UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

Título:

ELABORACIÓN DE UN MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2013 Y LEY DE PROTECCIÓN DE DATOS PERSONALES EN LA DIRECCIÓN DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL DEL SANTA

Tesis para Obtener el Título de

Ingeniero de Sistemas e Informática

Investigador:

BACH. JUAN CARLOS GUZMAN COMESAÑA

Asesor:

MG. HUGO ESTEBAN CASELLI GISMONDI

Nuevo Chimbote – Perú

2017

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas e Informática

TITULO

ELABORACIÓN DE UN MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2013 Y LEY DE PROTECCIÓN DE DATOS PERSONALES EN LA DIRECCIÓN DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL DEL SANTA

Tesis para optar el Título de Ingeniero de Sistemas e Informática

REVISADO Y APROBADO POR:

MG. HUGO ESTEBAN CASELLI GISMONDI

Asesor

NUEVO CHIMBOTE –PERU
2017

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas e Informática

TITULO

ELABORACIÓN DE UN MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2013 Y LEY DE PROTECCIÓN DE DATOS PERSONALES EN LA DIRECCIÓN DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL DEL SANTA

Tesis para optar el Título de Ingeniero de Sistemas e Informática

REVISADO Y APROBADO POR EL JURADO EVALUADOR:
Según Resolución N° 422-2017-UNS-CFI

----------	----------
Dr. Juan Pablo Sánchez Chávez	Mg. Hugo Esteban Caselli Gismondi
Presidente	Secretario
----------	----------
Ms. Camilo Ernesto Suárez Rebaza	Ms. Kene Abustamante Reyna Rojas
Integrante	Accesitario

NUEVO CHIMBOTE –PERU
2017

RESUMEN

El presente trabajo de investigación tiene como objetivo principal definir un Marco de Referencia para la Implementación de la Norma ISO/IEC 27001:2013 y Ley de Protección de Datos Personales en la Dirección de Admisión de la Universidad Nacional del Santa, para lo cual se plantea a través de un conjunto de fases documentadas las cuales serán evidenciadas con entregables por cada una de ellas.

A partir de éste informe de investigación se pretende establecer los procedimientos necesarios para una adecuada implementación de la Norma ISO/IEC 27001:2013 y Ley de Protección de Datos Personales con un enfoque basado en procesos y en riesgos.

Autor: Bach. Juan Carlos Guzman Comesaña

Asesor: Mg. Hugo Esteban Caselli Gismondi

ABSTRACT

The main objective of this research work is to define a Reference Framework for the Implementation of ISO / IEC 27001: 2013 and the Personal Data Protection Law in the Admission Office of the National University of Santa, for which purpose it is proposed through a set of documented phases which will be evidenced with deliverables for each one of them.

Based on this research report, we intend to establish the necessary procedures for an adequate implementation of ISO / IEC 2700z |ws1: 2013 and the Personal Data Protection Law with a process and risk based approach.

Author: Bach. Juan Carlos Guzman Comesaña

Adviser: Mg. Hugo Esteban Caselli Gismondi

Agradecimientos

A DIOS, por haberme dado sabiduría, fortaleza, salud, coraje, y no dejarme solo en los momentos difíciles. Principalmente por permitirme realizar uno de mis sueños en mi vida.

A mis padres, Rember el cual me observa y guía mi porvenir desde los cielos y Ana por ayudarme en la realización de mi proyecto de vida y hacer que verdaderamente crea en mí. Gracias por todo su amor, por su comprensión y por haberlo dado todo para darme la mejor educación. Ustedes hicieron que todo esto fuera posible, a ustedes les debo gran parte de lo que soy.

A mi pareja Annie y nuestro hijo André Joaquín, por ser el motor de mi vida por su amor, cariño, comprensión y paciencia.

A mi asesor de Tesis el Mg. Hugo Esteban Caselli Gismondi por su amabilidad, buena disposición, paciencia, por el tiempo que me dedico para que este trabajo culminara exitosamente, mi agradecimiento sincero por ser mi maestro y mentor, gracias por su confianza e invaluable apoyo.

A mis compañeros de universidad que luego de afrontar muchos retos juntos más que sólo compañeros se convirtieron en amigos para toda la vida.

ÍNDICE

ÍNDICE I
LISTA DE FIGURAS III
LISTA DE TABLAS VII
PRESENTACIÓN 9
CAPITULO I: LA INSTITUCIÓN 10
1.1. RESEÑA HISTÓRICA. 10
1.2. IDENTIFICACIÓN DE LA INSTITUCIÓN 10
1.3. MISION 11
1.4. VISION 11
1.5. PRINCIPIOS 11
1.6. OBJETIVOS 12
1.7. ORGANIZACIÓN 12
CAPITULO II: PLAN DE INVESTIGACIÓN 14
2.1. EL PLANTEAMIENTO DEL PROBLEMA 14
2.1.1. Realidad Problemática 14
2.1.2. Formulación del Problema 16
2.2. ANTECEDENTES DEL PROBLEMA 16
2.2.1. Antecedentes Locales 16
2.2.2. Antecedentes Nacionales 16
2.2.3. Antecedentes Internacionales 17
2.3. JUSTIFICACIÓN 18
2.4. IMPORTANCIA DE LA INVESTIGACION 19
2.5. OBJETIVOS 19
2.5.1. Objetivo General 19
2.5.2. Objetivos Específicos 19
2.6. METODOLOGÍA 20
CAPITULO III: MARCO REFERENCIAL 21
3.1. MARCO TEORICO 21
3.1.1. MARCO DE REFERENCIA 21
3.1.2. DEFINICIONES ESPECÍFICAS PARA EL SGSI SEGÚN LA NORMA ISO/IEC 27001:2013 21
3.1.3. ESTANDARES INVOLUCRADOS 24
3.1.4. LEY DE PROTECCIÓN DE DATOS PERSONALES 26
3.1.5. BUSINESS PROCESS MODEL AND NOTATION (BPMN) 28
3.1.6. OTROS REFERENTES 29
CAPITULO IV: MATERIALES Y METODOS 30
4.1. HIPÓTESIS 30
4.2. MÉTODO DE INVESTIGACIÓN 30
4.3. DISEÑO DE INVESTIGACIÓN 30
4.4. POBLACIÓN 31
4.5. TIPO DE MUESTREO 31
4.6. MUESTRA 31
4.7. TÉCNICAS E INSTRUMENTOS 31
CAPITULO V: RESULTADOS 32
5.1 FASE I- ANÁLISIS, DISEÑO Y DOCUMENTACIÓN DEL PROCESO DE ADMISIÓN DE PREGRADO 32
5.1.1 Objetivos de la Fase I 32
5.1.2 Marco de Trabajo de la Fase I 32
5.1.3 Desarrollo de la Fase I 32

5.2 FASE II- ANÁLISIS, DISEÑO Y DOCUMENTACIÓN PARA CLASIFICAR BANCOS DE DATOS PERSONALES 201
5.2.1 Objetivos de la Fase 2 201
5.2.2 Marco de Trabajo de la Fase 2 201
5.2.3 Desarrollo de la Fase 2 201
5.3 FASE III - ANÁLISIS DE BRECHAS 216
5.3.1 Objetivos de la Fase III 216
5.3.2 Marco de Trabajo la Fase III 216
5.3.3 Desarrollo de Fase la 3 216
5.4 FASE IV – METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 223
5.4.1 Objetivos de la Fase IV 223
5.4.2 Marco de Trabajo de la Fase IV 223
5.4.3 Desarrollo de la Fase IV 223
5.5 FASE V – ELABORACIÓN DE AVISO DE PRIVACIDAD Y PROCEDIMIENTO DE DERECHOS ARCO 233
5.5.1 Objetivos de la Fase V 233
5.5.2 Marco de Trabajo de la Fase V 233
5.5.3 Desarrollo de la Fase V 233
CAPITULO VI: DISCUSIÓN 241
6.1. CALIDAD DE LA VALIDEZ INTERNA 241
6.2. CALIDAD DE LA VALIDEZ EXTERNA 241
6.2.1. IMPLEMENTACIÓN DEL MÉTODO DELPHI 241
6.2.2. RESULTADOS DEL MÉTODO DELPHI 245
6.2.3. LISTADO DE EXPERTOS 250
CONCLUSIONES 251
RECOMENDACIONES 253
REFERENCIAS BIBLIOGRÁFICAS 254
ANEXOS 256

LISTA DE FIGURAS

Figura N° 1: Organigrama de la UNS....13
Figura N° 2: Diseño no Experimental según el paradigma Ex Post Facto....30
Figura N° 3: Notación BPMN 2.0 de la Herramienta Bizagi....35
Figura N° 4: PM01- Diagrama BPMN 2.0....41
Figura N° 5: PM01.01 (General) - Diagrama BPMN 2.0....45
Figura N° 6: PM01.01 (Parte 1) - Diagrama BPMN 2.0....46
Figura N° 7: PM01.01 (Parte 2) - Diagrama BPMN 2.0....47
Figura N° 8: PM01.01 (Parte 3) - Diagrama BPMN 2.0....48
Figura N° 9: PM01.01.01 - Diagrama BPMN 2.0....51
Figura N° 10: PM01.01.01.01 (General) - Ficha de Proceso....54
Figura N° 11: PM01.01.01.01 (Parte 1) - Ficha de Proceso....55
Figura N° 12: PM01.01.01.01 (Parte 2) - Ficha de Proceso....56
Figura N° 13: PM01.01.01.01 (Parte 3) - Ficha de Proceso....57
Figura N° 14: PM01.01.01.01 (Parte 4) - Ficha de Proceso....58
Figura N° 15: PM01.01.01.02 (General) - Diagrama BPMN 2.0....60
Figura N° 16: PM01.01.01.02 (Parte 1) - Diagrama BPMN 2.0....61
Figura N° 17: PM01.01.01.02 (Parte 2) - Diagrama BPMN 2.0....62
Figura N° 18: PM01.01.01.02 (Parte 3) - Diagrama BPMN 2.0....63
Figura N° 19: PM01.01.01.02 (Parte 4) - Diagrama BPMN 2.0....64
Figura N° 20: PM01.01.01.03 (General) - Diagrama BPMN 2.0....66
Figura N° 21: PM01.01.01.03 (Parte 1) - Diagrama BPMN 2.0....67
Figura N° 22: PM01.01.01.03 (Parte 2) - Diagrama BPMN 2.0....68
Figura N° 23: PM01.01.01.03 (Parte 3) - Diagrama BPMN 2.0....69
Figura N° 24: PM01.01.01.03 (Parte 4) - Diagrama BPMN 2.0....70
Figura N° 25: PM01.01.01.04 (General) - Diagrama BPMN 2.0....73
Figura N° 26: PM01.01.01.04 (Parte 1) - Diagrama BPMN 2.0....74
Figura N° 27: PM01.01.01.04 (Parte 2) - Diagrama BPMN 2.0....75
Figura N° 28: PM01.01.01.04 (Parte 3) - Diagrama BPMN 2.0....76
Figura N° 29: PM01.01.01.04 (Parte 4) - Diagrama BPMN 2.0....77
Figura N° 30: PM01.01.01.04 (Parte 5) - Diagrama BPMN 2.0....78
Figura N° 31: PM01.01.01.04 (Parte 6) - Diagrama BPMN 2.0....79
Figura N° 32: PM01.01.02 (General) - Diagrama BPMN 2.0....82
Figura N° 33: PM01.01.02 (Parte 1) - Diagrama BPMN 2.0....83
Figura N° 34: PM01.01.02 (Parte 2) - Diagrama BPMN 2.0....84
Figura N° 35 : PM01.01.02.01 (General) - Diagrama BPMN 2.0....86
Figura N° 36: PM01.01.02.01 (Parte 1) - Diagrama BPMN 2.0....87
Figura N° 37: PM01.01.02.01 (Parte 2) - Diagrama BPMN 2.0....88
Figura N° 38: PM01.01.02.02 (General) - Diagrama BPMN 2.0....90
Figura N° 39: PM01.01.02.02 (Parte 1) - Diagrama BPMN 2.0....91
Figura N° 40: PM01.01.02.02 (Parte 2) - Diagrama BPMN 2.0....92
Figura N° 41: PM01.01.02.02 (Parte 3) - Diagrama BPMN 2.0....93
Figura N° 42: PM01.01.02.02 (Parte 4) - Diagrama BPMN 2.0....94
Figura N° 43: PM01.01.02.03 (General) - Diagrama BPMN 2.0....96

Figura N° 44: PM01.01.02.03 (Parte 1) - Diagrama BPMN 2.0 97
Figura N° 45: PM01.01.02.03 (Parte 2) - Diagrama BPMN 2.0 98
Figura N° 46: PM01.01.02.03 (Parte 3) - Diagrama BPMN 2.0 99
Figura N° 47: PM01.01.02.04 (General) - Diagrama BPMN 2.0 101
Figura N° 48: PM01.01.02.04 (Parte 1) - Diagrama BPMN 2.0 102
Figura N° 49: PM01.01.02.04 (Parte 2) - Diagrama BPMN 2.0 103
Figura N° 50: PM01.01.02.05 (General) - Diagrama BPMN 2.0 105
Figura N° 51: PM01.01.02.05 (Parte 1) - Diagrama BPMN 2.0 106
Figura N° 52: PM01.01.02.05 (Parte 2) - Diagrama BPMN 2.0 107
Figura N° 53: PM01.01.03 - Ficha de Proceso 110
Figura N° 54: PM01.01.03.01 (General) - Diagrama BPMN 2.0 112
Figura N° 55: PM01.01.03.01 (Parte 1) - Diagrama BPMN 2.0 113
Figura N° 56: PM01.01.03.01 (Parte 2) - Diagrama BPMN 2.0 114
Figura N° 57: PM01.01.03.02 (General) - Diagrama BPMN 2.0 117
Figura N° 58: PM01.01.03.02 (Parte 1) - Diagrama BPMN 2.0 118
Figura N° 59: PM01.01.03.02 (Parte 2) - Diagrama BPMN 2.0 119
Figura N° 60: PM01.01.03.02 (Parte 3) - Diagrama BPMN 2.0 120
Figura N° 56: PM01.01.03.03 - Diagrama BPMN 2.0 122
Figura N° 62: PM01.01.03.03 (Parte 1) - Diagrama BPMN 2.0 123
Figura N° 63: PM01.01.03.03 (Parte 2) - Diagrama BPMN 2.0 124
Figura N° 64: PM01.01.03.03 (Parte 3) - Diagrama BPMN 2.0 125
Figura N° 65: PM01.01.04 (General) - Diagrama BPMN 2.0 128
Figura N° 66: PM01.01.04 (Parte 1) - Diagrama BPMN 2.0 129
Figura N° 67: PM01.01.04 (Parte 2) - Diagrama BPMN 2.0 130
Figura N° 68: PM01.01.04.01 - Diagrama BPMN 2.0 132
Figura N° 69: PM01.01.04.01 (Parte 1) - Diagrama BPMN 2.0 133
Figura N° 70: PM01.01.04.01 (Parte 1) - Diagrama BPMN 2.0 134
Figura N° 71:PM01.01.04.02 - Diagrama BPMN 2.0 137
Figura N° 72: PM01.01.04.02 (Parte 1) - Diagrama BPMN 2.0 138
Figura N° 73: PM01.01.04.02 (Parte 1) - Diagrama BPMN 2.0 139
Figura N° 74: PM01.01.04.02 (Parte 2) - Diagrama BPMN 2.0 140
Figura N° 75: PM01.01.04.02 (Parte 3) - Diagrama BPMN 2.0 141
Figura N° 76: PM01.01.04.02 (Parte 4) - Diagrama BPMN 2.0 142
Figura N° 77: PM01.01.04.02 (Parte 5) - Diagrama BPMN 2.0 143
Figura N° 78: PM01.01.04.03 - Diagrama BPMN 2.0 146
Figura N° 79: PM01.01.04.03 (Parte 1) - Diagrama BPMN 2.0 147
Figura N° 80: PM01.01.04.03 (Parte 2) - Diagrama BPMN 2.0 148
Figura N° 81: PM01.01.04.03 (Parte 3) - Diagrama BPMN 2.0 149
Figura N° 82: PM01.01.04.04 (General) - Diagrama BPMN 2.0 153
Figura N° 83: PM01.01.04.04 (Parte 1) - Diagrama BPMN 2.0 154
Figura N° 84: PM01.01.04.04 (Parte 2) - Diagrama BPMN 2.0 155
Figura N° 85: PM01.01.04.04 (Parte 3) - Diagrama BPMN 2.0 156
Figura N° 86: PM01.01.04.04 (Parte 4) - Diagrama BPMN 2.0 157
Figura N° 87: PM01.01.04.04 (Parte 5) - Diagrama BPMN 2.0 158
Figura N° 62: PM01.01.04.05 - Diagrama BPMN 2.0 161
Figura N° 89: PM01.01.04.05 (Parte 1) - Diagrama BPMN 2.0 162

Figura N° 90: PM01.01.04.05 (Parte 2) - Diagrama BPMN 2.0 163
Figura N° 91: PM01.01.04.05 (Parte 3) - Diagrama BPMN 2.0 164
Figura N° 92: PM01.01.05 (General) - Diagrama BPMN 2.0 167
Figura N° 93: PM01.01.05 (Parte 1) - Diagrama BPMN 2.0 168
Figura N° 94: PM01.01.05 (Parte 2) - Diagrama BPMN 2.0 169
Figura N° 95: PM01.01.05.01 - Diagrama BPMN 2.0 171
Figura N° 96: PM01.01.05.01 (Parte 1) - Diagrama BPMN 2.0 172
Figura N° 97: PM01.01.05.01 (Parte 2) - Diagrama BPMN 2.0 173
Figura N° 98: PM01.01.05.02 (General) - Diagrama BPMN 2.0 175
Figura N° 99: PM01.01.05.02 (Parte 1) - Diagrama BPMN 2.0 176
Figura N° 100: PM01.01.05.02 (Parte 2) - Diagrama BPMN 2.0 177
Figura N° 101: PM01.01.05.03 - Diagrama BPMN 2.0 179
Figura N° 102: PM01.01.05.03 (Parte 1) - Diagrama BPMN 2.0 180
Figura N° 103: PM01.01.05.03 (Parte 2) - Diagrama BPMN 2.0 181
Figura N° 104: PM01.01.06 (General) - Diagrama BPMN 2.0 184
Figura N° 105: PM01.01.06 (Parte 1) - Diagrama BPMN 2.0 185
Figura N° 106: PM01.01.06 (Parte 2) - Diagrama BPMN 2.0 186
Figura N° 107: PM01.01.06.01 (General) - Diagrama BPMN 2.0 188
Figura N° 108: PM01.01.06.01 (Parte 1) - Diagrama BPMN 2.0 189
Figura N° 109: PM01.01.06.01 (Parte 2) - Diagrama BPMN 2.0 190
Figura N° 110: PM01.01.06.01 (Parte 3) - Diagrama BPMN 2.0 191
Figura N° 111: PM01.01.06.01 (Parte 4) - Diagrama BPMN 2.0 192
Figura N° 112: PM01.01.06.02 (General) - Diagrama BPMN 2.0 194
Figura N° 113: PM01.01.06.02 (Parte 1) - Diagrama BPMN 2.0 195
Figura N° 114: PM01.01.06.02 (Parte 2) - Diagrama BPMN 2.0 196
Figura N° 115: PM01.01.06.03 (General) - Diagrama BPMN 2.0 198
Figura N° 116: PM01.01.06.03 (Parte 1) - Diagrama BPMN 2.0 199
Figura N° 117: PM01.01.06.03 (Parte 2) - Diagrama BPMN 2.0 200
Figura N° 118: PE04.01.02.01 - Diagrama BPMN 2.0 204
Figura N° 119: PE04.01.02.01 (Parte 1) - Diagrama BPMN 2.0 205
Figura N° 120: PE04.01.02.01 (Parte 2) - Diagrama BPMN 2.0 206
Figura N° 121: PE04.01.02.01 (Parte 3) - Diagrama BPMN 2.0 207
Figura N° 122: PE04.01.02.01 (Parte 4) - Diagrama BPMN 2.0 208
Figura N° 123: PE04.01.02.01 (Parte 5) - Diagrama BPMN 2.0 209
Figura N° 124: PE04.01.02.01 (Parte 6) - Diagrama BPMN 2.0 210
Figura N° 125: Grafico de Radar de cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013 217
Figura N° 126: Grafico de Radar de cumplimiento de los controles de la Norma ISO/IEC 27002:2013 221
Figura N° 127: Grafico de Barras de cumplimiento de los controles a nivel de dominio del Anexo A de la Norma ISO/IEC 27001:2013 222
Figura N° 128: PE04.01.01.01 (General) - Diagrama BPMN 2.0 227
Figura N° 129: PE04.01.01.01 (Parte 1) - Diagrama BPMN 2.0 228
Figura N° 130: PE04.01.01.01 (Parte 2) - Diagrama BPMN 2.0 229
Figura N° 131: PE04.01.01.01 (Parte 3) - Diagrama BPMN 2.0 230
Figura N° 132: PE04.01.01.01 (Parte 4) - Diagrama BPMN 2.0 231

