entrega recepción.	Actualización de inventario "control de cintas".			

4.3.9.6. Subproceso: Custodia de respaldos

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos	Documentación Habilitante
1	Recibir las cintas de respaldo	Diariamente el operador del Centro de Cómputo entrega las cintas correspondientes a los respaldos obtenidos al analista de Control Tecnológico. El analista de Control Tecnológico recibe las cintas y la impresión del Display del AS400 para almacenamiento.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Cintas físicas e impresión de Display AS400.	Cintas revisadas y documentos impresos.			ENTREGA-RESPALDOS1.pdf
2	Clasificar los respaldos según equipo	El analista de Control Tecnológico clasifica las cintas recibidas por tipo de equipo, registra la recepción en la bitácora correspondiente y prepara el contenedor en donde transportará las cintas para el almacenamiento.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Cintas revisadas y documentos impresos.	Contenedor para transporte de cintas y documentos impresos.			
3	Almacenar cintas en caja fuerte del subsuelo Edificio Dineros	Si el tipo de respaldo es diario. El analista de Control Tecnológico transporta las cintas en el contenedor hacia la bodega correspondiente, deposita las cintas en la caja fuerte, cierra la bodega y regresa a cargar nuevamente el contenedor con las cintas restantes.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Contenedor para transporte de cintas y documentos impresos.	Cintas almacenadas en caja fuerte subsuelo matriz Dineros.			
4	Almacenar cintas en caja fuerte del subsuelo Edificio Banco Pichincha	Si el tipo de respaldo es mensual. El analista de Control Tecnológico transporta las cintas en el contenedor hacia la bodega correspondiente, deposita las cintas en la caja fuerte, cierra la bodega y regresa a cargar nuevamente el contenedor con las cintas restantes.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Contenedor para transporte de cintas y documentos impresos.	Cintas almacenadas en caja fuerte subsuelo edificio Banco Pichincha.			
5	Guardar cintas en contenedores de seguridad de respaldo externo	Si el tipo de respaldo corresponde a la segunda copia del sistema AS400 o se trata de otras plataformas. El analista de Control Tecnológico almacena las cintas en las cajas de seguridad proporcionadas por el proveedor Wackenhut, llena el registro que se incluye en la caja de seguridad, cierra la caja con la cinta de seguridad, etiqueta la caja de seguridad y se comunica con el proveedor para que envíen a personal para retirar la caja de seguridad.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Contenedor para transporte de cintas y documentos impresos.	Cintas almacenadas en caja de seguridad.			
6	Enviar cintas mediante guía de remisión a custodia externa	El analista de Control Tecnológico entrega la caja de seguridad debidamente sellada al personal de Wackenhut, para ello llena la guía de remisión en donde se detalla la fecha, nomenclatura de caja entregada y los responsables que entregan/reciben la caja de seguridad para almacenamiento externo, firmada por los responsables.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico Proveedor Wackenhut		Cintas almacenadas en caja de seguridad.	Guía de remisión firmado.			
7	Archivar guías de remisión de envío a custodia externa	El analista de Control Tecnológico entrega una copia de la guía de remisión al responsable del proveedor encargado de transportar la caja de seguridad, para que realice el ingreso correspondiente en las bodegas de Wackenhut, adicionalmente guarda una copia del documento "guía de remisión", como constancia del envío para almacenamiento externo.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Guía de remisión firmado.	Almacenamiento de guía de remisión firmada.			

CONTINÚA →

8	Actualizar el archivo Excel de "Control de Cintas"	El analista de Control Tecnológico debe actualizar la bitácora de "Control de Cintas", registrando el movimiento de todas las cintas recibidas, tanto las de almacenamiento local, diario y mensual, como las cintas de almacenamiento externo, duplicados y de otras plataformas.	procedimiento de custodia de respaldos.doc	Analista Control Tecnológico		Almacenamiento de guía de remisión firmada.	Bitácora de control actualizada.			CONTROL DE CINTAS WACKENHUT.xls
---	----------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------	------------------------------	--	---------------------------------------------	----------------------------------	--	--	---------------------------------

4.3.9.7. Subproceso: Seguridad y control administrativo

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Reuniones semanales de seguimiento	Este proceso consiste en la gestión de reportes de estado de avances para las tareas y proyectos asignados a los analistas del área, así como la verificación del estado de cumplimiento de las mismas y la validación de tiempos de entrega.		Gerente Control Tecnológico Analista Control Tecnológico		Acta de reunión de semana anterior	Acta de reunión de semana actual	Acta_Reunión_13feb12.xls		
2	Informes de gestión del área	Semanalmente se entrega un informe de las actividades realizadas en el área por cada uno de los macro procesos definidos para la gestión. Este proceso consiste en realizar un informe del tipo gerencial que será entregado a la gerencia de Tecnología en donde se resumen las actividades realizadas por los analistas del área en un periodo de corte semanal.	procedimiento o generación de reportes_v2.doc	Gerente Control Tecnológico Analista Control Tecnológico	Barcelona04 Iron Port Juniper VPN SSL AS400	Reportes obtenidos de las distintas herramientas de monitoreo de seguridad.	Informe semanal.	Informe Semanal Tecnología 05_04_2012.ppt		
3	Revisión y actualización de procedimientos	Anualmente se realiza una revisión de los procedimientos, reglamentos o políticas que se elaboran en el área para actualización a situación actual.  Este proceso consiste en que los analistas de Control Tecnológico al inicio de cada año realizan una revisión de la documentación existente correspondiente a políticas, reglamentos o procedimientos levantados en el área con la finalidad de actualizar la información en base a la situación actual que está viviendo el área.	Política_Seg_Información.pdf	Gerente Control Tecnológico Analista Control Tecnológico	Intranet	Políticas, reglamentos y procedimientos del área.	Políticas, reglamentos y procedimientos actualizados del área y publicados para difusión.		La revisión de los procedimientos se debe realizar por lo menos una vez al año.	



4.3.10. Proceso: Gestión de accesos

4.3.10.1. Subproceso: Mantenimiento de usuarios

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Recibir el requerimiento de Service Desk	El área de Control Tecnológico recepta todos los requerimientos por medio de un requerimiento de solicitud en Service Desk con la aprobación de la Gerencia solicitante o quien la represente.	Reglamento de Gestión de Usuarios_V2.doc Procedimiento de Solicitud de Gestión de Usuarios	Analista de Accesos Control Tecnológico	Herramienta de Service Desk	Requerimiento en Service Desk enviado por Service Desk	Requerimiento en Service Desk recibido por Control Tecnológico	formulario de creación de usuarios(v10).xls	Todas las solicitudes se deben canalizar a través del Service Desk	
2	Analizar la solicitud	El Analista de Accesos de Control Tecnológico identifica el tipo de solicitud de acceso y verifica que el requerimiento incluya las debidas aprobaciones de la Gerencia solicitante y verifica además si se requiere la autorización del área de Riesgos (generalmente en casos de modificación de perfiles, agregar o eliminar opciones).		Analista de Accesos Control Tecnológico		Requerimiento en Service Desk recibido por Control Tecnológico	Solicitud recibida y analizadapor el Analista de Accesos de Control Tecnológico			
3	Asignar requerimiento al área de Riesgos	En caso de requerir aprobación del área de Riesgo, el Analista de Accesos de Control Tecnológico asigna el requerimiento en la herramienta de Service Desk al Oficial de Seguridad de la información del área de Riesgo registrando las aprobaciones verificadas.		Analista de Accesos Control Tecnológico	Herramienta de Service Desk	Solicitud recibida y analizada en primera instancia por el Analista de Accesos de Control Tecnológico	Requerimiento asignado al Oficial de seguridad de la información del área de riesgo en la herramienta de Service Desk			
4	Recibir el requerimiento	El oficial de Seguridad de la Información en Riesgos recibe los requerimientos de modificación de perfiles a través de la herramienta de Service Desk.	Reglamento de Gestión de Usuarios_V2.doc Procedimiento de Solicitud de Gestión de Usuarios	Oficial de Seguridad área de Riesgos	Herramienta de Service Desk	Requerimiento asignado al Oficial de seguridad de la información del área de riesgo en la herramienta de Service Desk	Requerimiento recibido en la herramienta de Service Desk por parte del Oficial de seguridad de la información			El área de Riesgo se convierte en un área resolutoria y por lo tanto debe recibir y escalar los requerimientos a través de la herramienta de Service Desk.
5	Analizar el requerimiento	El oficial de Seguridad de la Información en Riesgos evalúa si es necesario modificar un perfil autorizado o simplemente cambiar al solicitante de tipo de perfil para asignación de opciones.		Oficial de Seguridad área de Riesgos		Requerimiento recibido en la herramienta de Service Desk por parte del Oficial de seguridad de la información	Requerimiento analizado y por el Oficial de Seguridad de la Información.			

CONTINÚA →

6	Notificar Control Tecnológico a	En caso de que el requerimiento sea rechazado, el Oficial de Seguridad de la Información en Riesgos deberá notificar al Analista de Control Tecnológico indicando las razones de rechazo de la solicitud, a través de la herramienta de Service Desk.		Oficial de Seguridad área de Riesgos	Herramienta de Service Desk	Requerimiento analizado y por el Oficial de Seguridad de la Información.	Requerimiento rechazado asignado al Analista de Accesos de Control Tecnológico a través de la herramienta de Service Desk.			
7	Asignar requerimiento Control Tecnológico	En caso de aprobación, el Oficial de Seguridad de la Información, a través de la herramienta de Service Desk, asigna al Analista de Accesos de Control Tecnológico la solicitud aprobada.		Oficial de Seguridad área de Riesgos	Herramienta de Service Desk	Requerimiento analizado y por el Oficial de Seguridad de la Información.	Requerimiento aprobado asignado al Analista de Accesos de Control Tecnológico a través de la herramienta de Service Desk.			
8	Verificar el requerimiento	El analista del área de Control Tecnológico debe verificar en la herramienta de Service Desk que efectivamente el requerimiento haya pasado por los controles correspondientes.		Analista de Accesos Control Tecnológico	Herramienta de Service Desk	Solicitud recibida y analizada en primera instancia por el Analista de Accesos de Control Tecnológico.	Requerimiento verificado en la herramienta de Service Desk			
9	Cerrar requerimiento	En caso de no aprobar el requerimiento, el Analista de Accesos de Control Tecnológico cierra el requerimiento en la herramienta de Service Desk.		Analista de Accesos Control Tecnológico	Herramienta de Service Desk	Requerimiento verificado en la herramienta de Service Desk	Requerimiento cerrado en la herramienta de Service Desk			
10	Notificar solicitante a	El analista de Control Tecnológico debe enviar un correo al solicitante indicando las razones por las que no se procede a la atención de su solicitud.		Analista de Accesos Control Tecnológico		Requerimiento cerrado en la herramienta de Service Desk	Mail de notificación de rechazo de solicitud			
11	Asignar el requerimiento al analista del área resolutoria	El Analista de Accesos de Control Tecnológico debe asignar el requerimiento a través de la herramienta de Service Desk a un analista del área resolutoria para la correspondiente otorgación. Las áreas resolutorias pueden ser Control Tecnológico, Infraestructura y Networking o Centro de Cómputo Según tipología de acceso.	Reglamento de Gestión de Usuarios_V2.doc Procedimiento de Solicitud de Gestión de Usuarios	Analista de Accesos Control Tecnológico	Herramienta de Service Desk	Requerimiento verificado en la herramienta de Service Desk	Requerimiento asignado a analista del área resolutoria a través de la herramienta de Service Desk			Idealmente todas las solicitudes de accesos deben ser aprobadas y otorgadas por el área de Control Tecnológico.

CONTINÚA →

12	Recibir el requerimiento	El analista del área resolutoria recibe el requerimiento a través de la herramienta de Service Desk.		Analista del Área resolutoria	Herramienta de Service Desk	Requerimiento asignado a analista del área resolutoria a través de la herramienta de Service Desk	Requerimiento recibido por el analista del área resolutoria a través de la herramienta de Service Desk			
13	Analizar el requerimiento	El analista del área resolutoria verificará la o las aplicaciones sobre las que se solicita el acceso, así como los perfiles o usuarios similares para la asignación de opciones.		Analista del Área resolutoria		Requerimiento recibido por el analista del área resolutoria a través de la herramienta de Service Desk	Aplicaciones sobre las que se dará acceso y perfiles o usuarios similares identificados por el analista del área resolutoria.			
14	Solicitar acceso a banco asociado	El analista de Control Tecnológico en el caso de identificar solicitudes de acceso para aplicaciones gestionadas por bancos asociados debe generar la correspondiente solicitud en dichas entidades por medio de correo electrónico y debe realizar seguimiento para identificar el estado de dicha solicitud.	procedimiento o gestión usuarios siglo xxi.doc	Analista Control Tecnológico		Aplicaciones sobre las que se dará acceso y perfiles o usuarios similares identificados por el analista del área resolutoria.	Generación de solicitud de acceso a Banco asociado y envío de formularios.			
15	Recibir requerimiento ejecutado por banco asociado	El analista de Control Tecnológico recibe la información de creación de acceso por parte del banco asociado en la aplicación solicitada y la envía al usuario solicitante vía mail.	procedimiento o gestión usuarios siglo xxi.doc	Analista Control Tecnológico		Notificación de creación de acceso, envío de usuario y clave vía mail por parte del banco asociado.	Envío de usuario y clave vía mail a usuario solicitante.			
16	Ejecutar procedimiento de acceso según tipología	El analista del área resolutoria habilita el acceso a la aplicación solicitada de acuerdo al procedimiento detallado en el manual correspondiente, verificando la información adjunta registrada en la herramienta de Service Desk. Referirse al documento "Detalle tipologías de acceso".	Referirse a pestaña "Detalle Tipologías"	Analista del Área resolutoria	Referirse a pestaña "Detalle Tipologías"	Aplicaciones sobre las que se dará acceso y perfiles o usuarios similares identificados por el analista del área resolutoria.	Creación de usuario y acceso a aplicación solicitada y entrega de contraseña al solicitante.			
17	Verificar el acceso con el usuario	El analista del área resolutoria contacta al usuario solicitante vía mail o llamada telefónica y verifica el ingreso a la aplicación solicitada confirmando el acceso solicitado.		Analista del Área resolutoria		Envío de usuario y clave vía mail a usuario solicitante.	Confirmación del usuario solicitante de acceso exitoso a la o las aplicaciones.			