Figura N° 133: PE04.01.01.01 (Parte 5) - Diagrama BPMN 2.0 232
Figura N° 134: PE04.01.02.02 (General) - Diagrama BPMN 2.0 236
Figura N° 135: PE04.01.02.02 (Parte 1) - Diagrama BPMN 2.0 237
Figura N° 136: PE04.01.02.02 (Parte 2) - Diagrama BPMN 2.0 238
Figura N° 137: PE04.01.02.02 (Parte 3) - Diagrama BPMN 2.0 239
Figura N° 138: PE04.01.02.02 (Parte 4) - Diagrama BPMN 2.0 240
Figura N° 139: Bloque I-Pregunta N°1 245
Figura N° 140: Bloque II-Pregunta N°2 246
Figura N° 141: Bloque III-Pregunta N°3 246
Figura N° 142: Bloque III-Pregunta N°4 247
Figura N° 143: Bloque III-Pregunta N°5 247
Figura N° 144: Bloque IV-Pregunta N°6 248
Figura N° 145: Bloque IV-Pregunta N°7 248
Figura N° 146: Bloque V-Pregunta N°8 249
Figura N° 147: Bloque V-Pregunta N°9 249

LISTA DE TABLAS

Tabla N° 1: Cuestionario de referencia para la recolección de la información. 32
Tabla N° 2: Formato para Inventario de Procesos 33
Tabla N° 3: Formato para Inventario de Procedimientos 34
Tabla N° 4: Inventario de Procesos 36
Tabla N° 5: PM01 - Ficha de Proceso 38
Tabla N° 6: PM01.01- Ficha de Proceso 42
Tabla N° 7: PM01.01.01 - Ficha de Proceso 49
Tabla N° 8: PM01.01.01.01- Ficha de Proceso 52
Tabla N° 9: PM01.01.01.02- Ficha de Proceso 59
Tabla N° 10: PM01.01.01.03- Ficha de Proceso 65
Tabla N° 11: PM01.01.01.04- Ficha de Proceso 71
Tabla N° 12: PM01.01.02 - Ficha de Proceso 80
Tabla N° 13: PM01.01.02.01 - Ficha de Proceso 85
Tabla N° 14: PM01.01.02.02 - Ficha de Proceso 89
Tabla N° 15: PM01.01.02.03 - Ficha de Proceso 95
Tabla N° 16: PM01.01.02.04 - Ficha de Proceso 100
Tabla N° 17: PM01.01.02.05 - Ficha de Proceso 104
Tabla N° 18: PM01.01.02.05 - Ficha de Proceso 108
Tabla N° 19: PM01.01.03.01 - Ficha de Proceso 111
Tabla N° 20: PM01.01.03.02 - Ficha de Proceso 115
Tabla N° 21: PM01.01.03.03 - Ficha de Proceso 121
Tabla N° 22: PM01.01.04 - Ficha de Proceso 126
Tabla N° 23: PM01.01.04.01 - Ficha de Proceso 131
Tabla N° 24: PM01.01.04.02 - Ficha de Proceso 135
Tabla N° 25: PM01.01.04.03 - Ficha de Proceso 144
Tabla N° 26: PM01.01.04.04 - Ficha de Proceso 150
Tabla N° 27: PM01.01.04.05 - Ficha de Proceso 159
Tabla N° 28: PM01.01.05 - Ficha de Proceso 165
Tabla N° 29: PM01.01.05.01 - Ficha de Proceso 170
Tabla N° 30: PM01.01.05.02 - Ficha de Proceso 174
Tabla N° 31: PM01.01.05.03 - Ficha de Proceso 178
Tabla N° 32: PM01.01.06 - Ficha de Proceso 182
Tabla N° 33: PM01.01.06.01 - Ficha de Proceso 187
Tabla N° 34: PM01.01.06.02 - Ficha de Proceso 193
Tabla N° 35: PM01.01.06.03 - Ficha de Proceso 197
Tabla N° 36: PE04.01.02.01 - Ficha de Proceso 202
Tabla N° 37: Criterios para Clasificar Banco de Datos Personales 210
Tabla N° 38: Inventario de Banco de Datos Personales 212
Tabla N° 39: Nivel de Madurez adaptado para la Seguridad de la Información 216
Tabla N° 40: Nivel de Cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013 217
Tabla N° 41: Nivel de Cumplimiento de los 114 Controles de la Norma ISO/IEC 27002:2013 218

Tabla N° 42: PE04.01.01.01 - Ficha de Proceso 224
Tabla N° 43: PE04.01.02.02 - Ficha de Proceso 234
Tabla N° 44: Formato de Encuesta Método Delphi 243
Tabla N° 45: Valoración de Escala Likert 244
Tabla N° 46: Registro de Expertos 250

PRESENTACIÓN

Señores miembros del jurado:

En cumplimiento a lo dispuesto por el Reglamento General de Grados y Títulos de la Universidad Nacional del Santa, pongo a vuestra consideración el presente Informe de Trabajo de Investigación intitulado: **ELABORACIÓN DE UN MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2013 Y LEY DE PROTECCIÓN DE DATOS PERSONALES EN LA DIRECCIÓN DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL DEL SANTA.** Con el propósito de cumplir con los requisitos para optar el Título Profesional de Ingeniero de Sistemas e Informática.

Esperando que el presente cumpla los criterios evaluativos y de esta manera obtenga su aprobación.

Atentamente.

Bach. Juan Carlos Guzman Comesaña

CAPITULO I: LA INSTITUCIÓN

1.1. RESEÑA HISTÓRICA.

La Universidad Nacional del Santa, creada por Ley Nº 24035 del 20 de diciembre de 1984, es persona jurídica de derecho público. Se rige fundamentalmente por la Constitución Política del Perú, la Ley Universitaria Nº 30220, el Estatuto y sus Reglamentos.

La Universidad Nacional del Santa es una comunidad académica orientada a la investigación, docencia, extensión cultural y proyección social que brinda una formación humanista, científica y tecnológica con clara conciencia de nuestro país como realidad multicultural. Adopta el concepto de educación como derecho fundamental y servicio público esencial. Está integrada por docentes, estudiantes y graduados.

La Universidad Nacional del Santa ha sido concebida, desde su creación, como universidad para el desarrollo, con clara conciencia de su compromiso con el bienestar y la justicia social, su respeto por la ciencia y la cultura y la necesidad de su aporte al progreso del país y de la región, reconociendo los valores imprescriptibles de la libertad y la dignidad humana, los cimientos de la cultura nacional que hacen de la identidad del pueblo peruano, y la integración armónica de los sectores sociales que la componen.

1.2. IDENTIFICACIÓN DE LA INSTITUCIÓN

1.2.1. Denominación de la Institución

Universidad Nacional del Santa

1.2.2. Domicilio Legal

Av. Pacífico 508 - Nuevo Chimbote

1.2.3. Campus Universitario

Urbanización Bellamar s/n – Nuevo Chimbote

1.2.4. Registro Único del Contribuyente

Nº RUC: 20148309109

1.3. MISION

Brindar formación profesional humanística, científica y tecnológica a los estudiantes, con calidad y responsabilidad social y ambiental.

1.4. VISION

En el año 2019 la UNS es una institución licenciada, cuenta con sus Escuelas de Pregrado y Postgrado que participan en el desarrollo sostenible del país mediante la investigación + desarrollo e innovación, tecnología; sus egresados son profesionales líderes, competentes, creativos, proactivos inmersos en el mercado laboral nacional e internacional.

1.5. PRINCIPIOS

La Universidad Nacional del Santa se rige por los siguientes principios:

- Búsqueda, defensa y difusión de la verdad, afirmación de los valores, defensa de los derechos humanos y servicio a la comunidad.
- Calidad académica.
- Autonomía.
- Libertad de cátedra.
- Espíritu crítico y de investigación.
- Democracia institucional.
- Meritocracia.
- Pluralismo, tolerancia, diálogo intercultural e inclusión.
- Pertinencia y compromiso con el desarrollo sostenible del país.
- Afirmación de la vida y dignidad humana.
- Mejoramiento continúo de la calidad académica.
- Creatividad e innovación.
- Internacionalización.
- El interés superior del estudiante.

- Pertinencia de la enseñanza e investigación con la realidad social.
- Rechazo a toda forma de violencia, intolerancia y discriminación.
- Ética pública y profesional con transparencia en la gestión académica, administrativa y de gobierno.

1.6. OBJETIVOS

La Universidad Nacional del Santa tiene como objetivos los siguientes:

1.6.1. Lograr la excelencia académica en todas sus Facultades.

1.6.2. Asumir liderazgo en la promoción y difusión de la cultura a través de la proyección social, extensión universitaria e investigación.

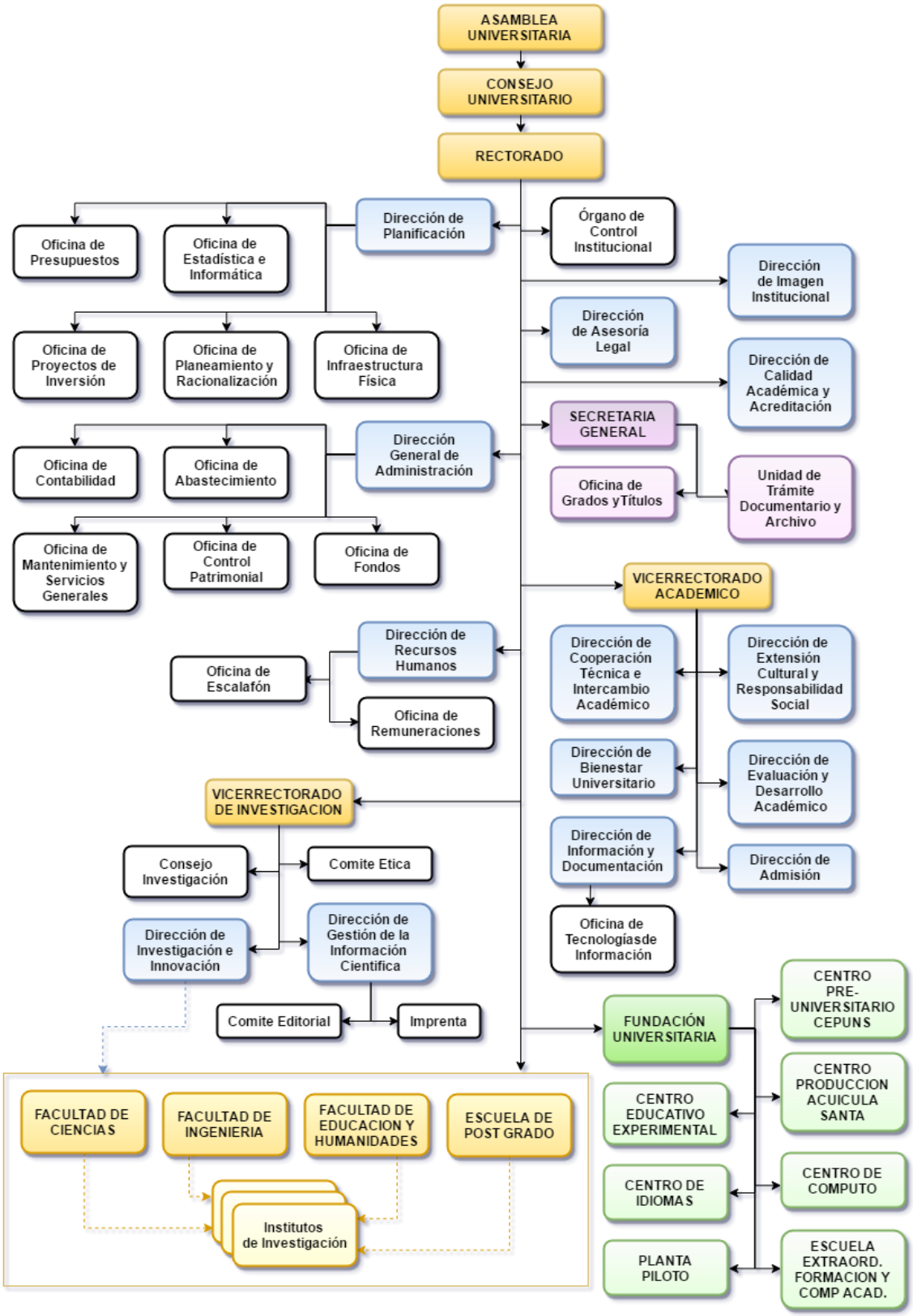
1.6.3. Impulsar el desarrollo de la región y el país a través de la investigación científica y tecnológica innovadora y la creación intelectual y artística.

1.6.4. Lograr una plana docente altamente calificada para el ejercicio de la docencia, la investigación y la proyección y extensión universitaria.

1.7. ORGANIZACIÓN

1.7.1. Organigrama

Figura N° 1: Organigrama de la UNS



CAPITULO II: PLAN DE INVESTIGACIÓN

2.1. EL PLANTEAMIENTO DEL PROBLEMA

2.1.1. Realidad Problemática

La Universidad Nacional del Santa (UNS) es una entidad que pertenece al sector público que brinda servicio educativo el cual tiene como funciones principales la enseñanza-aprendizaje, investigación y responsabilidad social. Como entidad educativa maneja información sobre sus postulantes y estudiantes de pregrado y posgrado a sus carreras profesionales respectivamente, docentes, colaboradores entre otros. La Dirección de Admisión (DADM) gestiona la información de los postulantes a las carreras profesionales de pregrado acorde con la Ley Universitaria-ley 30220 y los documentos normativos de la UNS como son: Estatuto aprobado con Resolución N°001-2017-AUT-R-UNS (05 de enero de 2017), el Reglamento General de la Universidad aprobado con Resolución N°305-2017-CU-R-UNS (25 de abril del 2017).

La DADM, almacena la información de los postulantes en medios informáticos como es la Base de Datos bajo responsabilidad de la Oficina de Tecnología de Información y Comunicaciones (OTIC) y en sus documentos (fichas de inscripción, formatos de control, hojas ópticas, etc.) para la Gestión del Proceso de Admisión, estos contienen información personal que identifican a los postulantes y debe ser protegida para evitar la fuga de información que pueda ser utilizada de manera maliciosa por alguna persona o institución externa. Como entidad pública la UNS se encuentra sujeto a las regulaciones establecidas por el estado en diferentes aspectos relacionados con las actividades que realiza, así tenemos la Ley de Protección de Datos Personales-Ley N°29733 (LPDP). Dicha norma establece directivas a seguir para la identificación de información personal y sensible, así como las consideraciones que las instituciones que utilizan este tipo de información deben tener en cuenta durante el manejo de la información. (Congreso de la República, 2017) (Personales, 2013)

Si bien se cuenta con una serie de normas estándar internacionales publicadas por la Organización Internacional de Normalización (ISO), para la gestión de

la seguridad de la información se hace uso del ISO/IEC 27001:2013.En el Perú se han definido leyes alineadas a éstos para que puedan ser aplicadas al contexto de las empresas y entidades existentes en el país en cuanto a la gestión de la seguridad de la información. Siendo así el estado peruano cuenta con la NTP ISO/IEC 27001:2014 la cuál es una adaptación del ISO/IEC 27001:2013 de la cual se ha determinado su uso obligatorio (Resolución Ministerial Nº 004-2016-PCM y su modificatoria Resolución Ministerial Nº 166-2017-PCM) con lo que se debe asegurar la implementación del Sistema de Gestión de Seguridad de la Información(SGSI) en su institución, priorizando en el alcance de los procesos misionales y aquellos que sean relevantes para su operatividad en las entidades públicas integrantes del Sistema Nacional de Informática. (ONGEI, El Peruano, 2017) (ONGEI, El Peruano, 2017)

Analizando el escenario actual, se puede apreciar que la UNS como parte de las instituciones públicas debe adaptarse a los nuevos cambios legislativos con las normas que regulan los temas de privacidad, mecanismos de control y seguimiento de seguridad de la información. Sin embargo la normativa aprobada da recomendaciones a seguir para la implementación de un SGSI, no indica exactamente la metodología o pasos a seguir para lograr este objetivo.

La necesidad de la UNS a través de la DADM de contar con un análisis que les permita realizar el diseño de un SGSI, en conjunto con los controles correspondientes al mismo como respuesta a la exigencia legal establecida por la LPDP previamente mencionada, además de la falta de un marco de referencia guía que acompañe el proceso a seguir para realizar dicho diseño a medida según los requerimientos específicos de una entidad educativa como la UNS, constituyen la problemática que este proyecto pretende resolver siguiendo las buenas prácticas, estándares internacionales y nacionales como la gestión por procesos bajo el estándar BPMN 2.0, los requisitos de la Norma ISO/IEC 27001:2013, la gestión del riesgo establecido por la Norma ISO/IEC 31000:2009 y los controles de la LPDP los cuales permitirán realizar una identificación de la información crítica con la que trabaja la DADM y en

consecuencia definir los riesgos a los que se encuentra expuesta y los controles que deberían implementarse para garantizar su seguridad y privacidad.

2.1.2. Formulación del Problema

¿De qué manera la elaboración de un marco de referencia permitirá la implementación de la norma ISO/IEC 27001:2013 y Ley de Protección de Datos Personales en la Dirección de Admisión de la Universidad Nacional del Santa?

2.2. ANTECEDENTES DEL PROBLEMA

2.2.1. Antecedentes Locales

El estudio de Ramos (2014) sobre el Desarrollo de un Sistema de Gestión para mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina, desarrollado para la Universidad Nacional del Santa, Nuevo Chimbote, Perú. Es una investigación del tipo aplicada y nivel descriptiva, que empleo una muestra no probabilística intencional empleando instrumentos fichas, fotografías, cuaderno de notas, cuestionarios, encuestas asimismo utilizo el ciclo PDCA para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001 e ISO/IEC 17799, llego a la conclusión que se mejoró la seguridad de la información Institución Servicios Industriales de la Marina a través de la implementación de los procesos del SGSI. Finalmente está investigación aporta información de los procesos que deben realizarse para el desarrollo de la Norma ISO/IEC 27001 que es tema a tratar en la investigación en curso.

2.2.2. Antecedentes Nacionales

El estudio de Alcántara Flores (2015)sobre la Guía de Implementación de la Seguridad basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del norte P.N.P en la ciudad de Chiclayo, desarrollado en la Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú. Es una investigación Tecnológica Aplicada Cuasi-Experimental, que empleo una muestra no probabilística intencional o por conveniencia empleando instrumentos tales como Ficha de Observación, Cuestionario de preguntas, Guía

de entrevistas, Guía de reportes. Para la implementación de la Norma ISO/IEC 27001 hizo uso de seis(6) fases que a continuación se detallan: definir una Política de seguridad de Información, definir el alcance del Modelo, efectuar un Análisis y Evaluación del Riesgo, definir Opciones del Tratamiento del Riesgo, seleccionar controles a implantar y preparar un enunciado de aplicabilidad. El autor entre sus conclusiones menciona que con el uso de la Guía de Implementación se logró mejorar el proceso para detectar las anomalías en la seguridad de la información reflejada en distintos mecanismos de seguridad para salvaguardarla y prevenir su mal uso y divulgación no adecuada que perjudiquen a la institución. Finalmente está investigación aporta información de los fases que deben realizarse y sus entregables resultantes para la implementación de la Norma ISO/IEC 27001 el cuál es tema a tratar en la investigación en curso.

2.2.3. Antecedentes Internacionales

El estudio de Contreras Esguerra (2017) sobre el Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la Dirección de Sistemas de la Gobernación de Boyacá desarrollado en la Universidad Nacional Abierta y a Distancia, Bogotá, Colombia. Es una investigación descriptiva del tipo analítica, que empleo una muestra no probabilística intencional empleando instrumentos tales como encuestas, fichas de Observación y la ejecución de pruebas. Para la implementación de la Norma ISO/IEC 27001 utilizo el ciclo PDCA para el desarrollo de un SGSI basado en la Norma ISO/IEC 27001 y para la gestión del Riesgo hizo uso de la metodología de libre uso del Consejo Superior de Administración Electrónica del Gobierno Español denominada Magerit (PÚBLICAS, 2012), llegando a la conclusión que el Diseño del SGSI en la Dirección de Sistemas de la Gobernación de Boyacá, puede ayudar al mejoramiento de actualización de diferentes procesos que esta lleva, a corto y mediano plazo, logrando fortalecer la continuidad de la Entidad, y mitigar riesgos a los que puede estar expuesta alguna información.

Finalmente está investigación aporta información de los procesos de la gestión del riesgo que es base para implementar un SGSI bajo la Norma ISO/IEC

27001:2013, siendo este tema de gran importancia a tratar en la investigación en curso.

2.3. JUSTIFICACIÓN

2.3.1. Económica

Permitirá la adecuación a nivel procesos, jurídico y tecnológico de la DADM para dar cumplimiento a lo establecido por la LPDP evitando multas y sanciones. Asimismo permitirá a la DADM gestionar y asegurar la confidencialidad, disponibilidad e integridad de los activos e información que hacen uso previniendo pérdidas y daños a la imagen de la institución.

2.3.2. Social

Permitirá mejorar la gestión de los procesos y de los riesgos en la DADM, lo cual es reflejado en la mejora de la calidad del servicio al contar con información debidamente salvaguardada y con controles adecuados para la privacidad de la misma lo cual permitirá a la Universidad dar cumplimiento a las regulaciones del estado peruano respecto a la protección de datos personales.

2.3.3. Técnica

Permitirá a través de la gestión del riesgo establecido por la ISO/IEC 31000 componente base de la ISO/IEC 27001:2013, determinar que controles tecnológicos deberá implementar la DADM para asegurar el tratamiento y la privacidad de la información asimismo de las instalaciones donde se procesan.

2.3.4. Operativa

Ayudará a mejorar la gestión de los procesos en la DADM puesto que al contar con procedimientos ordenados y documentados, se podrá determinar las medidas necesarias para un adecuado tratamiento de la información asimismo identificar los mecanismo para salvaguardarla evitando pérdidas, invasión de la privacidad de la misma. Permitiendo asegurar la confidencialidad, la disponibilidad e integridad de los procesos (activos e instalaciones) de la Universidad en un marco de cumplimiento de la Norma ISO/IEC 27001:2013 y la LPDP.

2.4. IMPORTANCIA DE LA INVESTIGACION

El presente informe de investigación tiene como finalidad establecer un marco de trabajo para la gestión de los procesos, tratamiento de la información y gestión de la tecnología utilizada en la DADM de la Universidad Nacional del Santa a fin de dar cumplimiento de los controles de seguridad de la información establecidos por la Norma ISO/IEC 27001:2013 y la Ley de Protección de Datos Personales.

2.5. OBJETIVOS

2.5.1. Objetivo General

Establecer un marco de referencia a nivel de procesos, tecnología y legales para la implementación de la Norma ISO/IEC 27001:2013 y Ley de Protección de Datos Personales en la Dirección de Admisión de la Universidad Nacional del Santa.

2.5.2. Objetivos Específicos

2.5.2.1. Identificar, elaborar y documentar los procesos principales de la Dirección de Admisión acorde con su reglamentación existente y la normativa del estado peruano respecto a la gestión por procesos (PCM, 2013) y las buenas prácticas basado en el estándar BPMN 2.0.

2.5.2.2. Elaborar un procedimiento documentado enmarcado en las buenas prácticas basadas en el estándar BPMN 2.0 para clasificar los Bancos de Datos Personales de la Dirección de Admisión acorde con la Ley de Protección de Datos Personales, su reglamento y su directiva de seguridad.

2.5.2.3. Elaborar un Análisis de Brechas (GAP) basado en el modelo de madurez CMMI (Network Security Advisors, s.f.) (Amendola, 2017), para revisar la situación actual de la Universidad respecto al cumplimiento de la seguridad de la información bajo la Norma ISO/IEC 27001:2013, Norma ISO/IEC 27002:2013 y la Ley de Protección de Datos Personales.

2.5.2.4. Elaborar una metodología de gestión de riesgos de seguridad de la información basado en la Norma ISO/IEC 31000:2009 de Gestión del Riesgo, la Norma ISO/IEC 27005:2011 de Gestión de Riesgos de Seguridad de la Información enmarcado en la Ley de Protección de Datos Personales, su reglamento y su directiva de seguridad.

2.5.2.5. Elaborar modelos de documentos de Aviso de privacidad, Procedimientos y formatos del ejercicio de los derechos ARCO (Justicia, Ministerio de Justicia)de la Ley de Protección de Datos Personales.

2.6. METODOLOGÍA

La Metodología que se utilizó para el desarrollo de la presente Tesis es un marco de trabajo propuesto basado en la Metodología BPMN 2.0, Modelo de Evaluación de la Madurez (CMMI), los requisitos de las Normas ISO/IEC 27001:2013, los controles de la Norma ISO/IEC 27002:2013 y los lineamientos propuestos por la Ley de Protección de Datos Personales, su Reglamento y su Directiva de Seguridad. Asimismo se contará con la evaluación continua del Director de Admisión como parte interesada principal del presente trabajo. Finalmente se contara con juicio de expertos de profesionales especializados y certificados en seguridad de la información para validar la propuesta del Marco de Referencia.

CAPITULO III: MARCO REFERENCIAL

3.1. MARCO TEORICO

3.1.1. MARCO DE REFERENCIA

Según (Bernal, pág. 125) define como marco de referencia: "Toda investigación debe realizarse dentro de un marco de referencia o conocimiento previo, es decir, es necesario ubicar la investigación que va a realizarse dentro de una teoría, un enfoque o una escuela. También se debe explicar la concepción de persona que enmarcará la investigación y, finalmente, se deben precisar los conceptos relevantes del estudio."

En consecuencia con lo descrito se plantea la elaboración de un marco guía basado en procesos acorde con las buenas prácticas de BPMN 2.0, los requisitos de la Norma ISO/IEC 27001:2013 para gestionar la seguridad de la información, los requisitos de la Norma ISO/IEC 31000:2009 y la Norma ISO/IEC 27005:2011 para gestionar riesgos de seguridad de la información, y los controles establecidos de privacidad por la Ley de Protección de Datos Personales en el marco de su cumplimiento. La abstracción de las normas y buenas prácticas mencionadas permitirá contar con procedimientos para la implementación de la Norma ISO/IEC 27001:2013 y Ley de Protección de Datos Personales en la Dirección de Admisión.

3.1.2. DEFINICIONES ESPECÍFICAS PARA EL SGSI SEGÚN LA NORMA ISO/IEC 27001:2013

Todas las definiciones mostradas a continuación provienen de la ISO/IEC 27000:2014 (STANDARDIZATION, ISO/IEC 27000:2014 Tecnología de Información - Técnicas de Seguridad -Sistemas de Gestión de Seguridad de Información - Descripción y vocabulario., 2014), marco referencial para comprender los términos en los estándares de la familia 27000.

Sistema de Gestión de Seguridad de Información:

Un Sistema de Gestión de Seguridad de la Información (SGSI) consiste en políticas, procedimientos, directrices, recursos asociados y actividades,

gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información.

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en la evaluación del riesgo y los niveles de aceptación del riesgo de la organización, diseñada para tratar y gestionar los riesgos de manera efectiva.

Analizar requisitos para la protección de los activos de información aplicar los controles adecuados para garantizar su protección, según sea necesario, contribuye a la implementación exitosa de un SGSI. (ISO/IEC 27000: 2014 - 3.2.1)

Información: La información es un activo que, al igual que otros activos de negocio importantes, es esencial para la misión de una organización y por lo tanto necesita ser protegida de forma adecuada. La información puede ser almacenada en muchas formas, incluyendo: forma digital (por ejemplo: archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo: en el papel), así como la información no estructurada en la forma de conocimiento de los empleados. La información puede ser transmitida por diversos medios, incluyendo: mensajería, comunicación electrónica o verbal. Cualquiera que sea la forma que adopte la información o el medio por el cual sea transmitida, siempre se necesita una protección adecuada.

En muchas organizaciones la información depende de la tecnología de la información y las comunicaciones. Esta tecnología es usualmente un elemento esencial en la organización y permite facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información. (ISO/IEC 27000: 2014 - 3.2.2)

Seguridad de información: La seguridad de información incluye tres dimensiones principales: la confidencialidad, disponibilidad e integridad. Consiste en la aplicación y gestión de medidas de seguridad apropiadas, lo que implica la consideración de una amplia gama de amenazas, con el fin de garantizar

el éxito y continuidad del negocio, de manera sostenida, y la minimización de los impactos de los incidentes de seguridad de la información.
Esto se logra mediante la implementación de un conjunto aplicable de controles, seleccionados a través del proceso de gestión de riesgos y administrados utilizando un SGSI; incluye las políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles deben ser especificados, implementados, monitoreados, revisados y mejorados cuando necesario, para asegurar que se cumplen los objetivos específicos de seguridad de información y del negocio son logrados. Se espera que los controles de seguridad de la información relevantes se integren a la perfección con los procesos de negocio de la organización. (ISO/IEC 27000: 2014 - 3.2.3)

Sistema de gestión: Un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos. (ISO/IEC 27000: 2014 - 3.2.5)

Confidencialidad: Propiedad de la limitación o restricción de la información a individuos, entidades o procesos no autorizados. (ISO/IEC 27000: 2014 - 2.61)

Integridad: Propiedad de [la información de] exactitud y completitud. (ISO/IEC 27000: 2014 - 2.40)

Disponibilidad: Propiedad de [la información de] ser accesible o usable cuando sea demandada por una entidad autorizada. (ISO/IEC 27000: 2014 - 2.9)

Riesgo: Efecto que genera incertidumbre sobre [el logro de] los objetivos [de seguridad de información]. (ISO/IEC 27000: 2014 - 2.68)

Control: Medida que modifica la situación del riesgo. (ISO/IEC 27000: 2014 - 2.68)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000: 2014 - 2.83)

Amenaza: Causa potencial de un incidente inesperado, que podría resultar e daño a un sistema o a la organización. (ISO/IEC 27000: 2014 - 2.83)

Consecuencia: Resultado de un evento, que afecta a los objetivos. Un evento puede llevar a un rango de consecuencias. Una consecuencia puede ser certera o incierta y en el contexto de la seguridad de información es usualmente negativa. Las consecuencias pueden ser expresadas de modo cualitativo o cuantitativo. Las consecuencias iniciales pueden escalar a través de efectos derivados. (ISO/IEC 27000: 2014 - 2.14)

Propietario del Riesgo: Persona o entidad con la capacidad y autoridad para gestionar un riesgo. (ISO/IEC 27000: 2014 - 2.68)

Requisito: Necesidad o expectativa que está establecida, generalmente implícita u obligatoria. "Generalmente implícita" significa que es costumbre o práctica común para la organización y partes interesadas cuya necesidad o expectativa bajo consideración es implícita. Un requerimiento especificado es aquel que está establecido, por ejemplo, en información documentada. (ISO/IEC 27000: 2014 - 2.63)

3.1.3. ESTANDARES INVOLUCRADOS

3.1.3.1. ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos

(STANDARDIZATION, SO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad., 2013)**.**

Es la última versión del estándar que establece los requisitos para los sistemas de gestión de seguridad de información. Define los requerimientos necesarios para el adecuado establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Es un estándar certificable.

3.1.3.2. ISO/IEC 27000:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Descripción y vocabulario

Sistemas de Gestión de Seguridad de Información. Descripción y vocabulario (STANDARDIZATION, ISO/IEC 27000:2014 Tecnología de Información - Técnicas de Seguridad -Sistemas de Gestión de Seguridad de Información - Descripción y vocabulario., 2014**).**

Contiene el glosario de términos y definiciones para la familia 27000. El contenido de este documento debe ser tomado en cuenta para el adecuado enfoque y entendimiento de las cláusulas y requisitos que exponen los estándares 27001,27002, 27005, entre otros.

3.1.3.3. ISO/IEC 27003:2010 Tecnología de Información. Técnicas de Seguridad. Directrices para la implementación de un sistema de gestión de seguridad de información

Directrices para la implementación de un sistema de gestión de seguridad de información (STANDARDIZATION, ISO/IEC 27003:2010 Tecnología de Información. Técnicas de Seguridad.Directrices para la implementación de un sistema de gestión de seguridad de información, 2010)

Propone una guía de implementación para un SGSI, para lo cual indica etapas, documentos y roles que pueden permitir la adecuada atención de los requisitos establecidos en la ISO/IEC 27001: 2013. Sin embargo, los lineamientos indicados en este documento no son de cumplimiento obligatorio, ya que es una propuesta de implementación que no pretende reemplazar a los requisitos que establece la ISO/IEC 27001: 2013. Este estándar fue publicado el 2010, antes de la última versión de la ISO/IEC 27001:2013, por lo que su desarrollo no está diseñado para atender todos los requisitos de este último.

3.1.3.4. ISO/IEC 27005:2011 Tecnología de Información. Técnicas de Seguridad. Gestión del Riesgo en Seguridad de Información

Gestión del Riesgo en Seguridad de Información (STANDARDIZATION, ISO/IEC 27005:2011 Tecnología de Información. Técnicas de Seguridad.Gestión del Riesgo en Seguridad de Información., 2011)

Este estándar propone un marco para la gestión de riesgos de seguridad de la información, bajo un enfoque en cuatro etapas: inventario, análisis,

evaluación y tratamiento de los riesgos de seguridad de información. Si bien constituye un esquema válido para la gestión de riesgos en seguridad de información, está más enfocado en la versión precedente del estándar 27001 (2005).

3.1.3.5. ISO 31000:2009 Gestión del Riesgo. Principios y Directrices

(STANDARDIZATION, ISO 31000:2009 Gestión del Riesgo. Principios y Directrices., 2009)

Propone un marco para la gestión de riesgos y oportunidades, a partir de una evaluación del contexto de la organización. Este enfoque es referenciado por la ISO/IEC 27001:2013, como fuente para establecer el contexto de la organización, además de identificar, evaluar y tratar los riesgos y oportunidades de seguridad de información.

3.1.3.6. IEC 31010:2009 Gestión de Riesgo. Técnicas de Apreciación del Riesgo

(STANDARDIZATION, IEC 31010:2009 Gestión de Riesgo. Técnicas de Apreciación del Riesgo., 2009)

Propone técnicas y estrategias para la identificación y evaluación de riesgos y oportunidades de seguridad de información de la organización, complementando las directrices establecidas en la ISO 31000:2009. Entre las estrategias propuestas se mencionan la técnica Delphi, la aplicación de Listas de Verificación, Análisis de Riesgos Preliminar (PHA), HAZOP, Análisis de peligros y puntos críticos de control(HACCP), Evaluación de Toxicidad, Técnica Estructurada "WHAT-IF" (SWIFT),Análisis de Escenarios, Análisis de Impacto en el Negocio (BIA), entre otros.

3.1.4. LEY DE PROTECCIÓN DE DATOS PERSONALES

La Ley N° 29733 de Protección de datos personales publicada en julio del 2011 y siendo aprobada su aplicación en marzo del 2013, regule la manera en la que se hace uso de la información personal en los procesos de todas las organizaciones que realicen operaciones en Perú.

Según detalla la ley, se considera dato personal a cualquier dato que pueda ser utilizado para identificar a una persona natural, de esta forma se puede

considerar como datos personales el nombre de una persona, su dirección, su sexo, etc. Profundizando más en este concepto, se define además como dato sensible a aquellos que comprendan los datos biométricos, origen racial, religión, etc.

Si bien es cierto que dichos datos casi siempre son necesarios para poder acceder a algún servicio ya sea financiero, educativo o de salud la ley detalla que el titular de dichos datos tiene los siguientes derechos respecto de esta información:

- Solicitar información sobre el uso que se dará a la información que facilite.
- Solicitar acceso a la información que la organización posee sobre él.
- Solicitar la actualización, rectificación, adición o supresión de datos.
- Solicitar que su información personal no sea suministrada a terceros.

Como objetivo respecto al reglamento que establece esta ley, se menciona a los dueños y encargados de los bancos de datos personales, tanto de la administración pública como privada los cuales deberán modificar sus procedimientos para poder cumplir los requerimientos de esta norma.

Se señala además que aquellos bancos de datos que sean de uso privado, así como los que se utilicen para las operaciones de la administración pública incluidas las que soportan los procedimientos de defensa nacional, seguridad pública e investigación penal se encuentras exceptuadas de la aplicación de la norma.