CONTINÚA →

18	Cerrar requerimiento	El analista del área resolutoria cerrará el requerimiento en la herramienta de Service Desk una vez se haya confirmado el acceso exitoso del usuario en la o las aplicaciones.		Analista del Área resolutoria	Herramienta de Service Desk	Confirmación del usuario solicitante de acceso exitoso a la o las aplicaciones.	Cierre y finalización de requerimiento en herramienta de Service Desk.			
19	Notificar al usuario	El analista del área solicitante notificará al usuario solicitante a través de la herramienta de Service Desk la finalización exitosa de la atención al requerimiento.		Analista del Área resolutoria	Herramienta de Service Desk	Cierre y finalización de requerimiento.	Notificación de finalización de atención de requerimiento.			

4.3.11. Proceso: Gestión de eventos

4.3.11.1. Subproceso: Gestión de eventos

#	Actividad	Descripción	Manuales de Detalle	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Gestión de la Disponibilidad	El proceso de Gestión de Eventos es una consecuencia de los eventos detectados durante los sub procesos de monitoreo que se enmarcan en el proceso de Gestión de la Disponibilidad.		Técnico/herramientas de monitoreo Infraestructura y Networking y Centro de Cómputo	Barcelona 04	Monitoreo de aplicaciones, servidores, infraestructura, equipos de comunicación y transacciones.	Eventos detectados		El gestor de eventos es el rol encargado de gestionar los eventos detectados por las herramientas de monitoreo. Este rol lo puede asumir más de una persona.	
2	Recibir requerimiento	Una vez detectado un evento en alguno de los sub procesos de monitoreo, la herramienta de Service Desk (para los casos en donde las herramientas de monitoreo estén integradas con la herramienta de Service Desk), o en su defecto el operador de Service Desk, notifica inmediatamente al gestor de eventos responsable de solucionar dicho evento a través de un ticket generado en la herramienta de Service Desk. El gestor de eventos puede ser notificado por otros medios dependiendo de la criticidad del evento (mail, teléfono, en persona) pero siempre debe existir un requerimiento en la herramienta de Service Desk dado que es allí donde se registran las acciones tomadas que posteriormente son utilizadas para actualizar la base de conocimiento.		Gestor de eventos de Service Desk	Herramienta de Service Desk	Eventos detectados	Requerimiento recibido por el gestor de eventos en la herramienta de Service Desk		El gestor de eventos puede ser notificado por otros medios dependiendo de la criticidad del evento (mail, teléfono, en persona) pero siempre debe existir un requerimiento en la herramienta de Service Desk.	
3	Revisar base de conocimiento	El gestor de eventos debe revisar la base de conocimientos que reside en la herramienta de Service Desk para ubicar el procedimiento de solución a seguir y ceñirse a él.		Gestor de eventos de Service Desk	Herramienta de Service Desk	Requerimiento recibido por el gestor de eventos en la herramienta de Service Desk	Base de conocimiento en Service Desk revisada en búsqueda de procedimientos o guías de solución.			
4	Ejecutar secuencia conocida de solución	Una vez ubicado el procedimiento o guía a seguir, el gestor de eventos recorre los pasos indicados en dicha guía con el ánimo de lograr la solución esperada y reestablecer el servicio en el menor tiempo posible. Todas las acciones realizadas deben quedar registradas en la herramienta de Service Desk para futura referencia.		Gestor de eventos de Service Desk	Herramienta de Service Desk	Procedimiento de solución para el evento ubicado en la base de conocimiento de Service Desk	Procedimiento o guía de solución ejecutado			

CONTINÚA →

5	Notificar a solicitante	Una vez que se ha reestablecido el servicio y que el evento ha sido controlado, el gestor de eventos procede a notificar a los involucrados que el evento ha sido normalizado, indicando las acciones realizadas. Esta notificación puede ser por correo, teléfono o verbalmente.		Gestor de eventos de Service Desk		Procedimiento de solución ejecutado y evento solucionado	Notificación de resolución del evento a los involucrados			
6	Cerrar requerimiento	Cuando los involucrados han sido notificados de la solución del evento, el gestor de eventos procede a cerrar el requerimiento en la herramienta de Service Desk.		Gestor de eventos de Service Desk	Herramienta de Service Desk	Notificación de resolución del evento a los involucrados	Requerimiento cerrado en la herramienta de Service Desk			
7	Escalar requerimiento al área solucionadora	En caso de no encontrar un procedimiento o guía de solución en la base de conocimiento de Service Desk o en caso de que el procedimiento o guía indicado no solucione el evento, el gestor de eventos debe escalar el requerimiento hacia el área solucionadora. Este escalamiento se realiza sobre la herramienta de Service Desk dejando claro allí los procedimientos intentados, si es que hubo alguno, y cualquier información adicional que el gestor de eventos considere relevante para su futura resolución.		Gestor de eventos de Service Desk	Herramienta de Service Desk	Procedimientos de solución no encontrados en base de conocimiento de Service Desk o intentos fallidos de resolución	Requerimiento escalado al área solucionadora a través de la herramienta de Service Desk.			
8	Gestión de problemas	El proceso de Gestión de Problemas engloba las distintas áreas solucionadoras que toman los eventos no resueltos en la gestión de eventos y que constituyen la última línea de solución de problemas desconocidos.		Área solucionadora (Centro de Cómputo, Infraestructura y Networking, Standby Desarrollo, Proveedores)		Requerimiento escalado al área solucionadora a través de la herramienta de Service Desk.	Problema solucionado y notificación a Service Desk			

4.3.11.2. Proceso: Gestión de la continuidad de TI

4.3.11.3. Subproceso: Contingencia Autorizador

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Lineamiento de Proceso	Requerimientos	Documento habilitante
1	Monitoreo de disponibilidad equipo CAO	Mediante el software Barcelona, se realiza un continuo monitoreo del servidor, en el caso de que se presente una incidencia se disparará una alerta notificando al operador por correo y alarma sonora la novedad presentada en la disponibilidad del equipo	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo	Barcelona04	Monitoreo permanente del servidor	Activación de alerta en caso de que se presente algún incidente			
2	Evaluar el incidente y comunicar a Gerencia de Tecnología	En el caso de que el servidor tenga problemas que no se pueden solucionar por el soporte de primer nivel, se comunica a la Gerencia de Tecnología para evaluar el incidente y de ser el caso aprobar la activación de contingencia	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo		Activación de alerta en caso de que se presente algún incidente	Comunicación a la Gerencia de Tecnología			
3	Solucionar incidente	En el caso de que la gerencia no apruebe la activación de contingencia, se debe solucionar el incidente escalando con el proveedor del servidor y el equipo interno de técnicos		Técnico de procesamiento de Centro de Computo	AS400	Activación de contingencia no aprobada	Solución del incidente			
4	Activar la contingencia	En el caso de que la gerencia apruebe la activación de la contingencia, se tiene dos escenarios en los que se debe proceder de acuerdo al evento: 1) Si se encuentra disponible el acceso al servidor de contingencia, ubicado en el Centro de Computo alterno de Guayaquil, la activación de la contingencia lo realiza el técnico del Centro de Computo de Quito  2) Si no es posible acceder al servidor de contingencia del Centro de Cómputo alterno, la activación de la contingencia lo realiza el técnico del Centro de Cómputo de Guayaquil, de acuerdo al procedimiento establecido.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo	AS400	Activación de contingencia aprobada	Inicio del procedimiento para activar la contingencia			
5	Desconectar ATALLA principal UIO	Si el evento presentado es no controlado relacionado con las cajas encriptadoras y se puede activar la contingencia desde Quito, se realiza lo siguiente: En caso de que no se encuentre operativa la caja Atalla principal o de contingencia en el Centro de Computo UIO se debe realizar lo siguiente: a) Bajar todos los drivers del CAO --> Bajar los drivers del Atalla. b) Desconectar el cable de red de Atalla producción. c) Conectar el cable de red en Atalla Backup. --> Encender este servidor.	procedimiento de recuperación para el autorizador instructivo_activación_llaves_pmfk_atalla_9100.pdf	Técnico de procesamiento de Centro de Computo	Cajas encriptadoras	Fallo en equipos Atalla	Activación de equipos Atalla			ACTIVIDADES CAMBIO DE ROL CAO

CONTINÚA →

6	Conectar ATALLA contingencia UIO	En caso de que no se encuentren operativas ninguna de las cajas Atalla UIO, se debe seguir el siguiente procedimiento para activar la caja Atalla GYE. a) Ingresar al programa. b) En el campo IP Address conectarse a la IP XX.XXX.X.XX y dar OK. c) Digitar el comando de activación de la llave. d) Dar enviar y verificar la respuesta. Una vez activada la caja Atalla, se debe activar en DNS el Atalla de contingencia.	procedimiento de recuperación para el autorizador instructivo_activación_llaves_pmfk_atalla_9100.pdf	Técnico de procesamiento de Centro de Computo	Cajas encriptadoras	Fallo en equipos Atalla	Activación de equipos Atalla			ACTIVIDADES CAMBIO DE ROL CAO
7	Llamar a Datafast e indicar que activen la contingencia y levanten el standin	Si el evento presentado es una actividad planificada para activar la contingencia desde Quito, se realiza lo siguiente: Contactar telefónicamente al operador de Datafast para indicarle que se va a activar la contingencia y que levante el stand in.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito		Activación de contingencia ejecutada	Notificación a Datafast sobre la activación de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
8	Notificar a usuarios y entidades externas para indicar que se activa la contingencia	Contactar telefónicamente a las siguientes áreas y entidades para comunicar que se activa la contingencia: - Llamar a usuarios de autorizaciones. - Llamar a usuarios de riesgo. - Llamar a usuarios de crédito. - Llamar a Banred. - Llamar al banco.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito		Notificación a Datafast sobre la activación de contingencia	Notificación a usuarios y entidades externas sobre la activación de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
9	Envío de sign off para las redes internacionales	Mediante el modulo grafico del CAO, se deben ejecutar las siguientes opciones para notificar a las entidades internacionales que se activa la contingencia: - Enviar un Sign off a MasterCard Internacional. - Enviar un Sign off a Visa Internacional. - Enviar un Sign off a Internacional.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	CAO modulo grafico	Notificación a usuarios y entidades externas sobre la activación de contingencia	Activación de contingencia para redes internacionales			ACTIVIDADES CAMBIO DE ROL CAO
10	Ejecutar la activación de la contingencia en el equipo AS4000 remoto	Se cuenta con un programa desarrollado en el software de replicación MIMIX, mediante el cual se tiene automatizado las siguientes actividades: Bajar aplicativos en el CAO de Producción Cambio de rol Subir aplicativos en el CAO de Contingencia Ejecutar los comando en el equipo CDTID	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	AS400	Notificación a usuarios y entidades externas sobre la activación de contingencia	Bajar aplicativos en el CAO de Producción Cambio de rol Subir aplicativos en el CAO de Contingencia			ACTIVIDADES CONTINÚA → ROL CAO
11	Direccionamiento a los iSeries de Contingencia para las entidades externas	Cambiar las direcciones IP en el Firewall DMZ	procedimiento para el cambio de direcciones ip de los as4000 en el firewall dmz	Técnico de procesamiento de Centro de Computo Quito	Firewall	Bajar aplicativos en el CAO de Producción	Activación de contingencia para conexión de entidades externas			ACTIVIDADES CAMBIO DE ROL CAO

CONTINÚA →



12	Notificar a Datafast para que desactiven el stand in y se conecten al equipo de contingencia	Contactar telefónicamente al operador de Datafast para indicarle que desactiven el stand in y se conecten al equipo de contingencia	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito		Bajar aplicativos en el CAO de Producción	Autorizaciones activas para Datafast mediante equipo de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
13	Actualizar DNS y verificar conectividad.local	Asociar la nueva Ip del CAO con el nombre AS4000 en el servidor de DNS	Procedimiento para el cambio de direcciones ip del as4000 en servidor dns.	Técnico de procesamiento de Centro de Computo Quito	Servidor DNS	Bajar aplicativos en el CAO de Producción	Activación de contingencia para conexión usuarios internos			ACTIVIDADES CAMBIO DE ROL CAO
14	Resetear aplicación para el servicio botón de pagos	En el servidor WEB ejecutar lo siguiente: Bajar servicio BOTÓN PAGOS Levantar servicio BOTÓN PAGOS Bajar servicio BOTÓN PAGOS	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	Servidor Windows	Activación de equipo contingencia	Activación de contingencia para servicio de botón de pagos			ACTIVIDADES CAMBIO DE ROL CAO
15	En el equipo CDUTID subir manualmente driver para la comunicación con red Nexo banco	En el equipo HAAD Desde el usuario OPERCA, ejecutar la siguiente opción: 22 122 SUBIR DRIVER NEXO	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	AS400	Activación de equipo contingencia	Activación de contingencia para servicio de cajeros			ACTIVIDADES CAMBIO DE ROL CAO
16	En el equipo AS4000SNA subir manualmente driver para la comunicación con red Nexo banco	En el equipo AS4000SNA desde el usuario OPERCA, ejecutar la siguiente opción: 22 122 SUBIR DRIVER ATM SNA EQUIPO ANTIGUO	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	AS400	Activación de equipo contingencia	Activación de contingencia para servicio de cajeros			ACTIVIDADES CAMBIO DE ROL CAO
17	Verificar que los servicios se encuentren operativos	a) Revisión de drivers activos mediante el comando WRKAB b) Revisión de mensajes de test 800 desde la aplicación para monitoreo.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	AS400	Activación de equipo contingencia	Verificación de servicios activos en el equipo de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
18	Levantar la réplica desde equipo CDUTID hacia equipo AUTID	Con el propósito de que las transacciones que ingresan en el equipo alterno se repliquen al equipo principal, desde la aplicación MIMIX se debe ejecutar en el equipo CDUTID el siguiente comando: 1) addlible mimix 2) strag agdfn(autor)	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Quito	AS400	Activación de equipo contingencia	Replicación de datos desde equipo de contingencia hacia equipo de producción			ACTIVIDADES CAMBIO DE ROL CAO

CONTINÚA →

CONTINÚA →

19	Llamar a Datafast e indicar que activen la contingencia y levanten el standin	Si el evento presentado es un incidente no planificado y no se puede acceder al equipo de contingencia desde el Centro de Cómputo de Quito, se debe realizar lo siguiente: Contactar telefónicamente al operador de Datafast para indicarle que se va a activar la contingencia y que levante el stand in.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil		Activación de contingencia aprobada desde el Centro de Computo alterno	Notificación a Datafast sobre la activación de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
20	Activar caja Atalla en Guayaquil	Activar la caja Atalla GYE. a) Ingresar al programa PCLITCP b) Constatar la IP c) Digitar el comando de activación de la llave.	procedimiento de recuperación para el autorizador instructivo_activación_llaves_pmfk_atalla_9100	Técnico de procesamiento de Centro de Computo Guayaquil	Cajas encriptadoras	Fallo en equipos Atalla	Activación de equipos Atalla			ACTIVIDADES CAMBIO DE ROL CAO
21	Activar en DNS caja Atalla de Guayaquil	Una vez activada la caja Atalla, se debe activar en DNS el Atalla de contingencia, con los siguientes pasos: a) Ingresar al servidor b) Abrir la consola DNS c) Ingresar al directorio Forward Lookup Zones d) Cambiar la IP	procedimiento de recuperación para el autorizador instructivo_activación_llaves_pmfk_atalla_9100	Técnico de procesamiento de Centro de Computo Guayaquil	Cajas encriptadoras	Fallo en equipos Atalla	Activación de equipos Atalla			ACTIVIDADES CAMBIO DE ROL CAO
22	Contactar con Visión Solutions para indicarles que se va a realizar un switch over no controlado	En base a lo indicado en el manual del proveedor de replicación, para este tipo de eventos se debe contactar con Visión Solutions para indicarles que se va a realizar un switch over no controlado.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil		Activación de contingencia aprobada desde el Centro de Computo alterno	Notificación sobre activación de contingencia al proveedor de software de replicación			ACTIVIDADES CAMBIO DE ROL CAO
23	Ejecutar la activación de la contingencia en el equipo AS4000 remoto	Se cuenta con un programa desarrollado en el software de replicación MIMIX, mediante el cual se tiene automatizado las siguientes actividades: Bajar aplicativos en el CAO de Producción Cambio de rol Subir aplicativos en el CAO de Contingencia Ejecutar los comandos requeridos en el equipo HCDAID	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipos Atalla	Bajar aplicativos en el CAO de Producción Cambio de rol Subir aplicativos en el CAO de Contingencia			ACTIVIDADES CAMBIO DE ROL CAO
24	Asociar la nueva ip del CAO con el nombre AS4000CA en el servidor de DNS	Asociar la nueva Ip del CAO con el nombre AS4000 en el servidor de DNS	procedimiento para el cambio de direcciones ip del as4000 en servidor dns	Técnico de procesamiento de Centro de Computo Guayaquil	Servidor DNS	Bajar aplicativos en el CAO de Producción	Activación de servicio de DNS en contingencia			ACTIVIDADES CAMBIO DE ROL CAO

CONTINÚA →

25	Cambiar rutas en el ruteador de Guayaquil para activar Electrón y Efectivo Express	Realizar las siguientes actividades para poder levantar Electrón y Efectivo Express con el BancoP: a) En el Ruteador Principal del Centro Alterno cambiar las Ip's indicadas en el manual.	procedimiento de recuperación para el autorizador procedimiento para el cambio de direcciones ip de los as4000 en el firewall dmz	Técnico de procesamiento de Centro de Computo Guayaquil	Firewall	Bajar aplicativos en el CAO de Producción	Activación de contingencia para servicios Electrón y Efectivo Express			ACTIVIDADES CAMBIO DE ROL CAO
26	Notificar a Datafast para que desactiven el stand in y se conecten al equipo de contingencia	Contactar telefónicamente al operador de Datafast para indicarle que desactiven el stand in y se conecten al equipo de contingencia	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil		Bajar aplicativos en el CAO de Producción	Autorizaciones activas para Datafast mediante equipo de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
27	Verificar que los servicios se encuentren operativos	a) Revisión de drivers activos mediante el comando WRKOB b) Revisión de mensajes de test 800 desde la aplicación para monitoreo.	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipo contingencia	Verificación de servicios activos en el equipo de contingencia			ACTIVIDADES CAMBIO DE ROL CAO
28	Modificar área de datos	Cuando se haya recuperado el equipo AUTID, modificar la siguiente área de datos en caso de que exista: 1) CHGDTAARA DTAARA(QGPL/MXSYLE) VALUE(S)	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipo contingencia	Revisión de configuración de software de replicación			ACTIVIDADES CAMBIO DE ROL CAO
29	Levantar la réplica desde equipo HAAUTID hacia equipo AUTID	Con el propósito de que las transacciones que ingresan en el equipo alterno se repliquen al equipo principal, desde la aplicación MIMIX se debe ejecutar en el equipo HATID el siguiente comando: 1) ADDLLE MIMIX 2) STRAG AGDFN(AUTOR)	procedimiento de recuperación para el autorizador	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipo contingencia	Replicación de datos desde equipo de contingencia hacia equipo de producción			ACTIVIDADES CAMBIO DE ROL CAO

4.3.11.4. Subproceso: Contingencia Gestor

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documento habilitante	Lineamiento de Proceso	Requerimientos
1	Monitoreo de disponibilidad equipo GESTOR	Mediante el software Barcelona, se realiza un continuo monitoreo del servidor, en el caso de que se presente una incidencia se disparará una alerta notificando al operador por correo y alarma sonora la novedad presentada en la disponibilidad del equipo	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo	Barcelona	Monitoreo permanente del servidor	Activación de alerta en caso de que se presente algún incidente			
2	Evaluar el incidente y comunicar a Gerencia de Tecnología	En el caso de que el servidor tenga problemas que no se pueden solucionar por el soporte de primer nivel, se comunica a la Gerencia de Tecnología para evaluar el incidente y de ser el caso aprobar la activación de contingencia	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo		Activación de alerta en caso de que se presente algún incidente	Comunicación a la Gerencia de Tecnología			
3	Solucionar incidente	En el caso de que la gerencia no apruebe la activación de contingencia, se debe solucionar el incidente escalando con el proveedor del servidor y el equipo interno de técnicos		Técnico de procesamiento de Centro de Computo	AS400	Activación de contingencia no aprobada	Solución del incidente			
4	Activar la contingencia	En el caso de que la gerencia apruebe la activación de la contingencia, se tiene dos escenarios en los que se debe proceder de acuerdo al evento: 1) Si se encuentra disponible el acceso al servidor de contingencia, ubicado en el Centro de Computo alternativo de Guayaquil, la activación de la contingencia lo realiza el técnico del Centro de Computo de Quito 2) Si no es posible acceder al servidor de contingencia del Centro de Cómputo alternativo, la activación de la contingencia lo realiza el técnico del Centro de Cómputo de Guayaquil, de acuerdo al procedimiento establecido.	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo	AS400	Activación de contingencia aprobada	Inicio del procedimiento para activar la contingencia			
5	Desconectar ATALLA principal UIO	Si el evento presentado es no controlado relacionado con las cajas encriptadora y se puede activar la contingencia desde Quito, se realiza lo siguiente:  En caso de que no se encuentre operativa la caja Atarla principal o de contingencia en el Centro de Computo UIO se debe realizar lo siguiente: a) Bajar todos los drivers del Gestor b) Desconectar el cable de red de Atalla producción. c) Conectar el cable de red en Atalla Backus.	procedimiento de recuperación para el gestor instructivo_activación_lleva_pmfk_atalla_9100.pdf	Técnico de procesamiento de Centro de Computo	Cajas encriptadora	Fallo en equipos Atarla	Activación de equipos Atarla	ACTIVIDADES CAMBIO DE ROL GESTOR		

CONTINÚA →

6	Conectar ATALLA contingencia UIO	En caso de que no se encuentren operativas ninguna de las cajas Atarla UIO, se debe seguir el siguiente procedimiento para activar la caja Atalla GYE. a) Ingresar al programa PCLIP b) Ingresar la IP c) Digitar el comando de activación de la llave. d) Dar enviar y verificar la respuesta e) Una vez activada la caja Atalla, se debe activar en DNS el Atalla de contingencia	procedimiento de recuperación para el gestor instructivo_activación_llaves_pmfk_atalla_9100.pdf	Técnico de procesamiento de Centro de Computo	Cajas encriptadora	Fallo en equipos Atarla	Activación de equipos Atarla	ACTIVIDADES CAMBIO DE ROL GESTOR		
7	Notificar a usuarios y entidades externas para indicar que se activa la contingencia	Si el evento presentado es una actividad planificada para activar la contingencia desde Quito, se realiza lo siguiente:  Contactar telefónicamente a las siguientes áreas y entidades para comunicar que se activa la contingencia: - Llamar a usuarios de autorizaciones - Llamar a usuarios de riesgo. - Llamar a usuarios de crédito. - Llamar al banco.	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Quito		Activación de contingencia aprobada	Notificación a usuarios y entidades externas sobre la activación de contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
8	Activar oficial en el Autorizador, en el módulo gráfico	Activar el oficial de crédito desde el módulo gráfico del equipo CAO, para que las autorizaciones sean procesadas desde el equipo autorizador	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Quito	CAO modulo grafico	Notificación a usuarios y entidades externas sobre la activación de contingencia	Activación de autorizaciones que se rutean al oficial en el equipo Autorizador	ACTIVIDADES CAMBIO DE ROL GESTOR		
9	Bajar servicios web y nuevo botón de pagos en el servidor WEBID	Con el usuario OPERWEB bajar todos los servicios. Verificar que estén todos los trabajos del subsistema QSMSSBS abajo, caso contrario bajarlos manualmente. Adicional bajar los siguientes trabajos del subsistema QINTER.	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Quito	Equipo Webid	Activación de contingencia aprobada	Finalización de los servicios web	ACTIVIDADES CAMBIO DE ROL GESTOR		
10	Ejecutar la activación de la contingencia en el equipo AS4000 remoto	Se cuenta con un programa desarrollado en el software de replicación MIMIX, mediante el cual se tiene automatizado las siguientes actividades: Bajar aplicativos en el GESTOR de Producción Cambio de rol Subir aplicativos en el GESTOR de Contingencia Ejecutar en el equipo HAGED los comandos indicados en el manual	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Quito	AS400	Activación de contingencia aprobada	Bajar aplicativos en el GESTOR de Producción Cambio de rol Subir aplicativos en el GESTOR de Contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
11	Direccionamiento a los iSeries de Contingencia para las entidades externas	Cambiar las direcciones IP en el Firewall DMZ	procedimiento para el cambio de direcciones ip de los as4000 en el firewall dmz	Técnico de procesamiento de Centro de Computo Quito	Firewall	Bajar aplicativos en el Gestor de Producción	Activación de contingencia para conexión de entidades externas	ACTIVIDADES CAMBIO DE ROL GESTOR		

CONTINÚA →

12	Actualizar DNS y verificar conectividad	Asociar la nueva Ip del Gestor con el nombre AS4000 en el servidor de DNS	Procedimiento para el cambio de direcciones ip del as4000 en servidor dns.	Técnico de procesamiento Centro de Computo Quito	Servidor DNS	Bajar aplicativos en el Gestor de Producción	Activación de contingencia para conexión usuarios internos	ACTIVIDADES CAMBIO DE ROL GESTOR		
13	Activar el oficial en el Gestor desde el modulo gráfico.	Habilitar la opción del oficial de crédito para que las autorizaciones sean ruteadas al equipo Gestor, para lo cual se debe cambiar en la opción "Estatus Gestor" del módulo gráfico en Activo para todas las marcas y solicitar al área crédito y riesgo ingresen normalmente.	procedimiento de recuperación para el gestor	Técnico de procesamiento Centro de Computo Quito	Servidor Windows	Activación de equipo contingencia	Activación de autorizaciones que se rutean al oficial en el equipo Gestor de contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
14	Levantar servicios web y nuevo botón de pagos en el servidor WEBID	Levantar servicios web y nuevo botón de pagos en el servidor WBID según manual.	procedimiento de recuperación para el gestor	Técnico de procesamiento Centro de Computo Quito	AS400	Activación de equipo contingencia	Activación de servicios web	ACTIVIDADES CAMBIO DE ROL GESTOR		
15	Verificar que los servicios se encuentren operativos	Se debe monitorear los siguientes procesos: Envió y Recepción de transacciones del CAO al Gestor y viceversa Verificar que las transacciones de autorizaciones se estén ruteando correctamente al oficial de Autorizaciones. Verificar que los drivers del subsistema ASEBSBS Verificar que el trabajo PTEN se encuentre activo Verificar que el trabajo LISTE se encuentre activo Verificar que el trabajo LIST10 se encuentre activo Verificar que el trabajo PLEND se encuentre activo Verificar que el trabajo PLS610 se encuentre activo Verificar que el subsistema QSMBS este activo y sometido el siguiente trabajo: SMISTEN	procedimiento de recuperación para el gestor	Técnico de procesamiento Centro de Computo Quito	AS400	Activación de equipo contingencia	Verificación de servicios activos en el equipo de contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
16	Levantar la réplica desde equipo HAGESID hacia equipo GESTORID	Con el propósito de que las transacciones que ingresan en el equipo alterno se repliquen al equipo principal, desde la aplicación MIMIX	procedimiento de recuperación para el gestor	Técnico de procesamiento Centro de Computo Quito	AS400	Activación de equipo contingencia	Replicación de datos desde equipo de contingencia hacia equipo de producción	ACTIVIDADES CAMBIO DE ROL GESTOR		
17	Activar caja Atalla en Guayaquil	Si el evento presentado es un incidente no planificado y no se puede acceder al equipo de contingencia desde el Centro de Cómputo de Quito, se debe realizar lo siguiente: Activar la caja Atalla GYE. a) Ingresar al programa PCLITCP b) Ingresar a la IP XXX.XXX.XXX.XXX c) Digitar el comando de activación de la llave.	procedimiento de recuperación para el gestor instructivo_activación_llaves_pmfk_atalla_9100	Técnico de procesamiento Centro de Computo Guayaquil	Cajas encriptadora	Activación de contingencia aprobada desde el Centro de Computo alterno	Activación de equipos Atarla	ACTIVIDADES CAMBIO DE ROL GESTOR		