El principal objetivo de la norma es que las personas naturales puedan tener conocimiento de quién tiene acceso a su información personal, además de conocer el tipo de uso que se le dará. De esta forma establece como garantía principal que el uso de datos personales debe estar sujeto al conocimiento previo, informado, expreso e inequívoco por parte del titular de dicha información. Sin embargo dicha garantía puede quedar invalidada en el caso que el ejercicio de éste derecho afecte, por ejemplo, intereses de terceros o investigaciones judiciales.

Dado su carácter de ley, todas las instituciones públicas o privadas que se encuentren en operación, deben garantizar el cumplimiento del reglamento especificado por la misma. (Congreso de la República, 2017) (Personales, 2013)

3.1.4.1. Directiva de Seguridad (Ley de Protección de Datos Personales 29733) (Autoridad Nacional de la , 2013)

Marco de recomendaciones en seguridad de información, relacionadas al adecuado tratamiento y custodia de la información de carácter personal. Documento emitido por la Autoridad Nacional de Datos Personales como marco complementario para la implementación de la Ley. En base a la categoría de los bancos de datos personales administrados por las organizaciones, esta directiva define niveles de requisitos a manejarse. A mayor volumen y complejidad de los datos, mayor el nivel de exigencia. En el nivel más alto se recomienda implementar un SGSI.

3.1.5. BUSINESS PROCESS MODEL AND NOTATION (BPMN)

(HITPASS, 2007)

Business Process Model and Notation (BPMN), en español Modelo y Notación de Procesos de Negocio, es una notación gráfica estandarizada que permite el modelado de procesos de negocio, en un formato de flujo de trabajo (workflow). BPMN fue inicialmente desarrollada por la organización Business Process Management Initiative (BPMI), y es actualmente mantenida por el Object Management Group (OMG), después de la fusión de las dos organizaciones en el año 2005.

El modelado de procesos es una tarea crítica y obligatoria para cualquier proyecto que pretenda establecer un SGSI bajo el ISO/IEC 27001:2013, en alguna organización, puesto que es necesario conocer cómo se desarrollan los distintos procesos de negocio, así como el flujo de información a través de los mismos. Esta metodología incluye diferentes herramientas tanto de documentación, como tecnológicas especializadas en el análisis de procesos de

negocio con la finalidad de detectar oportunidades de mejora que permitan optimizarlos.

A fin de obtener los procesos de la DADM, se utilizará las herramientas ofrecidas por esta metodología para la determinación del flujo de datos, actores y procedimientos que componen la Gestión de Admisión. El modelamiento de procesos se apoyará en la herramienta Bizagi, la cual permitirá presentar de manera gráfica el flujo de tareas que conforman los procesos de la Gestión de Admisión, así como la documentación que incluya los datos y conocimientos obtenidos en el levantamiento de información.

3.1.6. OTROS REFERENTES

NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos (INDECOPI, 2014)

Norma técnica peruana de requisitos para implementar un SGSI. Es una traducción del estándar ISO/IEC 27001:2013, razón por la cual cambia mucho respecto a la versión precedente (2008), actualmente se encuentra vigente se debe precisar su cumplimiento obligatorio para las entidades del estado peruano *mediante Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática y su modificatoria Resolución Ministerial Nº 166-2017-PCM que modifica el artículo 5 de la Resolución Ministerial Nº 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información*.

CAPITULO IV: MATERIALES Y METODOS

4.1. Hipótesis

Elaboración de un Marco de Referencia para la Implementación de la Norma ISO/IEC 27001:2013 y Ley de Protección de Datos Personales en la Dirección de Admisión de la Universidad Nacional del Santa.

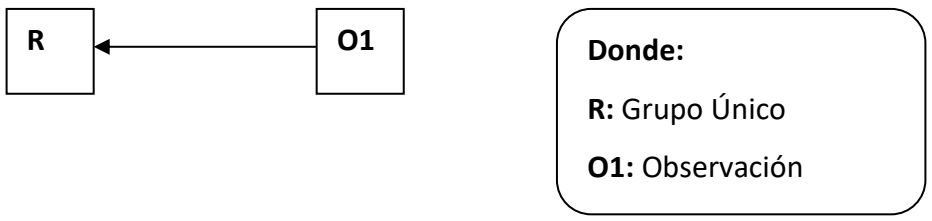
4.2. Método de Investigación

Descriptiva – transeccional, según (Hernández Sampieri, Baptista Lucio, & Fernández Collado, 2014) "El procedimiento consiste en ubicar en una o diversas variable a un grupo de personas u otros seres vivos, objetos, situaciones, contextos, fenómenos, comunidades, etc., y proporcionar su descripción. Son por tanto, estudios puramente descriptivos y cuando establecen hipótesis, éstas son también descriptivas".

4.3. Diseño de Investigación

El diseño es No experimental por ser una investigación puramente Descriptiva, con un único grupo y la observación respectiva (Ávila Baray, 2006).

Figura N° 2: Diseño no Experimental según el paradigma Ex Post Facto



Fuente: Elaboración Propia

La validez de la presente investigación se ejecutó a través de juicios expertos por profesionales en seguridad de la información, utilizando el método Delphi (Reguant Álvarez & Torrado Fonseca , 2016) (Varela Ruiz, Díaz Bravo, & García Durán, 2012), haciendo uso de la herramienta open source de Google denominada google forms para elaborar y analizar encuestas vía web (Google, 2017).

4.4. Población

El recurso humano de la DADM conformada por el Director, Coordinadores y colaboradores administrativos de la DADM de la Universidad Nacional del Santa.

4.5. Tipo de Muestreo

Para el informe de investigación se realizó un muestreo por selección intencionada o muestreo de conveniencia.

4.6. Muestra

Se utilizó un muestreo no probabilístico dirigido del recurso humano de la DADM, de tres (03) personas conformadas por el Director de Admisión, Coordinador Administrativo y Coordinador Académico.

4.7. Técnicas e instrumentos

Para la recolección de datos se usará:

- Entrevistas, llamadas telefónicas.
- Encuestas Online.

Instrumentos

Para la recolección de datos se usará:

- Formatos de encuestas.

CAPITULO V: RESULTADOS

5.1 Fase I- Análisis, Diseño y Documentación del Proceso de Admisión de Pregrado

5.1.1 Objetivos de la Fase I

- Revisar la documentación normativa de la Universidad (Estatuto, Reglamento General, Plan Estratégico, Plan Operativo, MOF) y de la Dirección de Admisión (Reglamento de Admisión).
- Definir los formatos y criterios para el inventario de los procesos y subprocesos de la Dirección de Admisión.
- Realizar el inventario de procesos de la Dirección de Admisión.

5.1.2 Marco de Trabajo de la Fase I

Para la descripción formal del modelo de Procesos se ha tomado como referencia la notación BPMN 2.0 y el documento de modernización de Procesos de la Presidencia de Consejo de Ministros (PCM, 2013, págs. 29-32).

5.1.3 Desarrollo de la Fase I

El instructivo utilizado a continuación fue el siguiente:

Tabla N° 1: Cuestionario de referencia para la recolección de la información.

Mapeo de Procesos: Entrevista para la recolección de información	
1	¿Cuál es la misión u objetivo general del proceso en el cual participa?
2	¿Cuál es el alcance del proceso? (es decir, ¿cuáles son los límites del proceso? ¿con qué actividad se inicia y con qué actividad termina?
3	¿El proceso se relaciona con otro proceso de la entidad?
4	¿Qué productos genera el proceso?
5	¿Quiénes reciben estos productos? (es decir, ¿Quiénes son los Clientes internos/externos?
6	¿Qué necesidades o expectativas tienen los clientes internos/externos con respecto a cada producto generado por el proceso?
7	¿Puede identificar las partes interesadas o stakeholders del proceso?
8	¿Cuáles son las expectativas o necesidades de las partes interesadas?
9	¿Cuentan con indicadores que midan el proceso que realiza?
10	¿Tiene alguno de sus procesos documentado?

Los Formatos propuestos para el Inventario de Procesos y Procedimientos es el siguiente en los cuales se especifica la información que se deberá registrar a partir de las entrevistas y revisión de documentación.

Tabla N° 2: Formato para Inventario de Procesos

	FICHA DE PROCESO DE NIVEL 0,1,2			**Código:** Código del Proceso	
				Versión: Número de versión	
I. DATOS GENERALES DEL PROCESO					
1. NOMBRE DEL PROCESO	Colocar nombre del proceso	**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Colocar el nombre del proceso del nivel superior	
2. OBJETIVO DEL PROCESO	¿Para qué se realiza el proceso?				
4. DUEÑO DEL PROCESO	¿Quién tiene la responsabilidad del desarrollo del proceso y garantiza la entrega del producto?	**5. LÍMITES DEL PROCESO**	**INICIO**	¿Con qué actividad se inicia el proceso?	
			FIN	¿Con qué actividad se termina el proceso?	
II. DESCRIPCIÓN DEL PROCESO					
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**	**9. CONTROLES APLICADOS**	**10. PRODUCTOS**	**11. CLIENTES**
¿De quién se reciben las entradas?	¿Qué origina el proceso?	Nombres de los procesos de nivel inferior	Actividades de control	¿Qué entrega?	¿A quién entrega?
III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO					
12. TIPO	**13. DESCRIPCIÓN**				
Infraestructura, personal o materiales	Características y cantidades de los recursos				
IV. DOCUMENTACIÓN DEL PROCESO					
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**				
Documentos generados en el proceso	Dispositivos normativos que se utilizan en el proceso				
V. INDICADORES					
16. NOMBRE DEL INDICADOR	**17. RESPONSABLE**	**18. TIPO DE INDICADOR**	**19. FÓRMULA**	**20. PERIODICIDAD DE MEDICIÓN**	
Colocar nombre del indicador	¿Quién lo mide?	Eficiencia, eficacia, calidad	¿Cómo se calcula el indicador?	Mensual, trimestral, semestral, anual, etc.	
ETAPA	**RESPONSABLE**		**FECHA**	**FIRMA Y SELLO**	
Formulado por:					
Cargo					
Revisado por:					
Cargo					
Revisado por:					
Cargo					
Aprobado por:					
Cargo					

Tabla N° 3: Formato para Inventario de Procedimientos

	FICHA DE PROCEDIMIENTO		**Código**: Código del procedimiento **Versión**: Número de versión
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	Nombre del proceso de nivel superior al que pertenece el procedimiento.
TÍTULO:	Nombre del procedimiento		
A. OBJETIVO:	Señalar ¿Qué se espera del documento?		
B. UNIDAD RESPONSABLE:	Órgano o unidad orgánica a cargo del procedimiento, inicio al fin		
C. BASE LEGAL:	Dispositivos legales que sustentan el objetivo del documento		
D. REQUISITOS DEL PROCEDIMIENTO:	Listado de documentos internos asociados al documento o en su caso versiones anteriores u otros requisitos para dar inicio al procedimiento.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**REGISTROS**
1	Descripción de las actividades del proceso	Señalar las horas expresados en minutos	Nombre del órgano o unidad orgánica	¿Quién realiza la actividad?	Registros que se generan en el proceso
2					
3					
4					
5					
6					
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:		Suma de duraciones			

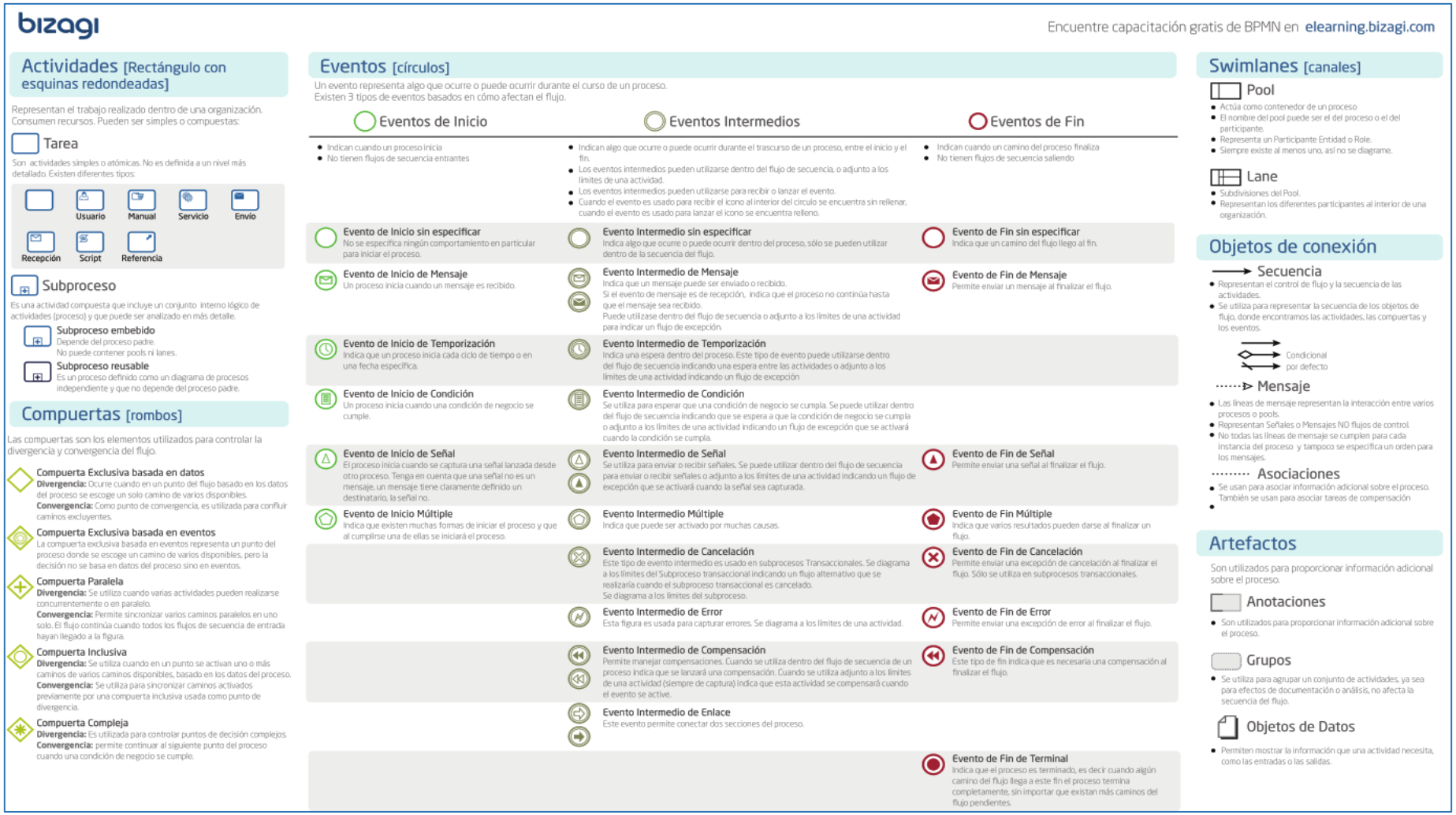
F. DIAGRAMA DE FLUJO:
Descripción gráfica del desarrollo identificando un paso a paso de acciones y responsables para la realización de la tarea o función

H. HOJA DE CONTROL DE CAMBIOS:	Colocar las versiones del documento
I. ANEXOS:	Instrumentos de ayuda y consulta

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:			
Cargo			
Revisado por:			
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

A continuación las notaciones utilizadas del estándar BPMN 2.0 por la herramienta Bizagi en la siguiente figura:

Figura N° 3: Notación BPMN 2.0 de la Herramienta Bizagi



Inventario de Procesos

En la siguiente figura se muestra el inventario de procesos y sus respectivos Niveles:

Tabla N° 4: Inventario de Procesos

INVENTARIO DE PROCESOS				
Tipo	**Nivel**	**Etapa**	**Código**	**Nombre del Proceso**
MACROPROCESO	0		**PM01**	Gestión de Admisión
PROCESO	1		**PM01.01**	Proceso de Admisión de Programas de Pregrado
PROCESO	1		**PM01.02**	Proceso de Admisión de Programas de Posgrado
SUBPROCESO	2	**Organización y Planificación**	**PM01.01.01**	Planificación del Proceso de Admisión de Pregrado
PROCEDIMIENTO	3		**PM01.01.01.01**	Elaboración y Aprobación del Plan de Trabajo y Presupuesto
PROCEDIMIENTO	3		**PM01.01.01.02**	Selección y captación del Recurso Humano de Apoyo
PROCEDIMIENTO	3		**PM01.01.01.03**	Elaboración y aprobación del Reglamento de Admisión
PROCEDIMIENTO	3		**PM01.01.01.04**	Elaboración del Prospecto de Admisión
SUBPROCESO	2	**Fomento**	**PM01.01.02**	Difusión del Proceso de Admisión de Pregrado
PROCEDIMIENTO	3		**PM01.01.02.01**	Convocatoria y reunión con Directores de Escuela
PROCEDIMIENTO	3		**PM01.01.02.02**	Elaboración y realización de publicidad
PROCEDIMIENTO	3		**PM01.01.02.03**	Publicación de cronograma del proceso de admisión
PROCEDIMIENTO	3		**PM01.01.02.04**	Realización de visitas locales y regionales
PROCEDIMIENTO	3		**PM01.01.02.05**	Elaboración y Presentación de Informe de Difusión
SUBPROCESO	2	**Ejecución**	**PM01.01.03**	Inscripción al Proceso de Admisión de Pregrado
PROCEDIMIENTO	3		**PM01.01.03.01**	Inscripción a las modalidades de Admisión para Pregrado
PROCEDIMIENTO	3		**PM01.01.03.02**	Presentación y validación de requisitos de inscripción
PROCEDIMIENTO	3		**PM01.01.03.03**	Control de las inscripciones
SUBPROCESO	2		**PM01.01.04**	Gestión de Exámenes del Proceso de Admisión de Pregrado
PROCEDIMIENTO	3		**PM01.01.04.01**	Elaboración y actualización de ítems del banco de preguntas

PROCEDIMIENTO	3			**PM01.01.04.02**	Selección de integrantes para las Subcomisiones del Proceso de Admisión
PROCEDIMIENTO	3			**PM01.01.04.03**	Elaboración de los Exámenes del Proceso de Admisión
PROCEDIMIENTO	3			**PM01.01.04.04**	Aplicación de los Exámenes del Proceso de Admisión
PROCEDIMIENTO	3			**PM01.01.04.05**	Aprobación y Publicación de resultados del Proceso de Admisión
SUBPROCESO	2			**PM01.01.05**	Acreditación de ingresantes a las Carreras Profesionales de Pregrado
PROCEDIMIENTO	3			**PM01.01.05.01**	Elaboración y visado de constancias de ingresantes
PROCEDIMIENTO	3			**PM01.01.05.02**	Presentación y validación de requisitos de ingresantes
PROCEDIMIENTO	3			**PM01.01.05.03**	Entrega de constancias de ingreso
SUBPROCESO	2		**Seguimiento**	**PM01.01.06**	Verificación del Proceso de Admisión de Pregrado
PROCEDIMIENTO	3			**PM01.01.06.01**	Presentación de Informe de Ejecución del Proceso de Admisión de Pregrado
PROCEDIMIENTO	3			**PM01.01.06.02**	Devolución de documentos de Postulantes No Ingresantes
PROCEDIMIENTO	3			**PM01.01.06.03**	Remisión de expedientes de Ingresantes Acreditados
Leyenda	**PM:** Proceso Misional				