CONTINÚA →

18	Activar en DNS caja Atalla de Guayaquil	Una vez activada la caja Atalla, se debe activar en DNS el Atarla de contingencia, con los siguientes pasos: a) Ingresar al servidor a través de escritorio remoto b) Abrir la consola DNS c) Ingresar al directorio Forward Look Sones d) Hacer clic derecho sobre el servidor ATLAOD e) Cambiar la IP	procedimiento de recuperación para el gestor instructivo_activación_llaves_pmfk_atalla_9100	Técnico de procesamiento de Centro de Computo Guayaquil	Cajas encriptadora	Fallo en equipos Atalla	Activación de equipos Atarla	ACTIVIDADES CAMBIO DE ROL GESTOR		
19	Activar oficial en el Autorizador, en el módulo gráfico	En cuanto se encuentre operativo el equipo HACDID de contingencia, activar el oficial de crédito desde el módulo gráfico del equipo CAO, para que las autorizaciones sean procesadas desde el equipo autorizador	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Quito	CAO modulo grafico	Activación de equipos Atarla	Activación de autorizaciones que se rutean al oficial en el equipo Autorizador	ACTIVIDADES CAMBIO DE ROL GESTOR		
20	Contactar con Visión Solutions para indicarles que se va a realizar un switch over no controlado	En base a lo indicado en el manual del proveedor de software de replicación, para este tipo de eventos se debe contactar con Visión Solutions para indicarles que se va a realizar un switch over no controlado al siguiente número: 001952	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Guayaquil		Activación de contingencia aprobada desde el Centro de Computo alterno	Notificación sobre activación de contingencia al proveedor de software de replicación	ACTIVIDADES CAMBIO DE ROL GESTOR		
21	Ejecutar la activación de la contingencia en el equipo AS4000 remoto	Se cuenta con un programa desarrollado en el software de replicación MIMIX, mediante el cual se tiene automatizado las siguientes actividades: Bajar aplicativos en el Gestor de Producción Cambio de rol Subir aplicativos en el Gestor de Contingencia Ejecutar en el equipo HADGID los comandos indicados en el manual.	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipos Atarla	Bajar aplicativos en el Gestor de Producción Subir aplicativos en el Gestor de Contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
22	Asociar la nueva ip del Gestor con el nombre AS4000F35 en el servidor de DNS	Asociar la nueva Ip del Gestor con el nombre AS4000 en el servidor de DNS	procedimiento para el cambio de direcciones ip del as4000 en servidor dns	Técnico de procesamiento de Centro de Computo Guayaquil	Servidor DNS	Bajar aplicativos en el Gestor de Producción	Activación de servicio de DNS en contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
23	Cambiar rutas en el ruteador de Guayaquil para activar la conexión de los usuarios del banco	Realizar las siguientes actividades para activar la conexión de los usuarios del Banco Hay que reversar todos los pasos cuando el sistema vuelva a la normalidad	procedimiento para el cambio de direcciones ip de los as4000 en el firewall dmz	Técnico de procesamiento de Centro de Computo Guayaquil	Firewall	Bajar aplicativos en el Gestor de Producción	Activación de contingencia para ingreso usuarios banco Pichincha	ACTIVIDADES CAMBIO DE ROL GESTOR		
24	Activar el oficial en el Gestor desde el modulo grafico	Activar el oficial de crédito desde el módulo gráfico del equipo CAO, para que las autorizaciones sean procesadas desde el equipo autorizador	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Quito	CAO modulo grafico	Activación de contingencia equipo Gestor	Activación de autorizaciones que se rutean al oficial en el equipo Autorizador	ACTIVIDADES CAMBIO DE ROL GESTOR		

CONTINÚA →

25	Verificar que los servicios se encuentren operativos	Se debe monitorear los siguientes procesos: Envió y Recepción de transacciones del CAO al Gestor y viceversa	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipo contingencia	Verificación de servicios activos en el equipo de contingencia	ACTIVIDADES CAMBIO DE ROL GESTOR		
26	Modificar área de datos	Cuando se haya recuperado el equipo GESTORID, modificar la siguiente área de datos en caso de que exista: 1) CHGDARA DTAARA(QGPL/YSROLE) VALE(S)	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipo contingencia	Revisión de configuración de software de replicación	ACTIVIDADES CAMBIO DE ROL GESTOR		
27	Levantar la réplica desde equipo HAGESID hacia equipo GESTORID	Con el propósito de que las transacciones que ingresan en el equipo alterno se repliquen al equipo principal, desde la aplicación MIMIX se debe ejecutar en el equipo HAID el siguiente comando:	procedimiento de recuperación para el gestor	Técnico de procesamiento de Centro de Computo Guayaquil	AS400	Activación de equipo contingencia	Replicación de datos desde equipo de contingencia hacia equipo de producción	ACTIVIDADES CAMBIO DE ROL GESTOR		



4.3.11.5. Subproceso: Contingencia Peoplesoft

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Identificar evento de contingencia	Si la contingencia de People Soft no se va a realizar por una actividad de mantenimiento, se debe identificar el evento que va a provocar dicha contingencia.		Administrador de servidores de Infraestructura y Networking		Necesidad de levantar contingencia	Evento de contingencia Identificado.			
2	Evaluar levantamiento de contingencia	Una vez que se ha identificado el motivo del levantamiento de la contingencia, el Sub gerente de Infraestructura y Networking procede a evaluar el impacto que va a provocar la puesta en marcha de la contingencia, es decir procede a analizar el tiempo que se demoraría el levantar la contingencia, por cuanto tiempo estaría levantada la contingencia y la carga de usuarios que sería capaz de soportar la contingencia.		Gerencia de Operación del Servicio		Evento de contingencia Identificado.	Factibilidad Analizada			
3	Notificar a áreas involucradas	En el caso de un mantenimiento de la Infraestructura o que se vaya a levantar la contingencia por cualquier motivo, se debe notificar a todas las áreas involucradas en el levantamiento de la contingencia para poder tener un cronograma de trabajo debidamente calendarizado así como comunicar los diferentes procesos para poder tener la contingencia levantada.		Administrador de servidores de Infraestructura y Networking		Evento de contingencia Identificado.	Áreas Notificadas y plan de contingencia aprobado y calendarizado.			
4	Detener procesos calendarizados en People soft	El Analista de Diseño de Servicio, procede a revisar que todos los procesos calendarizados se detengan correctamente antes de proceder a detener todo el sistema del People Soft.		Analista de Diseño de Servicio		Plan de contingencia aprobado y calendarizado.	Procesos calendarizados en People soft detenidos.			
5	Detener procesos de envío de archivos al FTP desde AS400	El Técnicos del Centro de Computo, procede a verificar y detener todos los procesos de FTP que estén siendo ejecutados hacia el servidor FTP de People Soft (srvfil3)		Técnico de procesamiento de Centro de Computo		Plan de contingencia aprobado y calendarizado.	FTP desde al AS400 detenido			
6	Bajar FTP de People soft	El Administrador de servidores de Infraestructura y Networking, ingresa al servidor srvfil3 y procede a detener el servicio de FTP.  *En el Administrador de IIS, expanda el equipo local, Expanda la carpeta Sitios FTP, Haga clic con el botón secundario del mouse en el sitio que desee detener y, A continuación, haga clic en Detener.	Manual para apagar encender servidor srvfileuio3	Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	FTP de People Soft detenido			
7	Detener servicios People soft	El Administrador de servidores de Infraestructura y Networking, procede a detener todos los servicios que componen el People Soft siguiendo el orden determinado.  Hacer referencia a manuales Adjuntos.	manual procedimiento para activar contingencia en gye	Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	Servicios Detenidos			

CONTINÚA →

8	Realizar switch over de base de datos	El Administrador de servidores de Infraestructura y Networking, procede a Switch over desde OP a OPGYE.  Se conecta vía ssh hacia el servidor dbpro155a como usuario root. Se cambia al usuario Oracle.  Y procede como indica el manual.	manual procedimiento para realizar un switchover entre las bases de datos del crm	Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	Switch Over de la Base de Datos realizada			
9	Intercambiar dirección IP en el DNS	El Administrador de servidores de Infraestructura y Networking, procede a cambiar las IPS de los servidores de People Soft en el DNS		Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	IP's cambiadas en el DNS			
10	Levantar servidor FTP de contingencia de	El Administrador de servidores de Infraestructura y Networking, ingresa al servidor srvfil3 y procede a detener el servicio de FTP. *En el Administrador de IIS, expanda el equipo local, Expanda la carpeta Sitios FTP, Haga clic con el botón secundario del mouse en el sitio que desee detener y A continuación, haga clic en Iniciar.	Manual para apagar encender servidor srvfileuio3	Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	Servidor FTP de contingencia de People soft levantado			
11	Levantar servicios People soft en contingencia	El Administrador de servidores de Infraestructura y Networking, procede a detener todos los servicios que componen el People Soft siguiendo el orden encendido.  Hacer referencia a manuales Adjuntos.	manual procedimiento para activar contingencia en gye	Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	Servicios Levantados			
12	Parametrizar en contingencia	El Administrador de servidores de Infraestructura y Networking, procede a realizar la Parametrización respectiva.		Administrador de servidores de Infraestructura y Networking		Plan de contingencia aprobado y calendarizado.	en contingencia Parametrizado			
13	Arrancar procesos calendarizados en contingencia	El Analista de Diseño de Servicio, procede a calendarizar los procesos en el servidor ssoft y DBCONT.		Analista de Diseño de Servicio		Plan de contingencia aprobado y calendarizado.	Calendarizados res Levantados			
14	Notificar a Gerencia	Una vez levantada y configurada la contingencia, El Administrador de servidores de Infraestructura y Networking procede a notificar a la Gerencia de Infraestructura y Networking que se encuentra funcional la contingencia.		Administrador de servidores de Infraestructura y Networking		Contingencia Levantada	Gerencia Notificada			
15	Solicitar asistencia al proveedor	En el caso de la contingencia no sea aprobada por algún motivo y se vea que se impactaría de menor manera con la asistencia del proveedor, se procede a contactarlo vía telefónica o vía email al proveedor y solicitar la asistencia necesaria.	Teléfono Email	Administrador de servidores de Infraestructura y Networking		Solicitar asistencia al proveedor	Proveedor Notificado.			

CONTINÚA →

16	Solucionar problema	El proveedor procede a la revisión y solución del problema reportado.		Administrador de servidores de Infraestructura y Networking		Proveedor Notificado.	Problema Solucionado			
----	---------------------	-----------------------------------------------------------------------	--	-------------------------------------------------------------	--	-----------------------	----------------------	--	--	--

4.3.12. Proceso: Gestión de la disponibilidad

4.3.13. Subproceso: Monitoreo de aplicaciones

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documento habilitante	Lineamiento de Proceso	Requerimientos
1	Determinar a aplicación monitorear	El monitoreo que se realiza en el centro de cómputo es un monitoreo constante de todos los componentes que forman los servicios que ofrece la organización, para lo cual se cuenta con el software Barcelona en donde se crean las alarmas para el monitoreo automático de las aplicaciones indicadas en el listado: Monitoreo de aplicaciones	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo	Barcelona04	Definición de aplicaciones a monitorear	Listado de aplicaciones identificado			
2	Ingresar a consola de monitoreo de la aplicación	Desde la consola de monitoreo se selecciona el componente donde están agrupadas todas las aplicaciones monitoreadas la cual despliega un listado con el estado actual de todas las aplicaciones	Manuales del proveedor	Técnico de monitoreo Centro de Computo	Barcelona04	Listado de aplicaciones identificado	Consola de monitoreo arriba			
3	Verificar estado de la aplicación	En el componente desde donde se monitorean todas las aplicaciones se puede verificar de forma gráfica el estado de la aplicación, la cual puede tener los siguientes estados, dependiendo de condiciones definidas en la configuración de las reglas de salud. Rojo: se tiene un evento crítico, que notifica al operador sobre el cambio de estado mediante correo o una alerta sonora Amarillo: La aplicación está llegando a los límites establecidos y puede convertirse en un evento crítico Azul: Es de tipo informativo para indicar que se está superando los límites normales Verde: La aplicación está funcionando correctamente	Manuales del proveedor	Técnico de monitoreo Centro de Computo	Barcelona04	Consola de monitoreo arriba	Verificación del estados de la aplicación			
4	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		
5	Determinar si se requiere simulación de usuario	Para monitorear que las aplicaciones estén prestando el servicio adecuado, se define un listado de las aplicaciones a las cuales se les va simular el uso por medio de la herramienta de monitoreo.	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo	Barcelona04	Consola de monitoreo arriba	Definición de aplicaciones a monitorear			

CONTINÚA →

6	Ingresar a la aplicación y simular el uso	La aplicación de monitoreo tiene un componente que permite simular el ingreso a una determinada aplicación, con el propósito de verificar de forma automática si se encuentra operativa. Si se tiene el caso de un cambio de estado el cual la herramienta notifica al operador, se ingresa a la aplicación para verificar su funcionamiento.		Técnico de monitoreo Centro de Computo	Barcelona04	Definición de aplicaciones a monitorear	Simulación de uso de la aplicación realizado			
7	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		

4.3.13.1. Subproceso: Monitoreo de centrales telefónicas, equipos de comunicación

#	Actividad	Descripción	Manual	Responsable	Sistema de Información	Entrada	Salida	Documentos habilitantes	Lineamiento de Proceso	Requerimientos
1	Determinar componente a monitorear	Se deben monitorear varios componentes entre los cuales tenemos: Centrales telefónicas Enlaces Equipos de comunicación (firewall, routers, switch)		Técnico de monitoreo de Centro de Cómputo		Necesidad de monitorear componente	Componente identificado para monitoreo.			
2	Ingresar a consola de monitoreo correspondiente	Se debe ingresar a la consola de monitoreo y verificar el consumo de procesamiento del equipo, tiempo de respuesta de los enlaces, consumo de ancho de banda en los enlaces, los puertos de comunicación, spools de la troncal.	pro_in_procedimiento para monitorear incidentes en central telefónica	Técnico de monitoreo de Centro de Cómputo	Consolas de monitoreo	Componente identificado para monitoreo.	Consola de monitoreo arriba			
3	Verificar consumo de procesamiento del equipo	Una vez dentro de la consola adecuada para el componente que se eligió se verifica el consumo de procesamiento del equipo para determinar si existe algún proceso que este consumiendo demasiado procesamiento.		Técnico de monitoreo de Centro de Cómputo	Consolas de monitoreo	Componente identificado para monitoreo.	Consumo de procesamiento verificado			
4	Notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta de monitoreo o en su defecto el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo	Herramienta de Service Desk	Evento detectado	Notificación de evento a gestor de eventos en Service Desk	bitacora de eventos		
5	Verificar tiempo de respuesta	Una vez dentro de la consola adecuada para el componente que se eligió se verifica el tiempo de respuesta entre los equipos seleccionados y se determina si algún componente está respondiendo más lento de lo normal.		Técnico de monitoreo de Centro de Cómputo	Consolas de monitoreo	Componente identificado para monitoreo.	Tiempo de respuesta de los enlaces Verificado			
6	Notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta de monitoreo o en su defecto el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo	Herramienta de Service Desk	Evento detectado	Notificación de evento a gestor de eventos en Service Desk	BITACORA DE EVENTOS		
7	Verificar consumo de ancho de banda	Una vez dentro de la consola adecuada para el componente que se eligió se verifica el consumo de ancho de banda de los diferentes enlaces existentes para determinar si el consumo de ancho de banda es muy alto y cuál es el proceso que está provocando dicho consumo.		Técnico de monitoreo de Centro de Cómputo	Consolas de monitoreo	Componente identificado para monitoreo.	Consumo de Ancho de Banda Verificado			
8	Notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta de monitoreo o en su defecto el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo	Herramienta de Service Desk	Evento detectado	Notificación de evento a gestor de eventos en Service Desk	BITACORA DE EVENTOS		
9	Verificar errores en puertos de comunicación	Una vez dentro de la consola adecuada para el componente que se eligió se verifican los puertos de comunicación para determinar si el consumo de ancho de banda es muy alto y cuál es el proceso que está provocando dicho consumo.		Técnico de monitoreo de Centro de Cómputo	Consolas de monitoreo	Componente identificado para monitoreo.	Puertos de Comunicación Verificados			

CONTINÚA →

10	Notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta de monitoreo o en su defecto el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo.	Herramienta de Service Desk	Evento detectado	Notificación de evento a gestor de eventos en Service Desk	BITACORA DE EVENTOS		
11	Verificar estado de spools de troncales	Una vez dentro de la consola adecuada se verifica el estado de los spools para detectar algún problema existente.	pro_in_procedimiento para monitorear incidentes en central telefónica	Técnico de monitoreo de Centro de Cómputo	Telefonía: Omnivista 4760 7400 ISS Network Manager Center (NMC)	Componente identificado para monitoreo.	Troncal Verificada			
12	Notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta de monitoreo o en su defecto el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio. La herramienta de Service Desk cuenta con una base de conocimiento con guías y procedimientos de resolución de eventos conocidos y constituye el insumo para que el gestor de eventos pueda reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Notificación de evento a gestor de eventos en Service Desk	BITACORA DE EVENTOS		

4.3.14. Subproceso: Monitoreo de servidores y discos

#	Actividad	Descripción	Manuales de Detalle	Responsable	Sistema de Información	Entrada	Salida	Documento habilitante	Lineamiento de Proceso	Requerimientos
1	Determinar servidor a monitorear	El monitoreo que se realiza en el centro de cómputo es un monitoreo constante de todos los componentes que forman los servicios que ofrece la organización, para lo cual se cuenta con el software Barcelona y System Center Operations Manager (SCOM), en donde se crean las alarmas para el monitoreo automático de los servidores indicados en el listado: Monitoreo de servidores	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo	Barcelona04, SCOM	Necesidad de monitoreo	Servidores a monitorear identificados		Todo el monitoreo de servidores y discos lo debe realizar el técnico de monitoreo de Centro de Computo	Capacitación a los técnicos de monitoreo del Centro de Computo en labores de monitoreo de servidores distribuidos.
2	Ingresar a consola de monitoreo del servidor	Desde la consola de monitoreo se selecciona el componente donde están agrupados todos los servidores monitoreados el cual despliega un listado con el estado actual de todas los servidores.	Manuales del proveedor	Técnico de monitoreo Centro de Computo	Barcelona04, SCOM	Servidores a monitorear identificados	Consola de monitoreo arriba			
3	Verificar consumo de CPU del servidor	Para los servidores configurados en el monitoreo, se tiene una regla de salud en el que cambia de estado si el consumo del CPU supera el 80%	Manuales del proveedor	Técnico de monitoreo Centro de Computo	Barcelona04, SCOM	Consola de monitoreo arriba	Verificación automática del consumo de CPU			
4	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		
5	Verificar consumo de memoria RAM del servidor	Para los servidores configurados en el monitoreo, se tiene una regla de salud en el que cambia de estado si el consumo del memoria es mayor a 2000Mb En el caso del System Center Operations Manager (SCOM), está establecido un umbral de consumo del 80% y en el caso de ser superado este umbral envía un email en forma Automática a los Técnicos de monitoreo	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo	Barcelona04, SCOM	Listado de servidores identificado	Verificación automática del consumo de memoria			
6	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		

CONTINÚA →



7	Verificar espacio en disco asignado al servidor	Para los servidores configurados en el monitoreo, se tiene una regla de salud en el que cambia de estado si el porcentaje de disco utilizado supera el 90%  En el caso del System Center Operations Manager (SCOM), está establecido un umbral de consumo del 80% y en el caso de ser superado este umbral envía un email en forma Automática a los Técnicos de monitoreo.	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo	Barcelona04, SCOM	Listado de servidores identificado	Verificación automática del espacio en disco disponible			
8	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		
9	Verificar disponibilidad de disco asignado al servidor	Para los servidores que tienen asignados discos en el IBM Storwize V7000 (storage) se ingresa vía web a la consola del IBM Storwize V7000 y se procede a verificar la disponibilidad de los discos asignados a los servidores.	Manuales del proveedor	Técnico de monitoreo Centro de Computo	IBM Storwize V7000	Listado de servidores identificado	Verificación en discos asignados al servidor disponibles			
10	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		
11	Verificar logs del sistema operativo	Para revisar los logs del Sistema operativo el Técnico de monitoreo tiene dos opciones. En el caso de Sistemas Operativos Windows se debe ingresar al Visor de Sucesos en el cual se registran todos los problemas que puede tener el Sistema Operativo o alguna aplicación instalada, se procede a revisar los logs y en caso de que existan problemas se debe reportar al gestor de eventos. Para el caso de Sistemas Operativos Linux y AIX de debe ingresar a la carpeta de Logs para revisar los logs y en caso de que exista problemas se debe reportar al gestor de eventos.		Técnico de monitoreo Centro de Computo	Visor de Sucesos Windows  Carpeta de Logs Sistemas Operativos Linux y AIX	Listado de servidores identificado	Verificación de Logs en Sistema Operativo.			

CONTINÚA →

12	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.		Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente )	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		
----	---------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--------------------------------------------------------------------------------------	-----------------------------	------------------	--------------------------------------------------------------------------------	---------------------	--	--

4.3.15. Subproceso: Monitoreo de transacciones

#	Actividad	Descripción	Manuales de Detalle	Responsable	Sistema de Información	Entrada	Salida	Documento habilitante	Lineamiento de Proceso	Requerimientos
1	Ingresar a consola de monitoreo Barcelona 04	El monitoreo que se realiza en el centro de cómputo es un monitoreo constante de la variación de las transacciones que ingresan por el Centro Autorizador , para lo cual se cuenta con el software Barcelona en donde se crean las alarmas para el monitoreo automático de la transaccionalidad de los canales indicados en el listado: Monitoreo de transacciones Las alarmas son configuradas para garantizar la disponibilidad de los servicios que monitorea el Centro de Computo y a petición de las áreas encargadas de monitoreos específicos	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo	Barcelona04	Definición de canales transaccionales a monitorear	Listado de canales transaccionales identificados			
2	Monitorear canales transaccionales	Desde la consola de monitoreo se selecciona el componente donde están agrupados todos los canales transaccionales el cual despliega un listado con el estado actual de las transacciones. Se selecciona el canal específico para verificar de forma gráfica el estado de variación de las transacciones que ingresaron en el equipo Autorizador, en un determinado tiempo que es parametrizado en la herramienta.		Técnico de monitoreo Centro de Computo	Barcelona04	Listado de canales transaccionales identificados	Monitoreo continuo de la transaccionalidad			
3	Revisar transacciones manualmente	En el caso de que se presente una alarma que notifique la ausencia de transacciones, la primera acción es revisar manualmente desde el modulo grafico del autorizador que exista transaccionalidad en los servicios		Técnico de monitoreo Centro de Computo	Barcelona04	Monitoreo continuo de la transaccionalidad	Verificación manual del ingreso de transacciones al centro autorizador			
4	Gestionar o notificar evento al gestor de eventos	En caso de detectar un evento o alerta, la herramienta (automáticamente) o en su defecto el técnico de monitoreo debe gestionar el evento según los procedimientos establecidos de resolución para los eventos conocidos y que estén a su alcance. En caso de no poder reestablecer el servicio el técnico de monitoreo debe informar inmediatamente al Service Desk para que dicho evento sea escalado al gestor de eventos quien procede reestablecer el servicio.	pro_cc_procedimiento de monitoreo de servicios y aplicaciones	Técnico de monitoreo Centro de Computo / herramienta de monitoreo (automáticamente)	Herramienta de Service Desk	Evento detectado	Evento gestionado o notificación de evento a gestor de eventos en Service Desk	Bitácora de eventos		

4.3.16. Proceso: Gestión de problemas

#	Actividad	Descripción	Manuales	Responsable	Sistema de Información	Entrada	Salida	Documentación Habilitante	Lineamiento de Proceso	Requerimientos
1	Gestión de eventos	El proceso de Gestión de Eventos es la entrada al proceso de Gestión de Problemas. Todos aquellos eventos que no son solucionados por el gestor de eventos se convierten en problemas que deben ser atendidos por las áreas solucionadoras que a su vez se convierten o asumen el rol de gestor de problemas.		Gestor de Eventos de Service Desk	Herramienta de Service Desk	Evento gestionado sin solución aparente	Evento escalado por el gestor de eventos			Herramienta de Service Desk
2	Recibir requerimiento	El gestor de problemas (área solucionadora) recibe el requerimiento escalado del gestor de eventos a través de la herramienta de Service Desk. Según la criticidad del evento, el gestor de eventos puede notificar al gestor de problemas el requerimiento a través de mail, teléfono o verbalmente. No obstante, siempre se debe escalar el requerimiento a través de la herramienta de Service Desk dado que la información de resolución queda almacenada allí.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico)	Herramienta de Service Desk	Evento escalado por el gestor de eventos	Requerimiento recibido por el gestor de problemas a través de la herramienta de Service Desk		El gestor de problemas es el rol encargado de identificar la causa raíz de los incidentes que se hayan reportado.	Se requiere que la herramienta de Service Desk cuente con la facilidad de flujo de trabajo y escalamiento de requerimientos.
3	Revisar historial del requerimiento	Antes de proceder a solucionar el problema, el gestor de problemas debe revisar el historial de resolución de dicho problema para entender que se ha intentado anteriormente y que retroalimentación se ha registrado para de esa manera definir un punto de partida para el análisis del problema. Este historial reside en la herramienta de Service Desk y ha sido documentado allí por todos los entes que han estado involucrados en su resolución.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico)	Herramienta de Service Desk	Requerimiento recibido por el gestor de problemas a través de la herramienta de Service Desk	Historial del requerimiento revisado en la herramienta de Service Desk			
4	Analizar causa raíz del problema	Una vez revisado el historial del requerimiento, el gestor de problemas procede a encontrar y analizar la causa raíz del problema y la registra en la herramienta de Service Desk.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico)	Herramienta de Service Desk	Historial del requerimiento revisado en la herramienta de Service Desk	Causa raíz del problema identificada			
5	Solicitar apoyo del proveedor	En los casos en donde el gestor de problemas identifica una causa raíz que considera fuera de su alcance, este procede a solicitar apoyo externo a un proveedor experto en la materia. En los casos en donde exista un contrato de mantenimiento, el contacto con el proveedor puede ser directo. En caso contrario, se debe gestionar con el área de administrativo el contacto con el proveedor.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico)		Causa raíz del problema identificada	Solicitud de apoyo gestionada con el proveedor			

CONTINÚA →

6	Corregir problema con el proveedor	Cuando se requiere el apoyo de un proveedor externo, el gestor de problemas acompaña al proveedor durante la corrección del problema para asegurar los recursos que se requieran durante la solución y adicionalmente para adquirir el conocimiento del proveedor con respecto al tema en cuestión. La solución del problema debe quedar registrada en la herramienta de Service Desk.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking,)	Herramienta de Service Desk	Solicitud de apoyo gestionada con el proveedor	Problema corregido con el proveedor y registrado en la herramienta de Service Desk			
7	Corregir causa raíz del problema	Si el gestor de problemas no requiere apoyo externo de un proveedor, procede a corregir la causa raíz del problema basándose en su conocimiento del tema. La solución del problema debe quedar registrada en la herramienta de Service Desk.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico)	Herramienta de Service Desk	Causa raíz del problema identificada	Problema corregido por el gestor de problemas y registrado en la herramienta de Service Desk			
8	Verificar solución con involucrados	Una vez corregido el problema, ya sea con el apoyo de un proveedor externo o no, el gestor de problemas notifica y verifica con los involucrados o afectados por el problema, que el servicio haya sido restituido. El contacto con los involucrados puede ser por medio de mail, teléfono o verbalmente.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico, Proveedores)	Herramienta de Service Desk	Problema corregido y registrado en la herramienta de Service Desk	Corrección del problema notificada y verificada con los involucrados			
9	Cerrar requerimiento	Para formalizar el cierre de la solución del problema, el gestor de problemas cierra el requerimiento en la herramienta de Service Desk anotando cualquier comentario adicional que sea pertinente dejar registrado.		Gestor de problemas Áreas solucionadoras (Centro de Cómputo, Infraestructura y Networking, Control Tecnológico)	Herramienta de Service Desk	Corrección del problema notificada y verificada con los involucrados	Requerimiento cerrado en la herramienta de Service Desk			
10	Administración de cambios	El proceso de Administración de Cambios pertenece al área de Diseño del Servicio y es allí donde se gestionan los problemas relacionados con los códigos fuente de las aplicaciones. Durante este proceso el técnico stand by soluciona el problema y entrega el procedimiento o guía de solución del problema en cuestión de manera que el analista de conocimiento pueda actualizar la base de conocimiento en Service Desk.		Stand by Diseño del Servicio	Herramienta de Service Desk	Evento escalado por el gestor de eventos al Stand by de Diseño del Servicio	Problema solucionado por el stand by junto con procedimiento o guía de solución.			
11	Recibir del stand by procedimiento de solución del problema	En el caso en el que el problema haya sido escalado al área de Diseño del Servicio, el Analista de conocimiento recibe el procedimiento o guía de solución del problema generado por el Stand by. Dicho procedimiento o guía se recibe en formato digital.		Analista de conocimiento	Herramienta de Service Desk	Problema solucionado por el stand by junto con procedimiento o guía de solución.	Procedimiento o guía de solución recibido por el Analista de conocimiento			