Tabla N° 5: PM01 - Ficha de Proceso

<table>
<tr><td colspan="2"></td><td colspan="3">FICHA DE MACROPROCESO O PROCESO DE NIVEL 0</td><td colspan="2">Código: PM01
Versión: 1.0</td></tr>
<tr><td colspan="7">I. DATOS GENERALES DEL PROCESO</td></tr>
<tr><td colspan="2">1. NOMBRE DEL PROCESO</td><td colspan="5">Gestión de Admisión</td></tr>
<tr><td colspan="2">2. OBJETIVO DEL PROCESO</td><td colspan="5">Implementar procesos de evaluación para asegurar que los postulantes cumplan con el perfil de ingreso de cada programa de pregrado y postgrado.</td></tr>
<tr><td colspan="2" rowspan="2">3. DUEÑO DEL PROCESO</td><td rowspan="2">Director de Admisión</td><td rowspan="2">4. LÍMITES DEL PROCESO</td><td>INICIO</td><td colspan="2">Inicia con la adecuación de la Ley Universitaria a los procesos de admisión de pregrado y posgrado.</td></tr>
<tr><td>FIN</td><td colspan="2">Culmina con el Informe de Ejecución del Proceso de Admisión de Programas de Pregrado y del Proceso de Admisión de Programas de Posgrado.</td></tr>
<tr><td colspan="7">II. DESCRIPCIÓN DEL PROCESO</td></tr>
<tr><td>5. PROVEEDORES</td><td>6. INSUMOS</td><td>7. PROCESOS DE NIVEL INFERIOR</td><td>8. CONTROLES APLICADOS</td><td>9. PRODUCTOS</td><td colspan="2">10. CLIENTES</td></tr>
<tr><td>Dirección de Admisión

Consejo Universitario</td><td>Plan de Trabajo de Admisión para Programas de Pregrado</td><td rowspan="5">PM01.01.Proceso de Admisión de Programas de Pregrado</td><td>Revisión del Plan Operativo de la Dirección de Admisión

Aprobación de Plan de Trabajo de Admisión para Programas de Pregrado</td><td>Plan de Trabajo de Admisión Aprobado</td><td colspan="2">Dirección de Admisión

Vicerrectorado Académico

Dirección General de Administración

Dirección de Planificación</td></tr>
<tr><td>Dirección de Admisión

Consejo Universitario</td><td>Estatuto

Reglamento General de la Universidad</td><td>Revisión de documentación normativa</td><td>Reglamento de Concurso de Admisión de Pregrado</td><td colspan="2">Dirección de Admisión</td></tr>
<tr><td>Dirección de Admisión

Vicerrectorado Académico</td><td>Plan de Difusión para Programas de Pregrado</td><td>Revisión del Plan Trabajo de la Dirección de Admisión

Aprobación del Plan de Difusión para Programas de Pregrado</td><td>Plan de Difusión de Programas de Pregrado Aprobado</td><td colspan="2">Dirección de Admisión

Vicerrectorado Académico

Dirección General de Administración

Dirección de Imagen</td></tr>
<tr><td rowspan="2">Postulantes (Estudiantes de 5° Secundaria, Egresados de Universidades)</td><td>Información personal de los postulantes</td><td>Se verifica la información personal y académica de los postulantes</td><td rowspan="2">Expedientes de Postulantes</td><td colspan="2">Dirección de Admisión</td></tr>
<tr><td>Voucher de Pago de Inscripción</td><td>Se verifica el código de voucher de pago</td><td colspan="2">Dirección General de Administración

Oficina de Contabilidad</td></tr>
</table>

	Ficha Socioeconómica		Se verifica el registro de la Ficha Socioeconómica		Dirección de Admisión Oficina de Estadística
Ingresantes	Información personal de los postulantes: certificados de estudios, DNI.		Se verifica la información personal y académica de los postulantes	Expedientes de Ingresantes	Dirección de Admisión
	Voucher de Pago de Acreditación		Se verifica el código de voucher de pago		Dirección de Escuela Profesional
Dirección de Admisión Consejo Universitario	Estatuto Reglamento General de la Universidad	**PM01.02.Proceso de Admisión de Programas de Posgrado**	Revisión de documentación normativa	Reglamento de Concurso de Admisión de Posgrado	Dirección de Admisión
Postulantes de Posgrado (Bachilleres)	Información personal de los postulantes		Se verifica la información personal y académica de los postulantes	Expedientes de Postulantes de Posgrado	Dirección de Admisión
	Voucher de Pago de Inscripción		Se verifica el código de voucher de pago		Dirección General de Administración Oficina de Contabilidad

III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO

11. TIPO	12. DESCRIPCIÓN
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica, 1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas, 2 Recepcionistas.
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).
	Material: Material de Oficina

IV. DOCUMENTACIÓN DEL PROCESO

13. REGISTROS DEL PROCESO	14. REFERENCIAS DOCUMENTALES
1. Registro de postulantes	1. Ley Universitaria 30220
2. Registro de ingresantes	2. Estatuto
3. Registro de vouchers de pago	3. Reglamento General
4. Registro de ingresantes acreditados	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento de Admisión
	8. Reglamento para Pago de Subvenciones al Personal

V. INDICADORES

15. NOMBRE DEL INDICADOR	16. RESPONSABLE	17. TIPO DE INDICADOR	18. FÓRMULA	19. PERIODICIDAD DE MEDICIÓN
Porcentaje de Postulantes por programas	Director de Admisión	Eficiencia	(N° de postulantes por programa/Total de postulantes inscritos) x 100	Semestral
Porcentaje de Ingresantes por programas	Director de Admisión	Eficiencia	(N° de ingresantes por programa/Total de ingresantes) x 100	Semestral

Nivel de Satisfacción del cliente	Director de Admisión	Eficiencia	(N° de Estudiantes al final del período académico - N° de Estudiantes nuevos)/Estudiantes al iniciar el período académico	Semestral

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 4: PM01- Diagrama BPMN 2.0

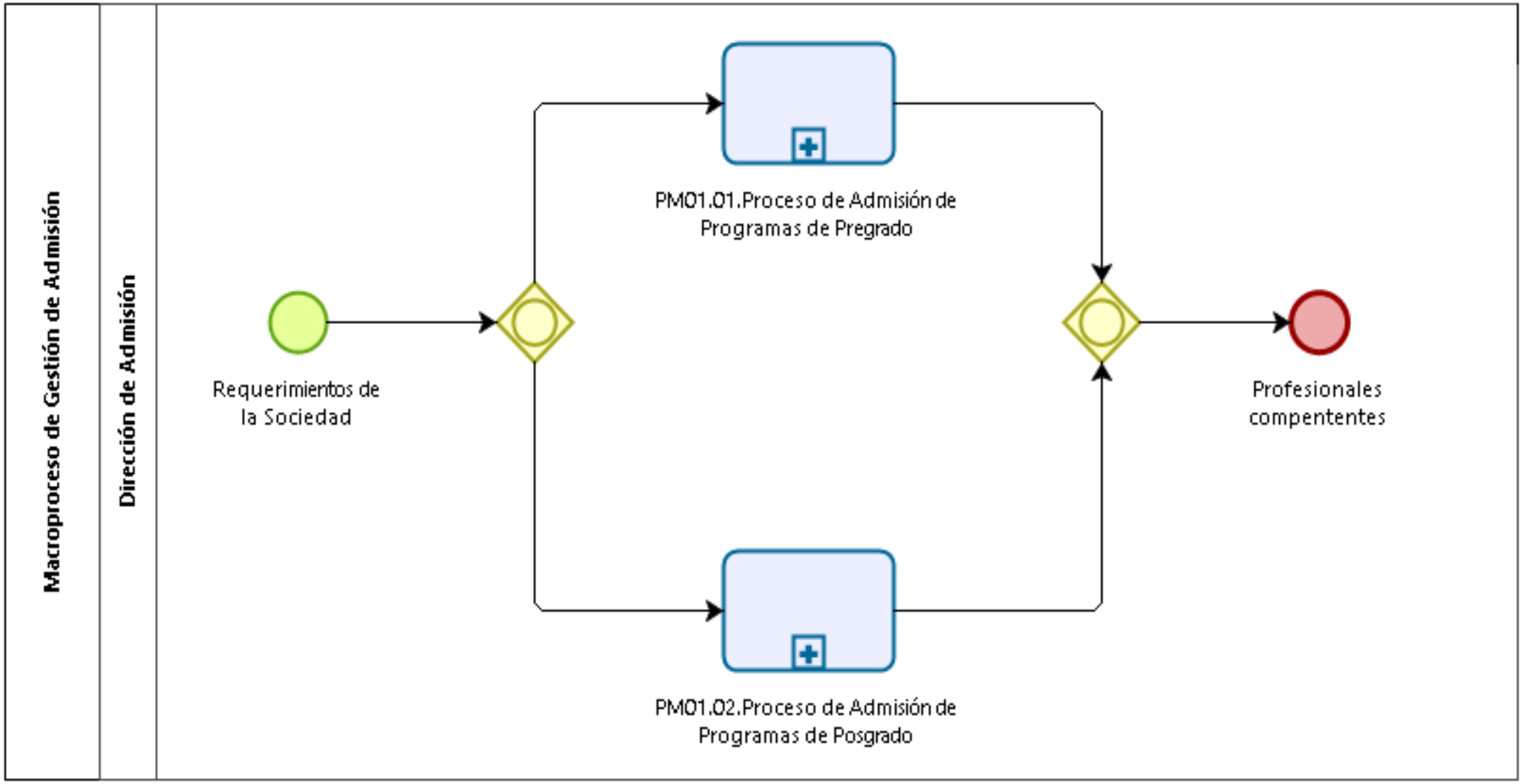


Tabla N° 6: PM01.01- Ficha de Proceso

	FICHA DE PROCESO DE NIVEL 1						**Código:** PM01.01 **Versión:** 1.0
I. DATOS GENERALES DEL PROCESO							
1. NOMBRE DEL PROCESO	Proceso de Admisión de Programas de Pregrado		**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Gestión de Admisión		
2. OBJETIVO DEL PROCESO	Implementar procesos de evaluación para asegurar que los postulantes cumplan con el perfil de ingreso de cada programa de pregrado.						
4. DUEÑO DEL PROCESO	Director de Admisión		**5. LÍMITES DEL PROCESO**	**INICIO**	Adecuación de la Ley de Universitaria al proceso de admisión de pregrado		
				FIN	Culmina con el Informe de Ejecución del Proceso de Admisión de Programas de Pregrado.		
II. DESCRIPCIÓN DEL PROCESO							
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**	**9. CONTROLES APLICADOS**		**10. PRODUCTOS**	**11. CLIENTES**	
Dirección de Admisión Consejo Universitario	Plan de Trabajo Plan Operativo Institucional	**PM01.01.01.Planificación del Proceso de Admisión de Pregrado**	Se verifica las actividades del Plan de Trabajo		Plan de actividades aprobado	Dirección de Admisión Dirección de Planificación	
	Presupuesto Plan Operativo Institucional		Se verifica el Presupuesto		Presupuesto aprobado	Dirección de Admisión Dirección General de Administración Dirección de Planificación	
Dirección de Admisión	Cuadro de Recurso Humano de Apoyo		Se realiza evaluación del recurso humano de apoyo		Acuerdo de Consejo Universitario con Cuadro de Recurso Humano Ganador	Dirección de Admisión Dirección General de Administración Dirección de Recursos Humanos	
MINEDU Consejo Universitario Dirección de Escuela	Ley Universitaria N°30220 Estatuto Reglamento General Cuadro de Vacantes		Se realizan reuniones para el análisis de las normas del estado y la universidad para la elaboración del Reglamento de Admisión de Pregrado		Resolución de aprobación del Reglamento de Admisión de Pregrado aprobado	Dirección de Admisión Consejo Universitario Dirección General de Administración	
Dirección de Admisión Dirección de Escuela	Reglamento de Admisión Cuadro de Vacantes Perfil de Ingreso Perfil del Egresado		Se realizan reuniones para analiza el perfil de ingreso y del egresado para la elaboración del Prospecto de Admisión y solicitar su		Prospecto de Admisión	Dirección de Admisión Dirección General de Administración Oficina de Abastecimiento	

			diseño, diagramado y elaboración		
Dirección de Admisión	Requisitos de spot publicitario Solicitud de souvenirs	**PM01.01.02.Difusión del Proceso de Admisión de Pregrado**	La Dirección de Imagen realiza elaboración de spot publicitario y este se valida con la Dirección de Admisión. La Dirección General de Administración gestiona a través de la Oficina de Abastecimiento la elaboración y compra de souvenirs.	Spot publicitario Souvenirs	Dirección de Admisión Dirección General de Administración Dirección de Imagen
Dirección de Admisión	Registro de Visitas Registros fotográficos y audiovisuales Actas		Se realiza evaluación del Informe de Difusión	Informe de Difusión verificado	Dirección de Admisión Vicerrectorado Académico
Postulante	Realiza Pago por derecho de inscripción en el Banco de la Nación. Registro de información personal y académica en Sistema de información de la UNS.	**PM01.01.03.Inscripción al Proceso de Admisión de Pregrado**	El Sistema de Información realiza verificaciones de voucher de derecho por inscripción con información personal.	Registro de inscripción al postulante	Dirección de Admisión Dirección General de Administración Oficina de Fondos
Dirección de Admisión	Exámenes del Proceso de Admisión	**PM01.01.04.Gestión de Exámenes del Proceso de Admisión de Pregrado**	Realizar aplicación y evaluación de los exámenes del Proceso de Admisión	Registro de Ingresantes	Dirección de Admisión Dirección de Imagen Ingresantes
Ingresantes Dirección de Admisión	Pago por derecho de certificado de ingreso en el Banco de la Nación Constancias de Ingresantes	**PM01.01.05.Acreditación de ingresantes a las Carreras Profesionales de Pregrado**	Realizar validación de constancias de ingreso y de requisitos de los ingresantes.	Constancia de Ingresante	Dirección de Admisión Ingresantes

Dirección de Admisión	Informe de Ejecución de Proceso de Admisión de Pregrado	**PM01.01.06.Verificación del Proceso de Admisión de Pregrado**	Realiza verificación del Informe de Ejecución y determina acciones de mejora	Informe de Ejecución de Proceso de Admisión de Pregrado verificado	Dirección de Admisión Vicerrectorado Académico

III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO	
12. TIPO	**13. DESCRIPCIÓN**
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica, 1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas, 2 Recepcionistas.
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).
	Material: Material de Oficina

IV. DOCUMENTACIÓN DEL PROCESO	
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**
1. Registro de postulantes de pregrado	1. Ley Universitaria 30220
2. Registro de ingresantes de pregrado	2. Estatuto
3. Registro de vouchers de pago de postulantes	3. Reglamento General
4. Registro de ingresantes acreditados	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento de Admisión
	8. Reglamento para Pago de Subvenciones al Personal

V. INDICADORES				
16. NOMBRE DEL INDICADOR	**17. RESPONSABLE**	**18. TIPO DE INDICADOR**	**19. FÓRMULA**	**20. PERIODICIDAD DE MEDICIÓN**
Porcentaje de objetivos alcanzadas	Director de Admisión	Eficacia	(N° de objetivos alcanzados/Total de objetivos propuestos) x 100	Mensual
Satisfacción de las actividades de difusión de Admisión	Director de Admisión	Eficiencia	(N° de usuarios satisfechos con la difusión/Total de usuarios entrevistados) x 100 *Los usuarios está conformado por la cantidad de alumnos y docentes de instituciones educativas	Mensual

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 5: PM01.01 (General) - Diagrama BPMN 2.0