CONTINÚA →

12	Actualizar base de conocimiento	Una vez conocida la solución al problema, el Analista de conocimiento procede a documentar dicha solución y posteriormente a actualizar la base de conocimiento en Service Desk. Los procedimientos o guías entregados por el área de Desarrollo simplemente se cargan a la base de conocimiento de Service Desk. Estos nuevos procedimientos o guías de solución se convierten ahora en los manuales de acción que utiliza el gestor de eventos para solucionar los eventos conocidos.		Analista de conocimiento	Herramienta de Service Desk	Procedimiento o guía de solución recibido por el Analista de conocimiento (caso stand by - Diseño del Servicio). Documentación de la solución del problema (caso gestor de problemas - Operación del Servicio)	Base de conocimiento actualizada en herramienta de Service Desk			
----	---------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--------------------------	-----------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------	--	--	--

4.4. SIPOC

A continuación se presenta el cuadro SIPOC de las mejoras encontradas en los procesos para la reestructuración del área de Operación del Servicio:

		S	I	P			O	C
Proceso Nuevo Modelo Operativo	Proceso actual	Proveedor	INPUTS	Actividad	Area	Responsable	OUTPUTS	CLIENTE
GESTIÓN DE LA DISPONIBILIDAD	MONITOREO DE SERVICIOS Y	BARCELONA04	INFORMACION EN LA CONSOLA	MONITOREO DE COMUNICACIONES	CENTRO DE COMPUTO	TECNICO 2 CC	INFORMACION DE MONITOREO	TECNICO 2 CC
		TECNICO 2 CC	INFORMACION DE MONITOREO	VERIFICA ENLACES Y EQUIPOS DE COMUNICACIONES	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	ENLACES OPERATIVOS	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SI: CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	NO: IDENTIFICA EQUIPO ENLACE CON PROBLEMA	CENTRO DE COMPUTO	TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	TECNICO 2 CC
		TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	NOTIFICA AL PROVEEDOR DE COMUNICACIONES Y NETWORKING	CENTRO DE COMPUTO	TECNICO 2 CC	MAIL O LLAMADA TELEFONICA	PROVEEDOR Y NETWORKING
		PROVEEDOR Y NETWORKING	MAIL O LLAMADA TELEFONICA	CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO INACTIVO	PROVEEDOR Y NETWORKING
GESTIÓN DE LA DISPONIBILIDAD	MONITOREO DE SERVICIOS Y	BARCELONA04	INFORMACION EN LA CONSOLA	MONITOREO DE SERVIDORES	CENTRO DE COMPUTO	TECNICO 2 CC	INFORMACION DE MONITOREO	TECNICO 2 CC
		TECNICO 2 CC	INFORMACION DE MONITOREO	VERIFICA SERVIDORES	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SERVIDORES OPERATIVOS	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SI: CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	NO: IDENTIFICA SERVIDOR CON PROBLEMA	CENTRO DE COMPUTO	TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	TECNICO 2 CC
		TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	NOTIFICA AL PROVEEDOR DE SERVIDOR Y NETWORKING	CENTRO DE COMPUTO	TECNICO 2 CC	MAIL O LLAMADA TELEFONICA	PROVEEDOR Y NETWORKING
		PROVEEDOR Y NETWORKING	MAIL O LLAMADA TELEFONICA	CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO INACTIVO	PROVEEDOR Y NETWORKING
GESTIÓN DE LA DISPONIBILIDAD	MONITOREO DE SERVICIOS Y	BARCELONA04	INFORMACION EN LA CONSOLA	MONITOREO DE APLICACIONES	CENTRO DE COMPUTO	TECNICO 2 CC	INFORMACION DE MONITOREO	TECNICO 2 CC
		TECNICO 2 CC	INFORMACION DE MONITOREO	VERIFICA APLICACIONES	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	APLICACIONES OPERATIVAS	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SI: CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	NO: IDENTIFICA APLICACION CON PROBLEMA	CENTRO DE COMPUTO	TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	TECNICO 2 CC
		TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	NOTIFICA AL SOPORTE EN STAND BY PARA SU REVISION	CENTRO DE COMPUTO	TECNICO 2 CC	MAIL O LLAMADA TELEFONICA	TECNICO EN STAND BY
		TECNICO EN STAND BY	MAIL O LLAMADA TELEFONICA	CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO INACTIVO	PROVEEDOR Y NETWORKING

		S	I	P			O	C
Proceso Nuevo Modelo Operativo	Proceso actual	Proveedor	INPUTS	Actividad	Area	Responsable	OUTPUTS	CLIENTE
GESTIÓN DE LA DISPONIBILIDAD	MONITOREO DE SERVICIOS Y	BARCELONA04	INFORMACION EN LA CONSOLA	MONITOREO DE EXPERIENCIA DE USUARIO	CENTRO DE COMPUTO	TECNICO 2 CC	INFORMACION DE MONITOREO	TECNICO 2 CC
		TECNICO 2 CC	INFORMACION DE MONITOREO	VERIFICA EXPERIENCIA DE USUARIO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	EXPERIENCIA DE USUARIO CORRECTA	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SI: CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	NO: IDENTIFICA SERVICIO CON PROBLEMA	CENTRO DE COMPUTO	TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	TECNICO 2 CC
		TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	NOTIFICA AL SOPORTE EN STAND BY PARA SU REVISION	CENTRO DE COMPUTO	TECNICO 2 CC	MAIL O LLAMADA TELEFONICA	TECNICO EN STAND BY
		TECNICO EN STAND BY	MAIL O LLAMADA TELEFONICA	CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO INACTIVO	PROVEEDOR Y NETWORKING
GESTIÓN DE LA DISPONIBILIDAD	MONITOREO DE SERVICIOS Y	BARCELONA04	INFORMACION EN LA CONSOLA	MONITOREA INDICADORES DE RENDIMIENTO	CENTRO DE COMPUTO	TECNICO 2 CC	INFORMACION DE MONITOREO	TECNICO 2 CC
		TECNICO 2 CC	INFORMACION DE MONITOREO	VERIFICA INDICADORES DE RENDIMIENTO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	INDICADORES CORRECTOS	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SI: CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	NO: IDENTIFICA INDICADOR CON PROBLEMA	CENTRO DE COMPUTO	TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	TECNICO 2 CC
		TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	NOTIFICA AL SOPORTE EN STAND BY PARA SU REVISION	CENTRO DE COMPUTO	TECNICO 2 CC	MAIL O LLAMADA TELEFONICA	TECNICO EN STAND BY
		TECNICO EN STAND BY	MAIL O LLAMADA TELEFONICA	CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO INACTIVO	PROVEEDOR Y NETWORKING
GESTIÓN DE LA DISPONIBILIDAD	MONITOREO DE SERVICIOS Y	MONITOREO DE MAQUINAS	INFORMACION EN LA CONSOLA	MONITOREO DE INFRAESTRUCTURA	CENTRO DE COMPUTO	TECNICO 2 CC	INFORMACION DE MONITOREO	TECNICO 2 CC
		TECNICO 2 CC	INFORMACION DE MONITOREO	VERIFICA DE UPS, PPC, AIRE ACONDICIONADO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	EQUIPOS FUNCIONAN CORRECTAMENTE	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD	SI: CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	TECNICO 2 CC
		TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL SERVICIO ACTIVO	NO: IDENTIFICA EQUIPO CON PROBLEMA	CENTRO DE COMPUTO	TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	TECNICO 2 CC
		TECNICO 2 CC	COMPONENTE EN ESTADO INACTIVO	NOTIFICA AL PROVEEDOR DE EQUIPOS Y ADMINISTRATIVO	CENTRO DE COMPUTO	TECNICO 2 CC	MAIL O LLAMADA TELEFONICA	PROVEEDOR Y ADMINISTRATIVO
		PROVEEDOR Y ADMINISTRATIVO	MAIL O LLAMADA TELEFONICA	CONTINUA CICLO DE MONITOREO	CENTRO DE COMPUTO	TECNICO 2 CC	ESTADO DE LA DISPONIBILIDAD DEL EQUIPO INACTIVO	PROVEEDOR Y ADMINISTRATIVO



		S	I	P			O	C
Proceso Nuevo Modelo Operativo	Proceso actual	Proveedor	INPUTS	Actividad	Area	Responsable	OUTPUTS	CLIENTE
GESTIÓN DE LA DISPONIBILIDAD	Monitoreo de Enlaces y Generación de Estadísticas	Gerencia Tecnología	Mail solicitud de informes semanales	<i>*Genera reporte de elaboración de estadísticas de los enlaces que se originan desde Quito</i>	Networking	Técnico 3 Networking	Creación de requerimiento en Remedy para elaboración de informes	Técnico 3 Networking
				Solicitud a Help Desk de creación de requerimiento en Remedy				
		Técnico 3 Networking	Creación de requerimiento para elaboración de informes	PD: Es elaboración de informe mensual?	Networking	Técnico 3 Networking	Informe mensual consolidado, Cierre de requerimiento en Remedy	Jefatura Networking
				SI: Consolida todos los informes semanales en uno solo y lo presenta el primer día del mes siguiente a su Línea de Supervisión				
				Depósito de informe semanal en repositorio común				
				Notificación a gerencia de informe depositado en repositorio común				
				Cierre de requerimiento en Remedy				
		Técnico 3 Networking	Creación de requerimiento para elaboración de informes	<b>*NO: Ingreso en herramienta de monitoreo y generación de reporte mediante sentencias SQL</b>	Networking	Técnico 3 Networking	Generación de información semanal	Técnico 3 Networking
		Técnico 3 Networking	Información semanal generada por herramienta	PD: Fin de mes se encuentra en la próxima semana?	Networking	Técnico 3 Networking	Elaboración de informe semanal, Notificación a gerencia de Networking vía mail de entrega de informe, Cierre de requerimiento en Remedy	Técnico 3 Networking Jefatura Networking
				*NO: Elabora informe semanal				
				Depósito de informe semanal en repositorio común				
				Notificación a gerencia de informe depositado en repositorio común				
				Cierre de requerimiento en Remedy				
		Técnico 3 Networking	Información semanal generada por herramienta	PD: Está próximo al siguiente miércoles día de reporte?	Networking	Técnico 3 Networking	Elaboración de informe semanal, Notificación a gerencia de Networking vía mail de entrega de informe, Cierre de requerimiento en Remedy	Técnico 3 Networking Jefatura Networking
				NO: Elabora informe semanal				
				Depósito de informe semanal en repositorio común				
				Notificación a gerencia de informe depositado en repositorio común				
				Cierre de requerimiento en Remedy				
		Técnico 3 Networking	Información semanal generada por herramienta	SI: Consultar a línea de supervisión fecha de corte para elaboración de informe	Networking	Técnico 3 Networking	Elaboración de informe semanal, Notificación a gerencia de Networking vía mail de entrega de informe, Cierre de requerimiento en Remedy	Técnico 3 Networking Jefatura Networking
				Depósito de informe semanal en repositorio común				
				Notificación a gerencia de informe depositado en repositorio común				
				Cierre de requerimiento en Remedy				

#### 4.5. Listado de ANS por proceso - Operación del Servicio

No.	Proceso	Subproceso	Descripción del servicio	Unidad Proveedora	Unidad Cliente	Descripción	Frecuencia Solicitud	Horarios	Formato Solicitud	Frecuencia Entrega	Formato Entrega	Nombre	%	Formulario	Fuente
1	Garantizar la seguridad de los sistemas	Paso a producción	Paso a producción	Control Tecnológico	Diseño del Servicio	Tiempo de paso de objetos, fuentes y SQL al ambiente de producción	Cuando se presente una necesidad de paso a producción	En horario laboral	Requerimiento en Service Desk	3 horas	Requerimiento en Service Desk	Electividad en paso a producción	95%	Requerimientos atendidos a tiempo / total de requerimientos en el mes	Barcelona 04
2	Garantizar la seguridad de los sistemas	Solicitud de respaldos	Entrega de cintas para recovery	Control Tecnológico	Centro de Cómputo	Tiempo de entrega de cintas de respaldo para ejecución de recovery	Cuando se presente una solicitud de respaldo	En horario laboral		3 horas	Requerimiento en Service Desk	Entrega de cintas para recovery	95%	Cintas entregadas a tiempo / total de cintas entregadas en el mes	Service Desk
3	Gestión de accesos	Matenimiento de usuarios	Aprobación de accesos	Control Tecnológico	Riesgo	Tiempo de aprobación para los accesos que deban ser validados por el área de Riesgo	Cuando se presente una solicitud de acceso	En horario laboral	Requerimiento en Service Desk	3 horas	Requerimiento en Service Desk	Aprobación de accesos	95%	Accesos aprobados a tiempo / total de accesos aprobados en el mes	Service Desk
4	Administración de la configuración	Mantenimiento de redes LAN	Instalación de puntos de red	Infraestructura y Networking	Administrativo	Tiempo de instalación de puntos de red	Cuando se presente una solicitud de punto de red que y no rse cuente con uno en la ubicación solicitada	En horario laboral	Orden de instalación física de punto de red	2 días	Mail	Instalación de puntos de red	95%	Puntos de red instalados a tiempo / total de puntos de red instalados en el mes	Service Desk
5	Administración de la mesa de servicio y los incidentes	Soporte a usuarios en Service Desk	Atención de requerimientos en Service Desk	Service Desk	Usuarios solicitantes	Tiempo de atención a requerimientos atendidos por Service Desk	Cuando se presente un requerimiento en el Service Desk	24X7	Requerimiento en Service Desk	Según solicitud (ver listado de tipificaciones de Service Desk)	Requerimiento en Service Desk	Atención de requerimientos en Service Desk	95%	Tipificaciones atendidas a tiempo / total de tipificaciones en el mes	Service Desk
6	Administración de operaciones	Procesamiento de transacciones y disponibilidad de la información	Notificación de finalización del proceso de avances	Centro de Cómputo	Facturación	Cumplimiento en la notificación de finalización del proceso de avances para ejecutar el traslado de las boletas	Diaria	24X7	e-mail	Por definir	e-mail	Notificación de finalización del proceso de avances	100%	Notificaciones a tiempo / total de notificaciones en el mes	e-mail
7	Administración de operaciones	Procesamiento de transacciones y disponibilidad de la información	Notificación de finalización del proceso de facturación	Facturación	Centro de Cómputo	Cumplimiento en la notificación de finalización del proceso de facturación para ejecutar el cierre diario.	Diaria	24X7	e-mail	Por definir	e-mail	Notificación de finalización del proceso de facturación	100%	Notificaciones a tiempo / total de notificaciones en el mes	e-mail
8	Administración de operaciones	Procesamiento de transacciones y disponibilidad de la información	Resolución de problemas en cierre diario	Centro de Cómputo	Diseño del Servicio	Resolución de problemas en cierre diario por parte del stand by del área de Diseño del Servicio	Diaria	24X7	Ticket en Service Desk	Por definir	Ticket en Service Desk	Resolución de problemas en cierre diario	100%	Problemas solucionados a tiempo / total de problemas en el mes	Herramienta de Service Desk
9	Administración de operaciones	Procesamiento de transacciones y disponibilidad de la información	Cierre diario	Centro de Cómputo	Negocio	Cumplimiento del cierre diario dentro del horario establecido	Diaria	24X7		Por definir	Reportes del proceso batch cargados en el sistema de gestión documental	Cierre diario	100%	Cierres diarios ejecutados a tiempo / total de cierres diarios en el mes	Reportes del proceso batch
10	Administración de operaciones	Servicio de back up	Ejecución de back up diario	Centro de Cómputo	Negocio	Cumplimiento en la ejecución de los back up diarios entre los que se incluye: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta equipos Gestor y CAO producción Perú 3) Cinta equipo DESARID, ambiente desarrollo 4) Cinta equipo F170, ambiente desarrollo 5) Cinta base de datos software Tivoli, ambiente de producción para plataformas distintas al AS400.	Diaria	En horario nocturno		Diaria antes de las 22 horas	Cinta de back up	Ejecución de back up diario	100%	Respaldos diarios ejecutados a tiempo / total de respaldos diarios en el mes	AS400, Tivoli
11	Administración de operaciones	Servicio de back up	Ejecución de back up semanal	Centro de Cómputo	Negocio	Cumplimiento en la ejecución de los back up semanales entre los que se incluye: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta equipos Gestor y CAO producción Perú 3) Cinta equipo DESARID, ambiente desarrollo 4) Cinta equipo F170, ambiente desarrollo 5) Cinta base de datos software Tivoli, ambiente de producción para plataformas distintas al AS400.	Semanal	En horario nocturno		Viernes antes de las 22 horas	Cinta de back up	Ejecución de back up semanal	100%	Respaldos semanales ejecutados a tiempo / total de respaldos semanales en el mes	AS400, Tivoli
12	Administración de operaciones	Servicio de back up	Ejecución de back up mensual	Centro de Cómputo	Negocio	Cumplimiento en la ejecución de los back up mensuales entre los que se incluye: 1) Cinta equipos Gestor y CAO producción Ecuador 2) Cinta equipos Gestor y CAO producción Perú 3) Cinta equipo DESARID, ambiente desarrollo 4) Cinta equipo F170, ambiente desarrollo 5) Cinta base de datos software Tivoli, ambiente de producción para plataformas distintas al AS400.	Mensual	En horario nocturno		Ultimo día del mes antes de las 22 horas	Cinta de back up	Ejecución de back up mensual	100%	Respaldos mensuales ejecutados a tiempo / total de respaldos mensuales en el año	AS400, Tivoli
13	Gestión de la continuidad de TI	Contingencia Autorizador	Contingencia Autorizador	Centro de Cómputo	Negocio	Garantizar la continuidad del servicio en caso de contingencia del Autorizador, en el tiempo establecido.	Cuando se presente una contingencia en el Autorizador	24X7		Por definir		Contingencia Autorizador	100%	Contingencias del Autorizador levantadas a tiempo / total de contingencias del Autorizador en el año	
14	Gestión de la continuidad de TI	Contingencia Gestor	Contingencia Gestor	Centro de Cómputo	Negocio	Garantizar la continuidad del servicio en caso de contingencia del Gestor, en el tiempo establecido.	Cuando se presente una contingencia en el Gestor	24X7		Por definir		Contingencia Gestor	100%	Contingencias del Gestor levantadas a tiempo / total de contingencias del Gestor en el año	
15	Gestión de la continuidad de TI	Contingencia Peoplesoft	Contingencia Peoplesoft	Centro de Cómputo	Negocio	Garantizar la continuidad del servicio en caso de contingencia del Peoplesoft, en el tiempo establecido.	Cuando se presente una contingencia en el Peoplesoft	24X7		Por definir		Contingencia Peoplesoft	100%	Contingencias del Peoplesoft levantadas a tiempo / total de contingencias del Peoplesoft en el año	
16	Evaluación y administración los riesgos de TI	Evaluación y administración los riesgos de TI	Evaluación de los riesgos de TI	Operación del Servicio	Gerencia de TI	Garantizar la evaluación de los riesgos asociados al ambiente de producción por lo menos una vez al año.	Anual	En horario laboral		Ultima semana del mes de enero	Matriz de riesgos y controles	Evaluación de los riesgos de TI	1	Cantidad de evaluaciones de riesgos asociados al ambiente de producción	

4.6. Listado de KPI's por proceso - Operación del Servicio

#	PROCESO	SUB PROCESO	NOMBRE DEL INDICADOR	INDICADOR (Fórmula matemática)	Unidad de Medida	¿Qué medir y por qué medir? Objetivo, propósito de la medición	Meta del indicador	¿Cuándo y cada cuánto se debe medir? Frecuencia	¿Cuál es la fuente de datos y el registro del indicador?	¿Cómo medir? (Solo para manuales)	Responsable de alimentar el indicador (solo para manuales)	Responsable de administrar el indicador
	<i>Indicar el Proceso asociado al indicador de desempeño (KPI)</i>	<i>Indicar el sub proceso asociado al indicador de desempeño (KPI)</i>	<i>Registrar los indicadores que se definieron en el Proceso. Cada indicador se debe nombrar de una manera concreta, que identifique el objetivo de su medición.</i>	<i>Definir la fórmula matemática del indicador. Las variables de medición deben ser las mismas (las mismas unidades de medida) tanto en el numerador como en el denominador (Ejm: # solicitudes atendidas / total de solicitudes).</i>	<i>Especificar la unidad en la cual se está midiendo el indicador; %, cantidad, volumen, fechas, etc.</i>	<i>Es el objetivo de hacer la medición del indicador.</i>	<i>Meta del indicador, definida en la misma unidad de medida del indicador (Real y cuantificable)</i>	<i>Es el momento en que se debe medir el indicador (momento en que se genera la información) y la frecuencia en la que se debe hacer.</i>	<i>Cual es la herramienta de la cual se debe obtener la información para el indicador. Para indicadores manuales aplica también para el lugar donde se debe realizar la medición y donde se debe registrar</i>	<i>Es la forma en que se miden los datos para la toma del indicador. En este punto se describen si existen unas tareas específicas o condiciones que deben garantizarse para llevar a cabo la medición</i>	<i>Es el cargo de la(s) persona(s) responsable(s) de alimentar y/o medir el indicador</i>	<i>Dueño del proceso o subproceso. Es quien toma decisiones de gestión de acuerdo a los resultados del indicador.</i>
1	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Pasos a producción	Cantidad de pasos a producción autorizados / total de pasos a producción	Porcentaje	Monitorear la cantidad de pasos a producción no autorizados	100%	Semanal	Barcelona 04		Analista de Control Tecnológico	Gerente de Control Tecnológico
2	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Violación a la política de transferencias	Cantidad de violaciones a la política de transferencias	Cantidad	Monitorear el número de violaciones a la política de transferencias	0	Semanal	Barcelona 04		Analista de Control Tecnológico	Gerente de Control Tecnológico
3	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Creación de usuarios en AS400	Cantidad de usuarios creados con autorización / total de usuarios creados	Porcentaje	Monitorear la creación de accesos no autorizados en el AS400	100%	Semanal	Barcelona 04		Analista de Control Tecnológico	Gerente de Control Tecnológico
4	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Eliminación de usuarios en AS400	Cantidad de usuarios eliminados con autorización / total de usuarios eliminados	Porcentaje	Monitorear la eliminación de accesos no autorizados en el AS400	100%	Semanal	Barcelona 04		Analista de Control Tecnológico	Gerente de Control Tecnológico
5	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Uso de claves administrativas	Cantidad de accesos autorizados con contraseña administrativas / total de accesos con contraseña administrativa	Porcentaje	Monitorear el uso no autorizados de claves administrativas	100%	Semanal	Barcelona 04		Analista de Control Tecnológico	Gerente de Control Tecnológico
6	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Ingresos fallidos	Cantidad de ingresos fallidos	Cantidad	Monitorear la cantidad de ingresos fallidos (ingresos que superan 3 intentos de acceso)	0	Semanal	Barcelona 04		Analista de Control Tecnológico	Gerente de Control Tecnológico
7	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Vulnerabilidades en la red interna y externa	Cantidad de vulnerabilidades en la red interna y externa	Cantidad	Monitorear la cantidad de vulnerabilidades detectadas en la red interna y externa	0	Semanal	McAfee Secure		Analista de Control Tecnológico	Gerente de Control Tecnológico
8	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Errores de conexión en VPN	Cantidad de errores de conexión en VPN	Cantidad	Monitorear la cantidad de errores de conexión en VPN	0	Semanal	Juniper VPN		Analista de Control Tecnológico	Gerente de Control Tecnológico
9	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Ataques a la red interna y externa	Cantidad de ataques a la red interna y externa no controlados a tiempo / total de ataques a la red interna y externa	Porcentaje	Monitorear los ataques a la red interna y externa de la organización	100%	Semanal	Site Protector IBM		Analista de Control Tecnológico	Gerente de Control Tecnológico
10	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Ataques a los portales web	Cantidad de ataques a los portales web no controlados a tiempo / total de ataques a los portales web	Porcentaje	Monitorear los ataques a los portales web de la organización	100%	Semanal	WAF		Analista de Control Tecnológico	Gerente de Control Tecnológico
11	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Fuga de información	Cantidad de archivos con información confidencial detectados en equipos no autorizados	Cantidad	Monitorear la fuga de información confidencial de la organización	0	Semanal	McAfee DLP		Analista de Control Tecnológico	Gerente de Control Tecnológico
12	Garantizar la seguridad de los sistemas	Monitoreo de seguridad	Acceso a periféricos	Accesos autorizados a periféricos / total de accesos a periféricos	Porcentaje	Monitorear el acceso a periféricos no autorizados	100%	Semanal	McAfee DLP		Analista de Control Tecnológico	Gerente de Control Tecnológico
13	Garantizar la seguridad de los sistemas	Administración de la seguridad de la información	Cifrado de discos	Discos cifrados / discos a cifrar según cronograma	Porcentaje	Monitorear la ejecución del cronograma de cifrado de discos	100%	Mensual	McAfee DLP Sophos		Analista de Control Tecnológico	Gerente de Control Tecnológico
14	Garantizar la seguridad de los sistemas	Administración de la seguridad de la información	Certificados digitales	Certificados digitales caducados sin renovación	Cantidad	Administrar la renovación de certificados digitales próximos a vencer.	0	Semanal	Open SSL		Analista de Control Tecnológico	Gerente de Control Tecnológico
15	Administración de la mesa de servicio y los incidentes	Soporte a usuarios en Service Desk	Tiempo de resolución de requerimientos en Service Desk	Tiempo medio para resolver un requerimiento (agrupado por categoría)	Cantidad	Monitorear el tiempo promedio de resolución de requerimientos en Service Desk	Por definir	Mensual	Service Desk		Sub gerente de Service Desk	Sub gerente de Service Desk
16	Administración de la mesa de servicio y los incidentes	Soporte a usuarios en Service Desk	Eficiencia de primera línea en Service Desk	Requerimientos resueltos en primera línea / total de requerimientos	Porcentaje	Monitorear la eficiencia de primera línea en Service Desk (resolución en primera línea)	70%	Mensual	Service Desk		Sub gerente de Service Desk	Sub gerente de Service Desk
17	Administración de la mesa de servicio y los incidentes	Soporte a usuarios en Service Desk	Eficiencia de Service Desk	Requerimientos resueltos en primera o segunda línea / total de requerimientos	Porcentaje	Monitorear la eficiencia en Service Desk (resolución en primera o segunda línea)	90%	Mensual	Service Desk		Sub gerente de Service Desk	Sub gerente de Service Desk
18	Administración de la mesa de servicio y los incidentes	Soporte a usuarios en Service Desk	Satisfacción de usuarios de Service Desk	Cantidad de calificaciones con rango satisfecho o muy satisfecho / total de calificaciones	Porcentaje	Monitorear la satisfacción de los usuarios de Service Desk (rango: insatisfecho, satisfecho, muy satisfecho)	80%	Mensual	Service Desk		Sub gerente de Service Desk	Sub gerente de Service Desk
19	Administración de la mesa de servicio y los incidentes	Soporte a usuarios en Service Desk	Satisfacción de operadores de Service Desk	Cantidad de calificaciones con rango satisfecho o muy satisfecho / total de calificaciones	Porcentaje	Monitorear la satisfacción de los operadores de Service Desk (rango: insatisfecho, satisfecho, muy satisfecho)	80%	Mensual	Service Desk		Sub gerente de Service Desk	Sub gerente de Service Desk
20	Administrar el desempeño y la capacidad	Administrar el desempeño y la capacidad	Capacidad instalada	Cantidad de incidentes ocurridos debido a falta de capacidad instalada	Cantidad	Monitorear la cantidad de incidentes debido a la falta de capacidad instalada de infraestructura de TI	0	Mensual	Service Desk		Técnico de monitoreo	Sub gerente de Infraestructura y Networking