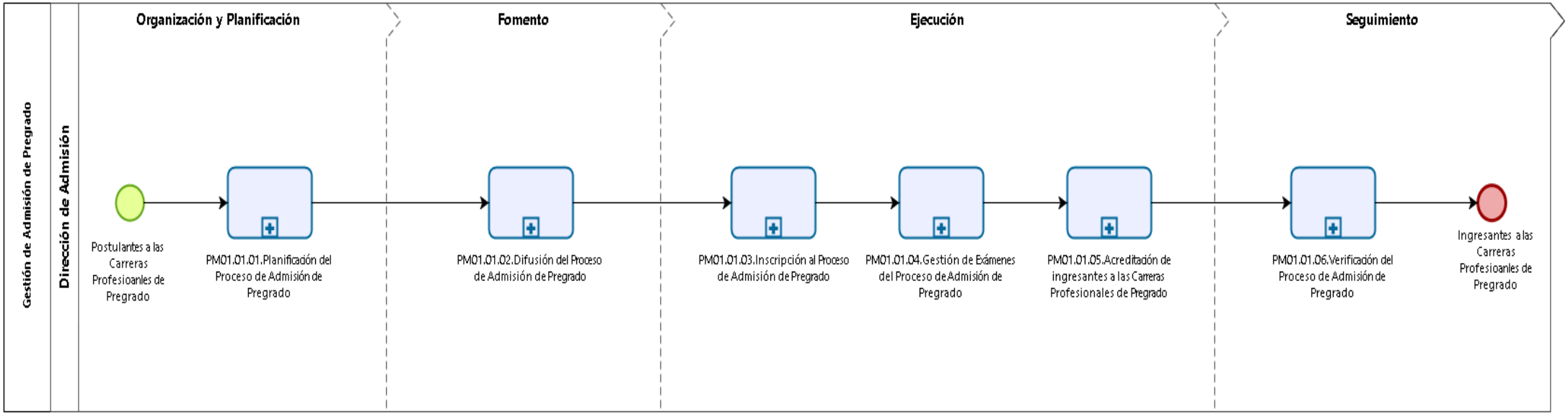


Figura N° 6: PM01.01 (Parte 1) - Diagrama BPMN 2.0

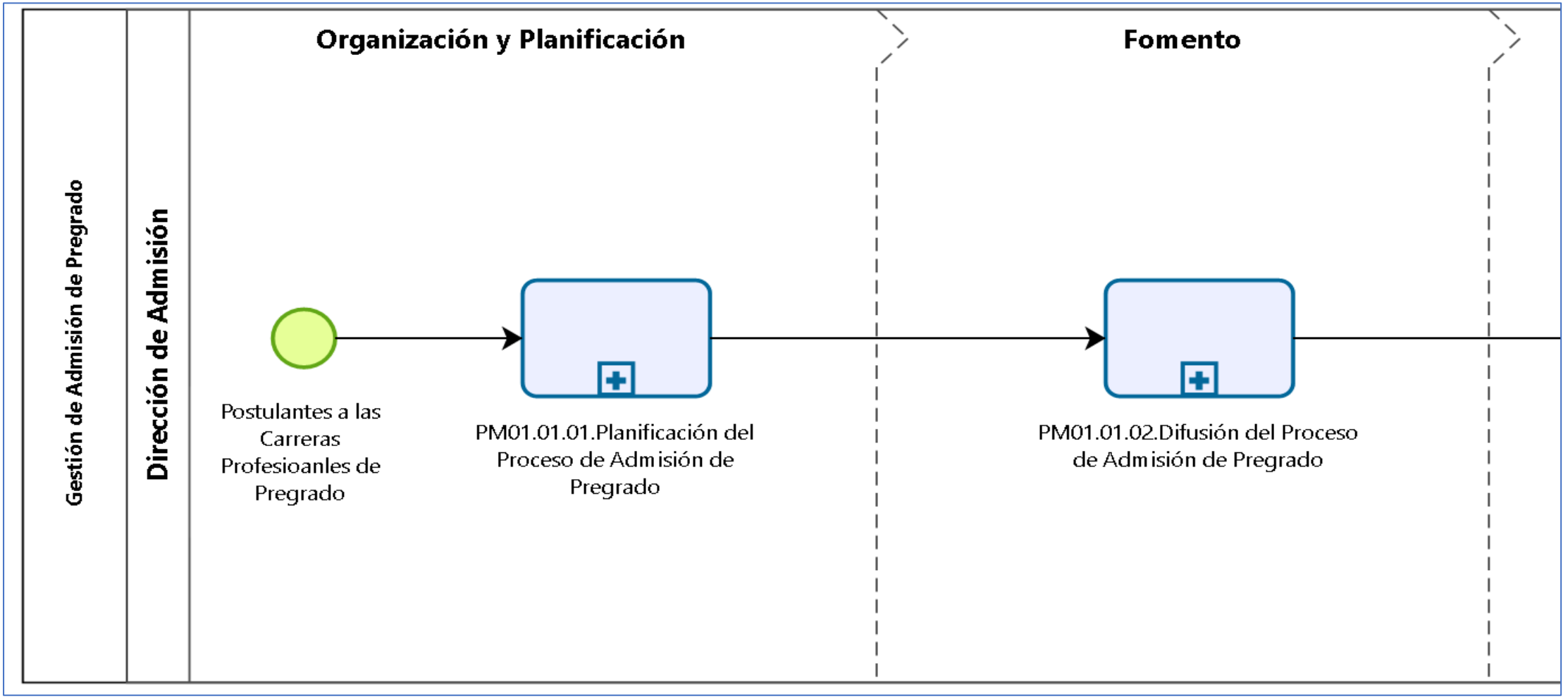


Figura N° 7: PM01.01 (Parte 2) - Diagrama BPMN 2.0

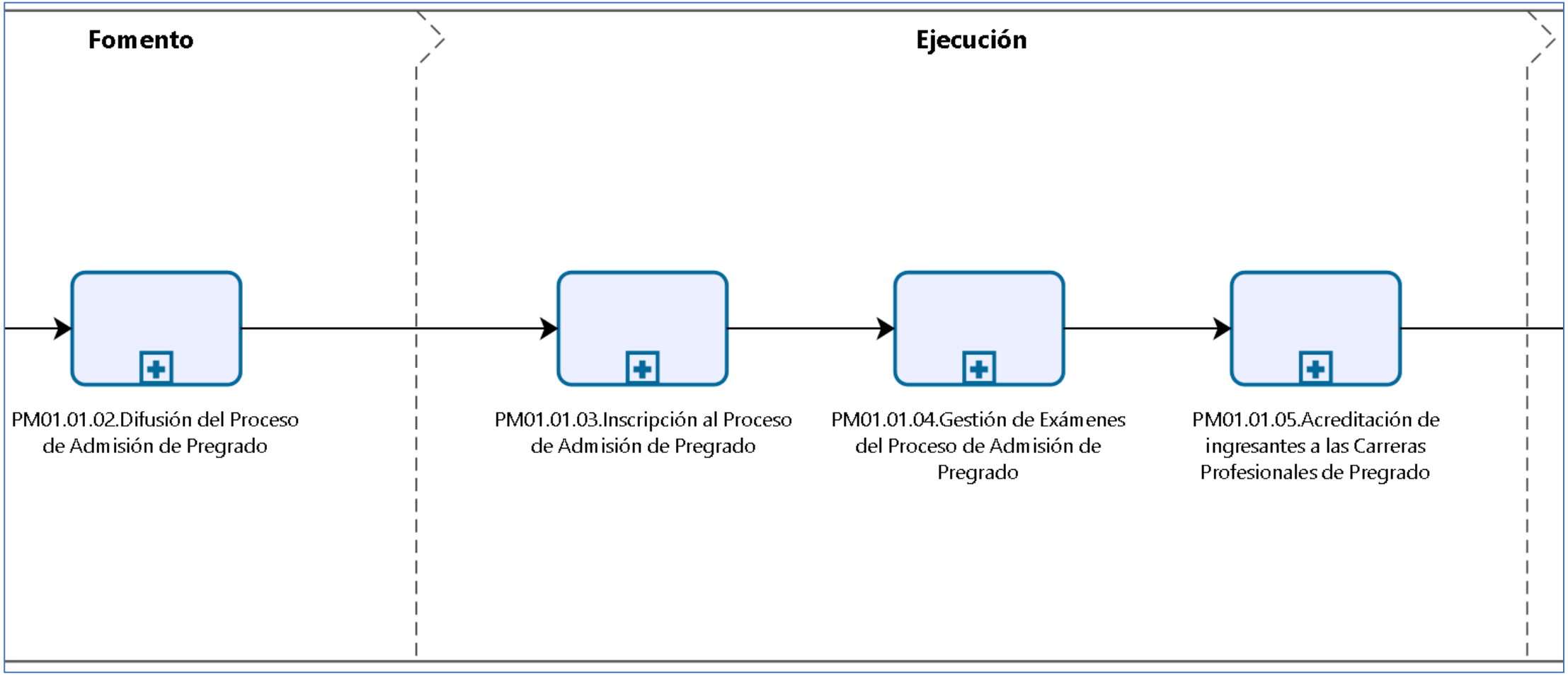


Figura N° 8: PM01.01 (Parte 3) - Diagrama BPMN 2.0

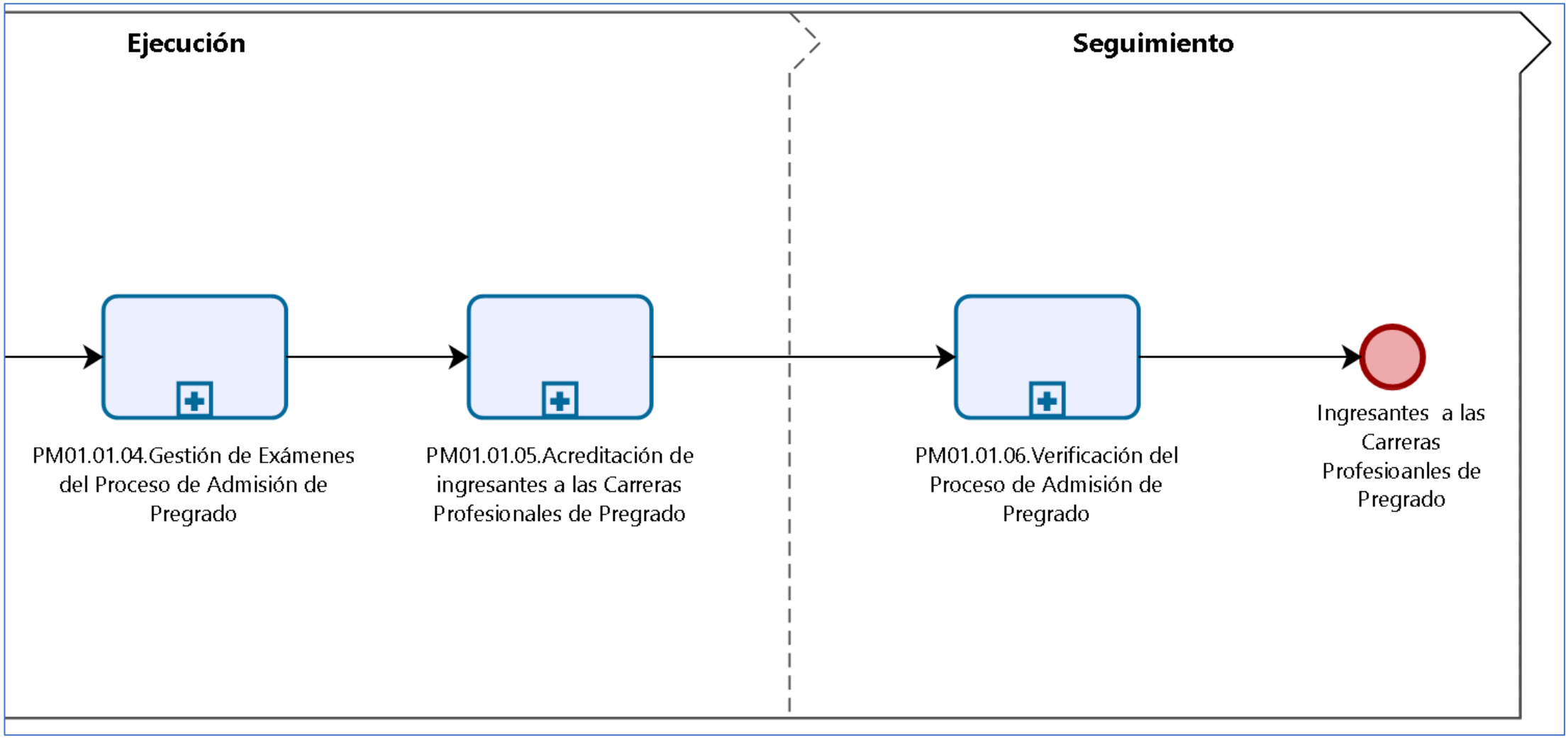


Tabla N° 7: PM01.01.01 - Ficha de Proceso

	FICHA DE PROCESO DE NIVEL 2					**Código:** PM01.01.01 **Versión:** 1.0
I. DATOS GENERALES DEL PROCESO						
1. NOMBRE DEL PROCESO	Planificación del Proceso de Admisión de Pregrado		**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Proceso de Admisión de Programas de Pregrado	
2. OBJETIVO DEL PROCESO	Planificar los recursos y personal para el proceso de admisión de pregrado.					
4. DUEÑO DEL PROCESO	Director de Admisión		**5. LÍMITES DEL PROCESO**	**INICIO**	Elaboración del Plan de Trabajo del Proceso de Admisión de Pregrado	
				FIN	Culmina con la recepción del prospecto de admisión aprobado con Resolución de Consejo Universitario	
II. DESCRIPCIÓN DEL PROCESO						
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**		**9. CONTROLES APLICADOS**	**10. PRODUCTOS**	**11. CLIENTES**
Dirección de Admisión Consejo Universitario	Plan de trabajo Plan Operativo Institucional	**PM01.01.01.01.Elaboración y Aprobación del Plan de Trabajo y Presupuesto**		Se verifica las actividades del Plan de Trabajo Se verifica el Presupuesto	Plan de Trabajo y Presupuesto aprobado	Dirección de Admisión Dirección General de Administración Dirección de Planificación
Dirección de Admisión	Cuadro de Recurso Humano de Apoyo	**PM01.01.01.02.Selección y captación del Recurso Humano de Apoyo**		Se realiza evaluación del recurso humano de apoyo	Acuerdo con Cuadro de Recurso Humano Ganador	Dirección de Admisión Dirección General de Administración Dirección de Recursos Humanos
Dirección de Admisión Dirección de Escuela	Reglamento de Admisión Cuadro de Vacantes	**PM01.01.01.03.Elaboración y aprobación del Reglamento de Admisión**		Se realizan reuniones para el análisis de las normas del estado y la universidad para la elaboración del Reglamento de Admisión de Pregrado y solicitar su aprobación	Resolución de aprobación del Reglamento de Admisión de Pregrado aprobado	Dirección de Admisión Consejo Universitario Dirección General de Administración
Dirección de Admisión Dirección de Escuela	Reglamento de Admisión Cuadro de Vacantes Perfil de Ingreso Perfil del Egresado	**PM01.01.01.04.Elaboración del Prospecto de Admisión**		Se realizan reuniones para analizar el perfil del ingresante y del egresado para la elaboración del Prospecto de Admisión y solicitar su diseño, diagramado y solicitar su elaboración	Archivo de Prospecto de Admisión	Dirección de Admisión Dirección General de Administración Oficina de Abastecimiento

Dirección de Admisión	Reglamento de Admisión Cuadro de Vacantes de Carrera profesional por modalidad Perfil de Ingreso Perfil del Egresado		Se realizan reuniones para analizar el perfil de ingreso y del egresado, para la elaboración del Prospecto de Admisión para luego solicitar su confección e impresión.	Prospecto de Admisión	Dirección de Admisión Dirección General de Administración Oficina de Abastecimiento

III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO	
12. TIPO	**13. DESCRIPCIÓN**
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica, 1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas, 2 Recepcionistas.
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).
	Material: Material de Oficina

IV. DOCUMENTACIÓN DEL PROCESO	
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**
1. Actas de Reuniones	1. Ley Universitaria 30220
2. Registro de Recurso Humano de Apoyo	2. Estatuto
3. Registro de vouchers de pago de postulantes	3. Reglamento General
	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento para Pago de Subvenciones al Personal

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 9: PM01.01.01 - Diagrama BPMN 2.0

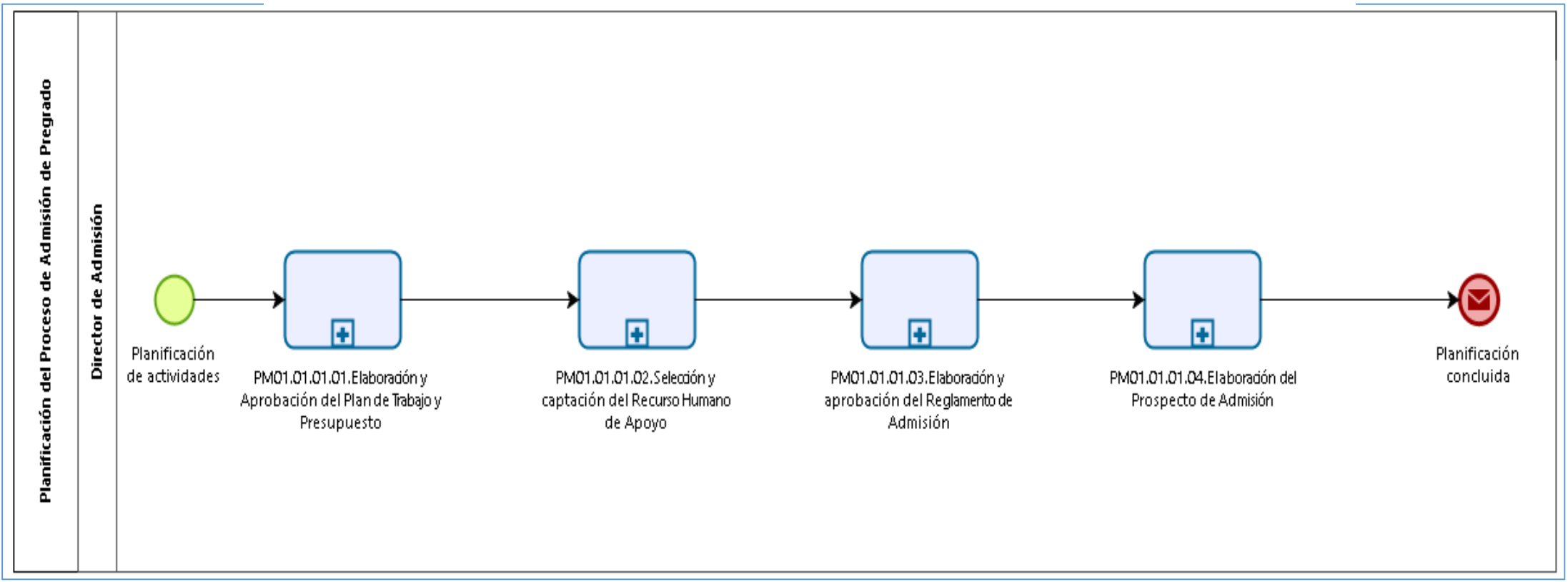


Tabla N° 8: PM01.01.01.01- Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.01.01 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.01.Planificación del Proceso de Admisión de Pregrado
TÍTULO:	Elaboración y Aprobación del Plan de Trabajo y Presupuesto		
A. OBJETIVO:	Elaborar el plan de Trabajo para el proceso de admisión de programas de pregrado.		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Estatuto, Reglamento General.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo.		

	E. DESCRIPCIÓN DEL PROCEDIMIENTO:	**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Revisar Plan Operativo Institucional (POI).		Dirección de Admisión	Director(a) de Admisión	Plan Operativo Institucional
2	Organizar Trabajo y cronograma acorde con el POI.		Dirección de Admisión	Director(a) de Admisión	Actas
3	Elaborar Plan de Trabajo y Presupuesto.		Dirección de Admisión	Director(a) de Admisión	Actas
4	Solicitar aprobación del Plan de Trabajo y Presupuesto.		Dirección de Admisión	Director(a) de Admisión	Oficio, Plan de Trabajo y Presupuesto
5	Recepcionar y validar Plan de Trabajo y Presupuesto.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio, Plan de Trabajo y Presupuesto
6	Solicitar aprobación del Plan de Trabajo y Presupuesto.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio
7	Revisar Plan de Trabajo y Presupuesto.		Consejo Universitario	Consejo Universitario	Oficio, Plan de Trabajo y Presupuesto
	Se cuenta con observaciones continuar, caso contrario ir al paso 9.		Consejo Universitario	Consejo Universitario	
8	Retornar Plan de Trabajo y Presupuesto, ir al paso 3.		Consejo Universitario	Consejo Universitario	Acuerdo
9	Aprobar Plan de Trabajo y Presupuesto, registrar en libro de actas.		Consejo Universitario	Secretario(a) General	Libro de Actas
10	Redactar resolución de aprobación del Plan de Trabajo y Presupuesto.		Secretaría General	Secretario(a) General	Registro de Resoluciones
11	Enviar resolución a la Dirección de Admisión y dependencias interesadas.		Secretaría General	Secretario(a) General	Resolución de Consejo Universitario
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento

I. ANEXOS:			
ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 10: PM01.01.01.01 (General) - Ficha de Proceso

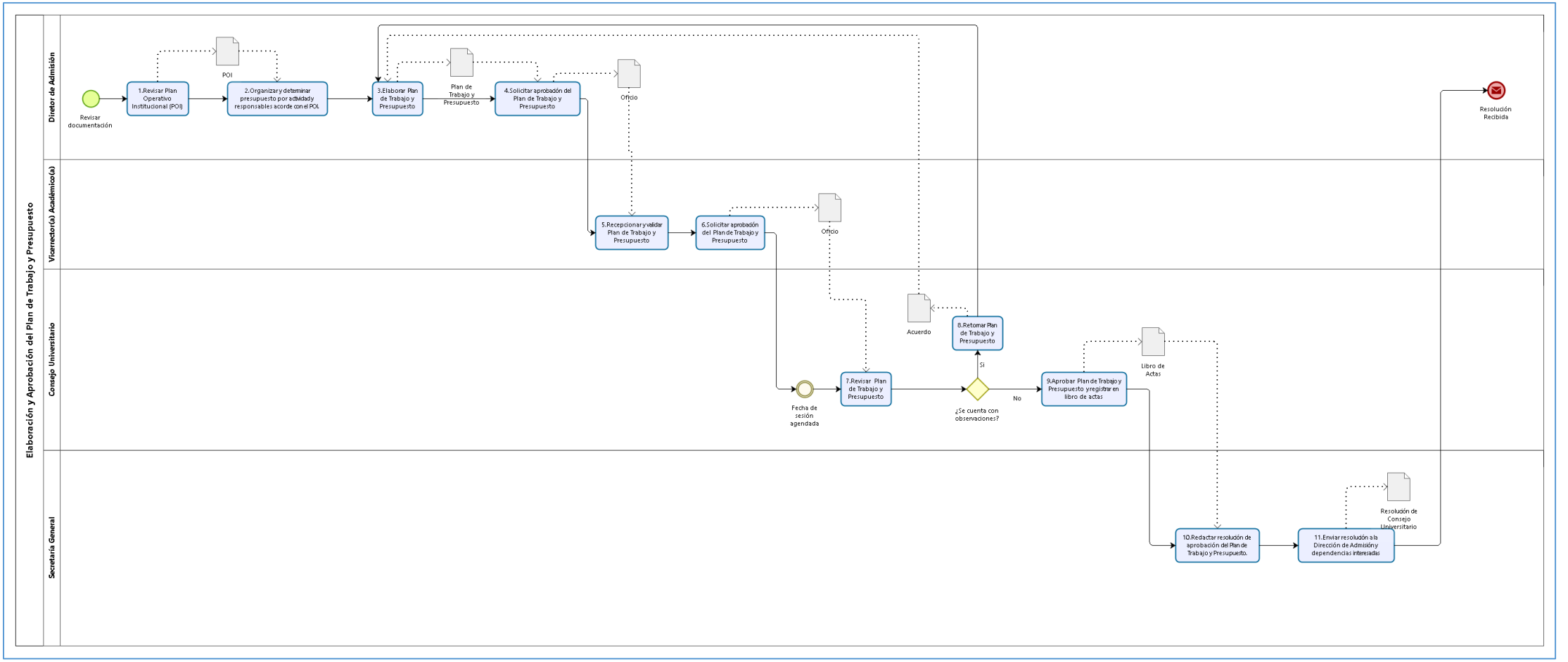


Figura N° 11: PM01.01.01.01 (Parte 1) - Ficha de Proceso

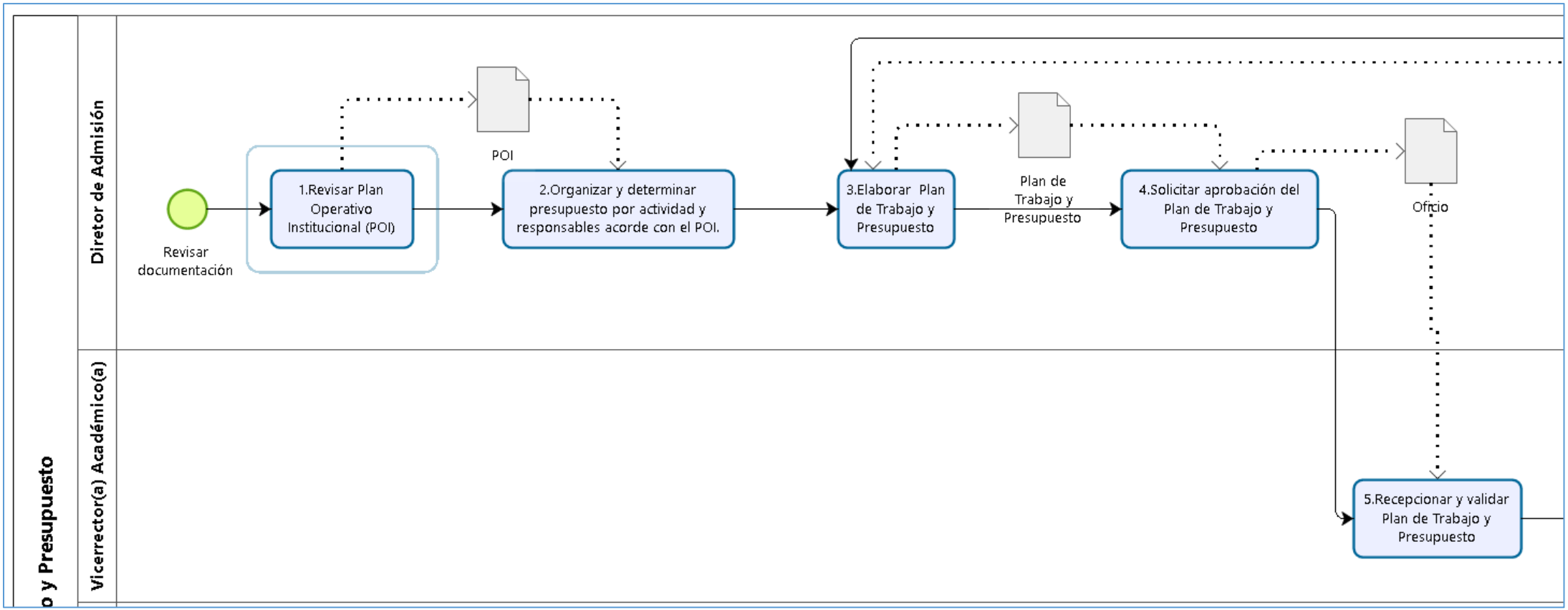


Figura N° 12: PM01.01.01.01 (Parte 2) - Ficha de Proceso

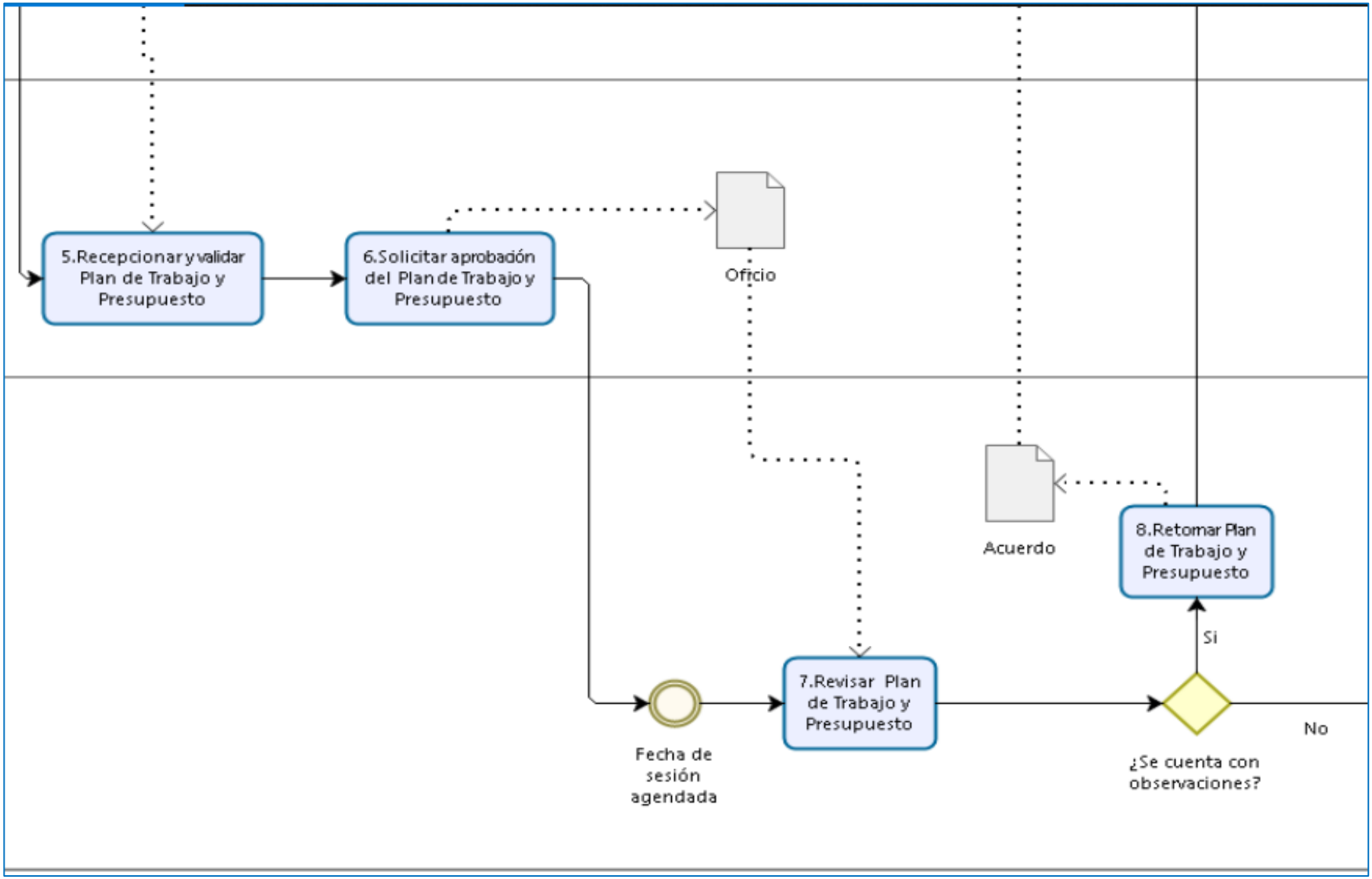


Figura N° 13: PM01.01.01.01 (Parte 3) - Ficha de Proceso

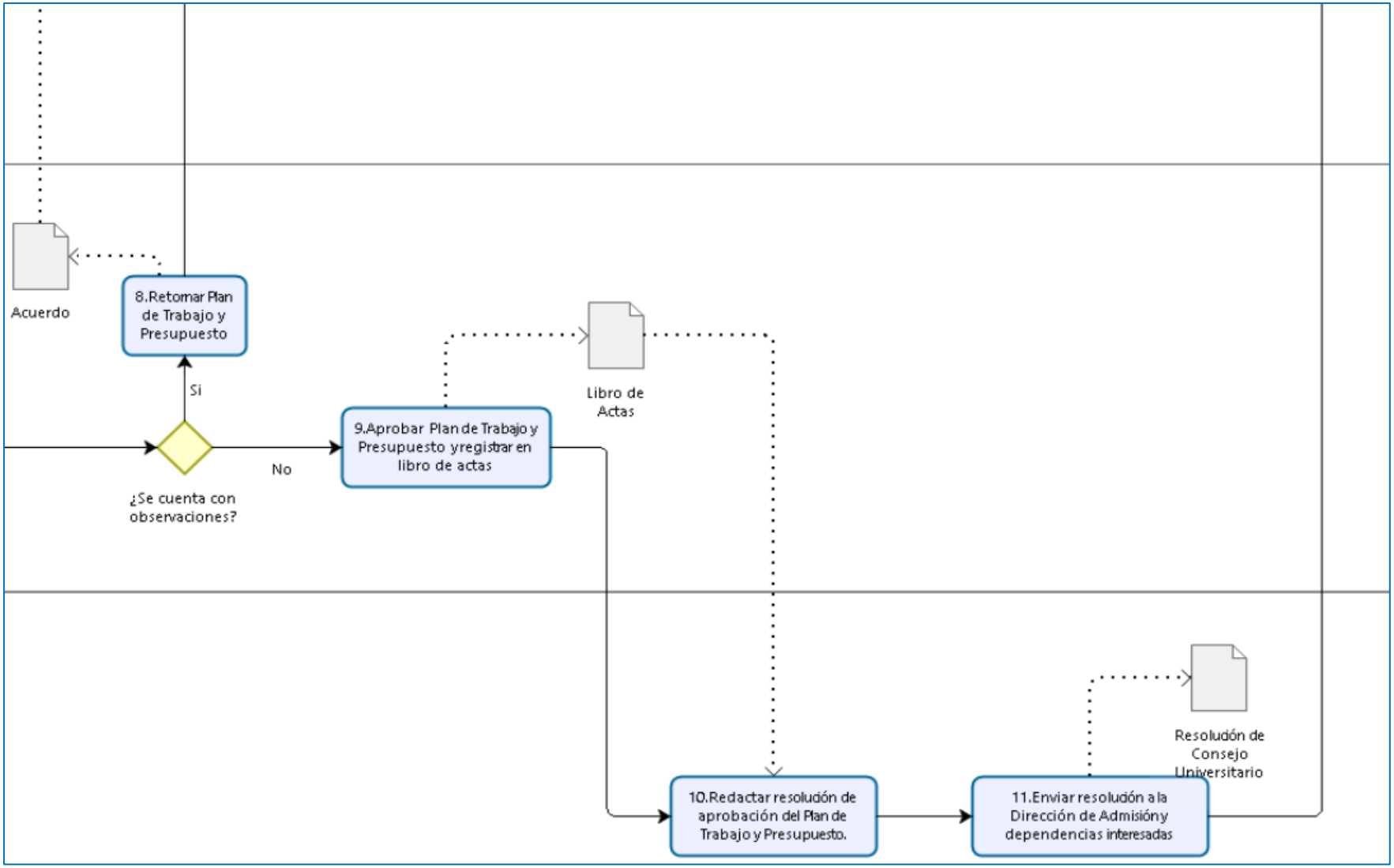


Figura N° 14: PM01.01.01.01 (Parte 4) - Ficha de Proceso

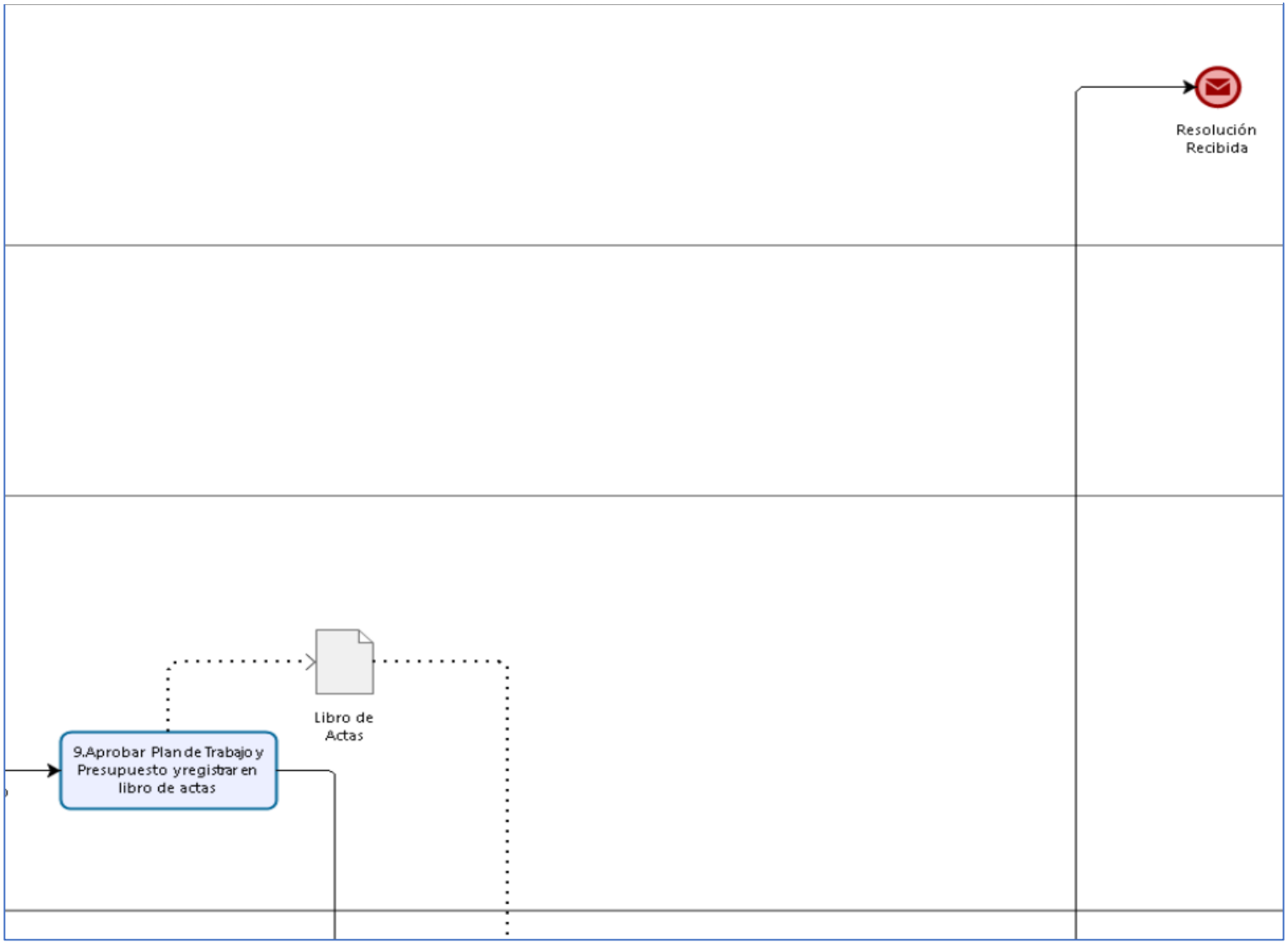


Tabla N° 9: PM01.01.01.02- Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.01.02 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.01.Planificación del Proceso de Admisión de Pregrado
TÍTULO:	Selección y captación del Recurso Humano de Apoyo		
A. OBJETIVO:	Determinar el recurso humanos de apoyo.		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Estatuto, Reglamento General		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo.		