#	PROCESO	SUB PROCESO	NOMBRE DEL INDICADOR	INDICADOR (Fórmula matemática)	Unidad de Medida	¿Qué medir y por qué medir? Objetivo, propósito de la medición	Meta del indicador	¿Cuándo y cada cuánto se debe medir? Frecuencia	¿Cuál es la fuente de datos y el registro del indicador ?	¿Cómo medir? (Solo para manuales)	Responsable de alimentar el indicador (solo para manuales)	Responsable de administrar el indicador
	Indicar el Proceso asociado al indicador de desempeño (KPI)	Indicar el sub proceso asociado al indicador de desempeño (KPI)	Registrar los indicadores que se definieron en el Proceso. Cada indicador se debe nombrar de una manera concreta, que identifique el objetivo de su medición.	Definir la fórmula matemática del indicador. Las variables de medición deben ser las mismas (las mismas unidades de medida) tanto en el numerador como en el denominador (Ejm: # solicitudes atendidas / total de solicitudes).	Especificar la unidad en la cual se está midiendo el indicador; %, cantidad, volumen, fechas, etc.	Es el objetivo de hacer la medición del indicador.	Meta del indicador, definida en la misma unidad de medida del indicador (Real y cuantificable)	Es el momento en que se debe medir el indicador (momento en que se genera la información) y la frecuencia en la que se debe hacer.	Cual es la herramienta de la cual se debe obtener la información para el indicador. Para indicadores manuales aplica también para el lugar donde se debe realizar la medición y donde se debe registrar	Es la forma en que se miden los datos para la toma del indicador. En este punto se describen si existen unas tareas específicas o condiciones que deben garantizarse para llevar a cabo la medición	Es el cargo de la(s) persona(s) responsable(s) de alimentar y/o medir el indicador	Dueño del proceso o subproceso. Es quien toma decisiones de gestión de acuerdo a los resultados del indicador.
21	Administrar el desempeño y la capacidad	Administrar el desempeño y la capacidad	Aumentos en capacidad no planeados	Cantidad de aumentos no planeados a la capacidad instalada	Cantidad	Monitorear la cantidad de aumentos no planeados a la capacidad instalada	0	Mensual	Plan anual de capacidad		Sub gerente de Centro de Cómputo	Sub gerente de Infraestructura y Networking
22	Administrar el desempeño y la capacidad	Administrar el desempeño y la capacidad	Presición de la proyección de capacidad	(Capacidad proyectada - Capacidad actual) / Capacidad proyectada	Porcentaje	Monitorear la diferencia entre la capacidad proyectada y la capacidad actual para asegurar un optimo uso de recursos y prevenir interrupciones del servicio. Se debe medir para cada componente o servicio proyectado	< 5%	Mensual	Plan anual de capacidad		Sub gerente de Centro de Cómputo	Sub gerente de Infraestructura y Networking
23	Gestión de la disponibilidad	Monitoreo de aplicaciones	Disponibilidad de las aplicaciones	Tiempo arriba / tiempo total	Porcentaje	Monitorear la disponibilidad de las aplicaciones instaladas para asegurar una entrega de servicio adecuada	99.9%	Mensual	Barcelona 04		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
24	Gestión de la disponibilidad	Monitoreo de servidores y discos	Disponibilidad de los servidores	Tiempo arriba / tiempo total	Porcentaje	Monitorear la disponibilidad de los servidores instalados para asegurar una entrega de servicio adecuada	99.9%	Mensual	Barcelona04, SCOM		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
25	Gestión de la disponibilidad	Monitoreo de servidores y discos	Consumo de CPU	Consumo de CPU / total de capacidad de CPU	Porcentaje	Monitorear el consumo de CPU de los servidores centrales y distribuidos	< 80%	Mensual	Barcelona04, SCOM		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
26	Gestión de la disponibilidad	Monitoreo de servidores y discos	Consumo de memoria RAM	Consumo de memoria RAM / total de memoria RAM instalada en el equipo	Porcentaje	Monitorear el consumo de memoria RAM de los servidores centrales y distribuidos	< 80%	Mensual	Barcelona04, SCOM		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
27	Gestión de la disponibilidad	Monitoreo de servidores y discos	Espacio en disco	Consumo de disco / total de capacidad de disco instalada en el equipo	Porcentaje	Monitorear el consumo de disco de los servidores centrales y distribuidos	< 80%	Mensual	Barcelona04, SCOM		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
28	Gestión de la disponibilidad	Monitoreo de centrales telefonicas, equipos de comunicación y enlaces	Disponibilidad de telefonía	Tiempo arriba / tiempo total	Porcentaje	Monitorear la disponibilidad de los equipos de telefonía instalados para asegurar una entrega de servicio adecuada	99.9%	Mensual	Comunicaciones: what up, PRTG, Solaris Wins, Putty, Cisco Network assistant, Cisco ASDM Telefonía: Omnivista 4760, 7400 ISS, Network Manager Center (NMC)		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
29	Gestión de la disponibilidad	Monitoreo de centrales telefonicas, equipos de comunicación y enlaces	Disponibilidad de enlaces	Tiempo arriba / tiempo total	Porcentaje	Monitorear la disponibilidad de los enlaces instalados para asegurar una entrega de servicio adecuada	99.9%	Mensual	Comunicaciones: what up, PRTG, Solaris Wins, Putty, Cisco Network assistant, Cisco ASDM Telefonía: Omnivista 4760, 7400 ISS, Network Manager Center (NMC)		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
30	Gestión de la disponibilidad	Monitoreo de centrales telefonicas, equipos de comunicación y enlaces	Disponibilidad de redes	Tiempo arriba / tiempo total	Porcentaje	Monitorear la disponibilidad de las redes instaladas para asegurar una entrega de servicio adecuada	99.9%	Mensual	Comunicaciones: what up, PRTG, Solaris Wins, Putty, Cisco Network assistant, Cisco ASDM Telefonía: Omnivista 4760, 7400 ISS, Network Manager Center (NMC)		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
31	Gestión de la disponibilidad	Monitoreo de centrales telefonicas, equipos de comunicación y enlaces	Consumo de procesamiento	Consumo de procesamiento / total de capacidad de procesamiento	Porcentaje	Monitorear el consumo de procesamiento en equipos de comunicaciones	< 80%	Mensual	Comunicaciones: what up, PRTG, Solaris Wins, Putty, Cisco Network assistant, Cisco ASDM Telefonía: Omnivista 4760, 7400 ISS, Network Manager Center (NMC)		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
32	Gestión de la disponibilidad	Monitoreo de centrales telefonicas, equipos de comunicación y enlaces	Tiempo de respuesta	Tiempo de respuesta equipos de comunicaciones	Cantidad	Monitorear el tiempo de respuesta de los equipos de comunicaciones	Por definir	Mensual	Comunicaciones: what up, PRTG, Solaris Wins, Putty, Cisco Network assistant, Cisco ASDM Telefonía: Omnivista 4760, 7400 ISS, Network Manager Center (NMC)		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
33	Gestión de la disponibilidad	Monitoreo de centrales telefonicas, equipos de comunicación y enlaces	Consumo de ancho de banda	Consumo de ancho de banda / total de ancho de banda asignado	Porcentaje	Monitorear el consumo de ancho de banda asignado a los enlaces de comunicación	Por definir	Mensual	Comunicaciones: what up, PRTG, Solaris Wins, Putty, Cisco Network assistant, Cisco ASDM Telefonía: Omnivista 4760, 7400 ISS, Network Manager Center (NMC)		Técnico de monitoreo	Sub gerente de Infraestructura y Networking
34	Gestión de la disponibilidad	Monitoreo de transacciones	Flujo transaccional	Cantidad de veces que el canal transaccional esta disponible pero no registra transacciones	Cantidad	Monitorear el flujo de transacciones de negocio a través de los canales indicados	0	Mensual	Barcelona 04		Técnico de monitoreo	Sub gerente de Centro de Cómputo

#### 4.7. Propuesta de la nueva Estructura para la Gerencia de Operación del Servicio

A continuación se presenta una propuesta de la nueva Estructura del área de Producción y Servicio.

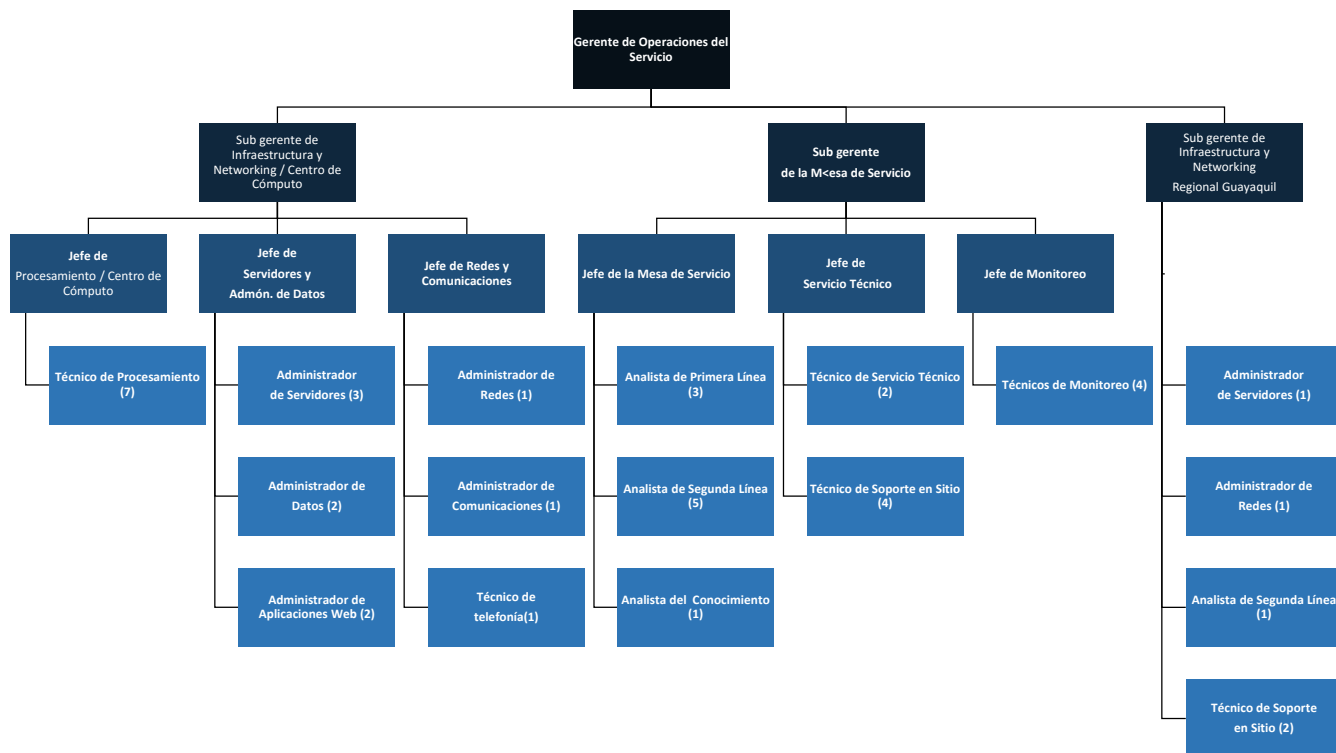


Figura 59. Nueva Estructura del área de productos y servicios

## CAPITULO V

### 5.1 Conclusiones.

- Se pudo identificar los procesos existentes dentro del área de Infraestructura y Networking, así como de las áreas de: Comunicaciones, Centro de Cómputo y Service Desk que son las que interactúan directamente con el área y comparten la mayoría de procesos.
- Mediante la identificación de los procesos existentes en el área se pudo consolidar los mismos para poder determinar cuáles procesos se encontraban redundantes entre las áreas ocasionando un desgaste tanto en recursos humanos como económicos.
- Con la consolidación de los procesos se realizó el respectivo análisis para poder determinar y optimizar el tiempo de cumplimiento de los mismos, estableciendo el cuadro de ANS.
- Con la obtención del SIPOC se logró determinar cuáles son los procesos a mejorar y ser transferibles dentro del área de Operación del Servicio donde se encontraría Infraestructura y Networking de acuerdo a la nueva estructura que se plantea como una mejora del área.

## 5.2 Recomendaciones

- Es necesario realizar un levantamiento continuo de los procesos existentes con el fin de mantener actualizado el cuadro de procesos encontrado.
- Se debe realizar una revisión continua de los procesos existentes y nuevos procesos que se vayan integrando al área para determinar si no se están creando procesos repetitivos que deban ser optimizados o eliminados.
- Se debe hacer un recorrido de procesos constante para determinar las mejores prácticas de los mismos y poder ir ajustando continuamente los ANS de los mismos, para poder tener unos procesos eficaces y eficientes.
- Se recomienda tomar en cuenta este estudio e iniciar con la reestructuración del área en un plazo no más allá de 2 meses ya que de ser mayor el tiempo los procesos podrían ir variando en el tiempo y quedar obsoletos.

**BIBLIOGRAFÍA**

Arevalo, L. (11 de Mayo de 2015). Gerente de Producción y Servicio. (V. Sarabia, Entrevistador)

Pleguazuelos, T. (1999). *Calidad total en la Administración Pública*. Granada: Unión Iberoamericana de Municipalidades.