	E. DESCRIPCIÓN DEL PROCEDIMIENTO:	**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Elaborar perfil del recurso humano de apoyo.		Dirección de Admisión	Director(a) de Admisión	Convocatoria
2	Solicitar publicación de convocatoria en el Portal Web.		Dirección de Admisión	Director(a) de Admisión	Oficio
3	Publicar convocatoria en el Portal Web.		Dirección de Imagen	Personal de la Dirección de Imagen	Registro en Portal Web
4	Realizar entrevistas.		Dirección de Admisión	Director(a) de Admisión	Registro de entrevistas
5	Revisar CVs y determinar seleccionados.		Dirección de Admisión	Director(a) de Admisión	Actas, Cuadro de Mérito
6	Solicitar aprobación del recurso humano ganador.		Dirección de Admisión	Director(a) de Admisión	Oficio
7	Recepcionar y solicitar aprobación del recurso humano ganador.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio
8	Revisar solicitud y cuadro del recurso humanos ganador.		Consejo Universitario	Consejo Universitario	Oficio, Cuadro de Recurso Humano
9	Aprobar recurso humano y registrar en libro de actas.		Consejo Universitario	Secretario(a) General	Libro de Actas
10	Redactar acuerdo de aprobación del recurso humano.		Secretaría General	Secretario(a) General	Registro de Acuerdos
11	Enviar acuerdo a la Dirección de Admisión y dependencias interesadas.		Secretaría General	Secretario(a) General	Acuerdo de Consejo Universitario
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 15: PM01.01.01.02 (General) - Diagrama BPMN 2.0

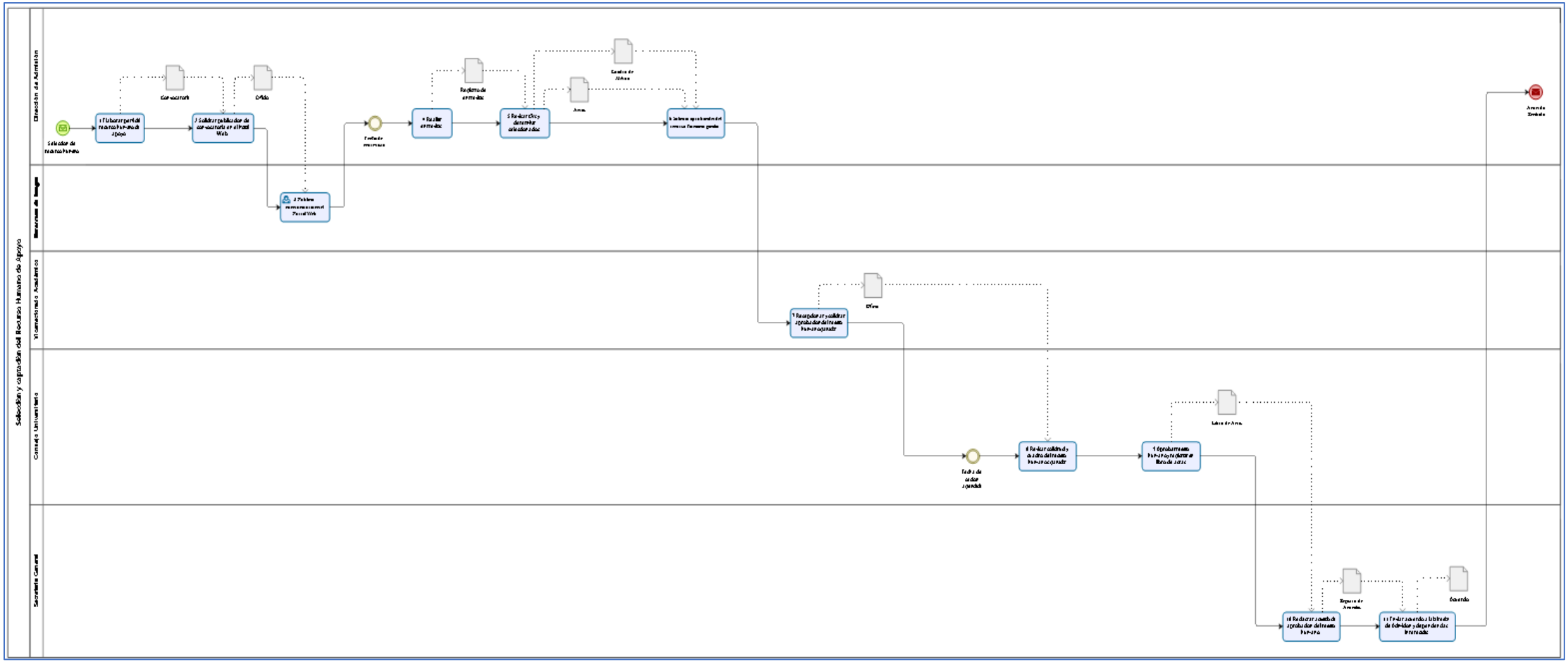


Figura N° 16: PM01.01.01.02 (Parte 1) - Diagrama BPMN 2.0

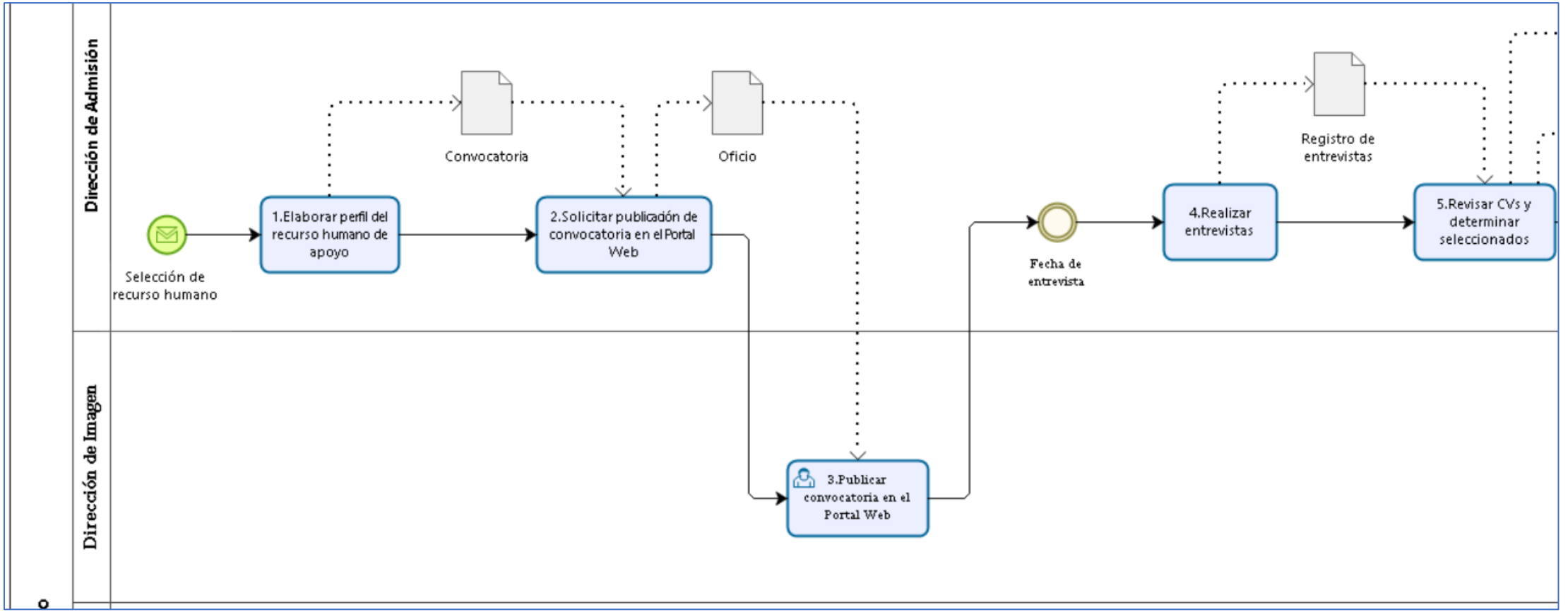


Figura N° 17: PM01.01.01.02 (Parte 2) - Diagrama BPMN 2.0

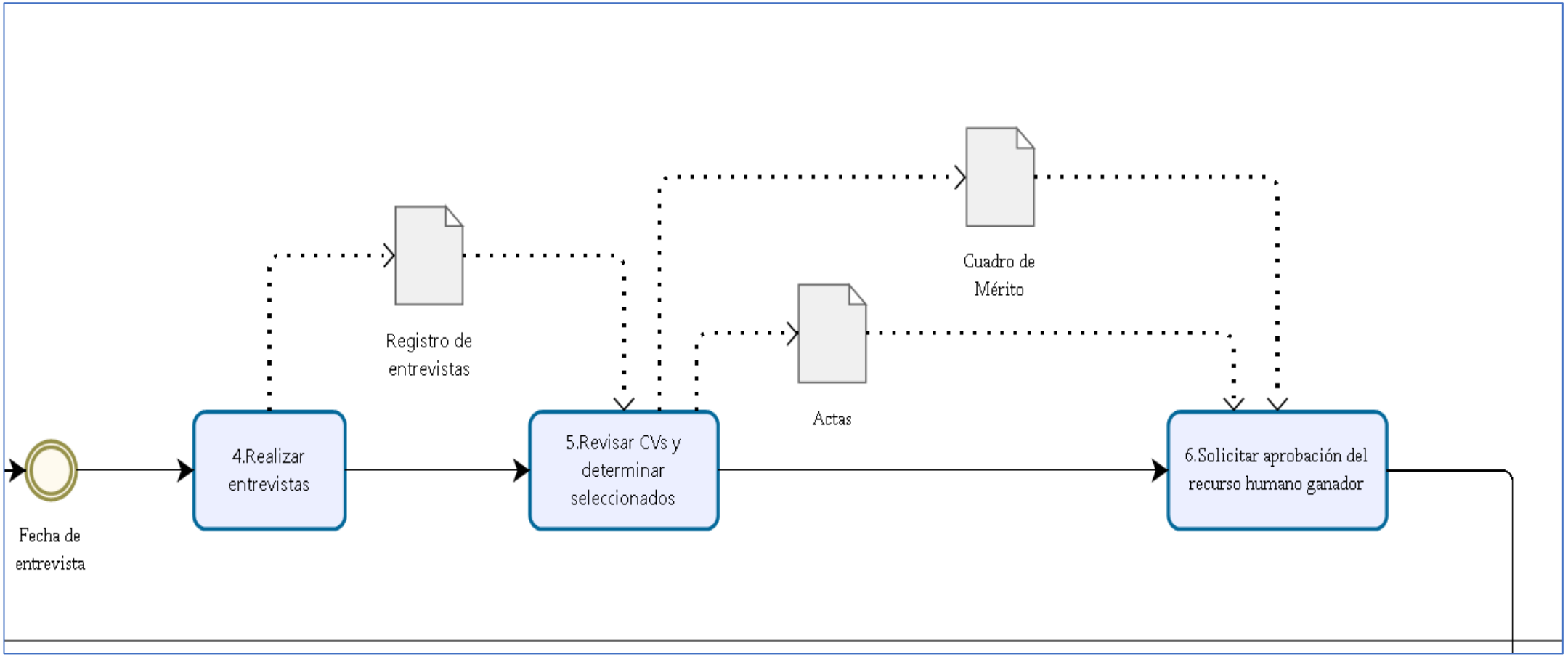


Figura N° 18: PM01.01.01.02 (Parte 3) - Diagrama BPMN 2.0

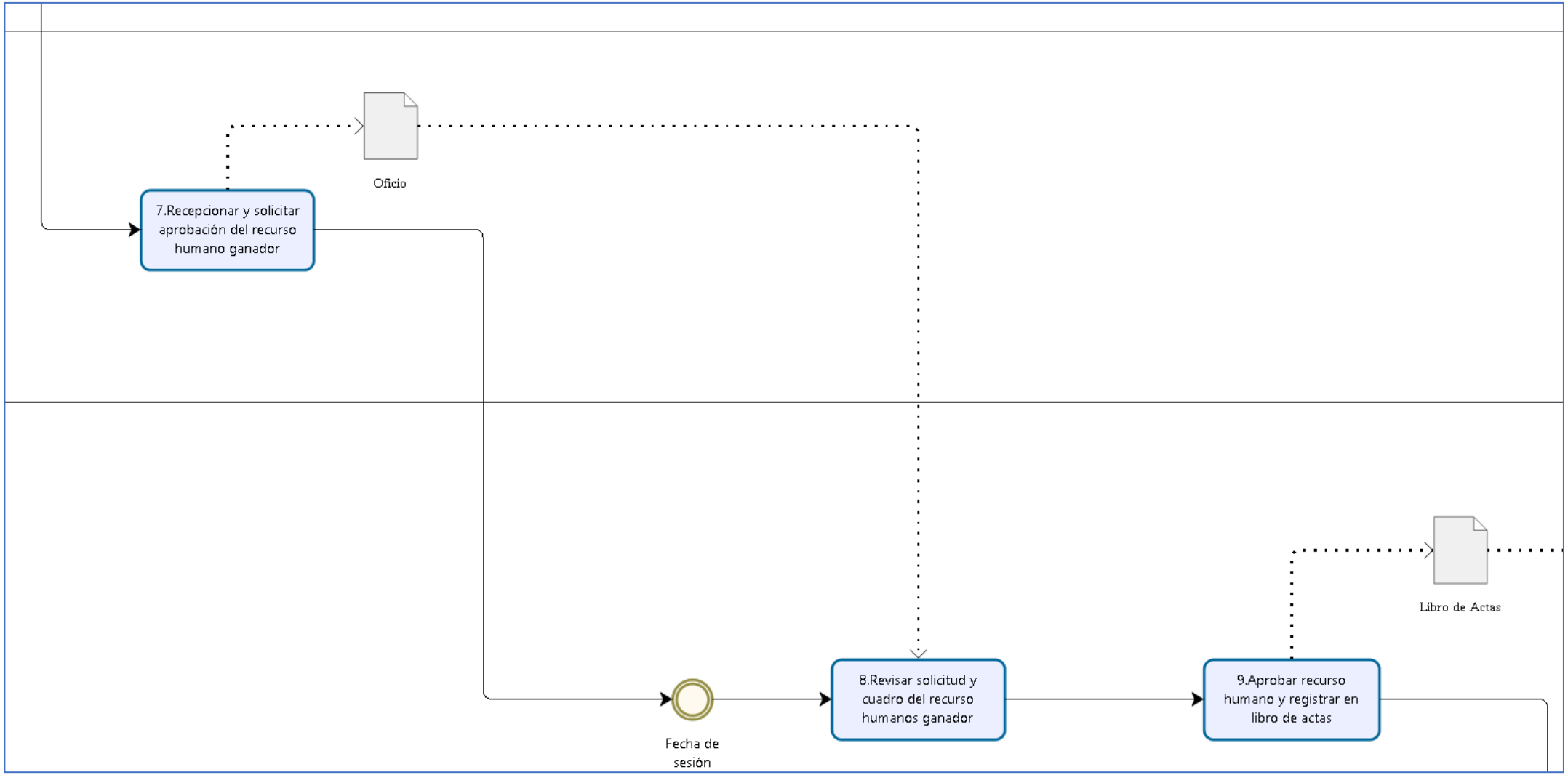


Figura N° 19: PM01.01.01.02 (Parte 4) - Diagrama BPMN 2.0

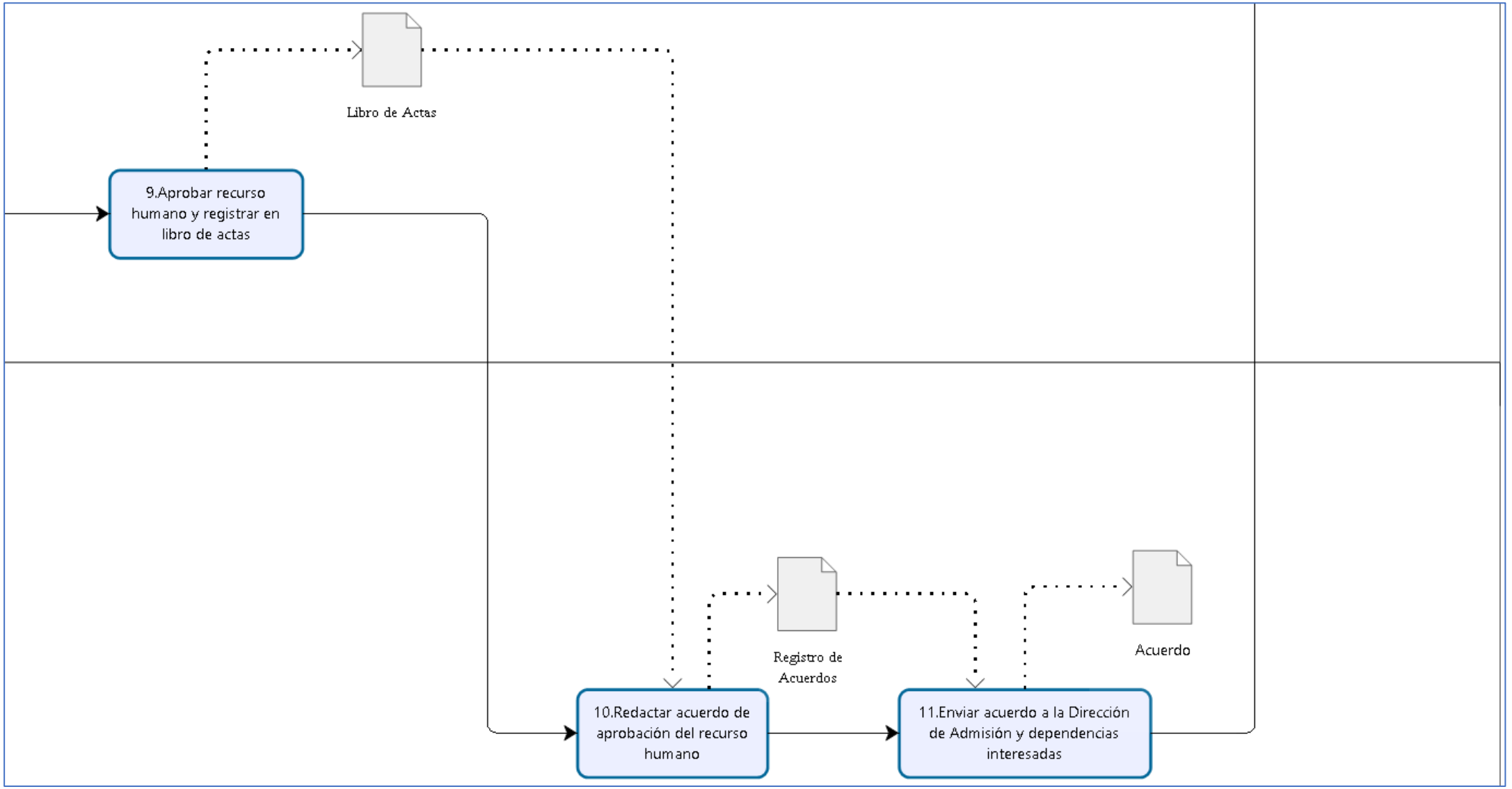


Tabla N° 10: PM01.01.01.03- Ficha de Proceso

		FICHA DE PROCEDIMIENTO		**Código**: PM01.01.01.03	
				Versión: 1.0	
TIPO:	PROCEDIMIENTO		**PROCESO DE NIVEL SUPERIOR:**	PM01.01.01.Planificación del Proceso de Admisión de Pregrado	
TÍTULO:	Elaboración y aprobación del Reglamento de Admisión				
A. OBJETIVO:		Elaborar y aprobar Reglamento de Admisión			
B. UNIDAD RESPONSABLE:		Dirección de Admisión			
C. BASE LEGAL:		Ley Universitaria N°30220, Estatuto, Reglamento General.			
D. REQUISITOS DEL PROCEDIMIENTO:		Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo.			
E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Elaborar y/o actualizar Reglamento de Admisión de Pregrado.		Dirección de Admisión	Director(a) de Admisión	Actas
2	Solicitar aprobación del Reglamento de Admisión de Pregrado.		Dirección de Admisión	Director(a) de Admisión	Oficio, Reglamento de Admisión de Pregrado
3	Recepcionar y solicitar aprobación del Reglamento de Admisión de Pregrado.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio
4	Revisar Reglamento de Admisión de Pregrado.		Consejo Universitario	Consejo Universitario	Oficio
5	Aprobar Reglamento de Admisión de Pregrado y registrar en libro de actas.		Consejo Universitario	Secretario(a) General	Libro de Actas
6	Redactar resolución de aprobación de Reglamento de Admisión de Pregrado.		Secretaría General	Secretario(a) General	Registro de Resoluciones
7	Enviar resolución a la Dirección de Admisión y dependencias interesadas.		Secretaría General	Secretario(a) General	Resolución de Consejo Universitario
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:		Versión 1.0: Elaboración del Documento			
I. ANEXOS:					
ETAPA		**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**	
Formulado por:		Juan Carlos Guzman Comesaña			
Cargo:					
Revisado por:					
Cargo					
Aprobado por:					
Cargo:					

Figura N° 20: PM01.01.01.03 (General) - Diagrama BPMN 2.0

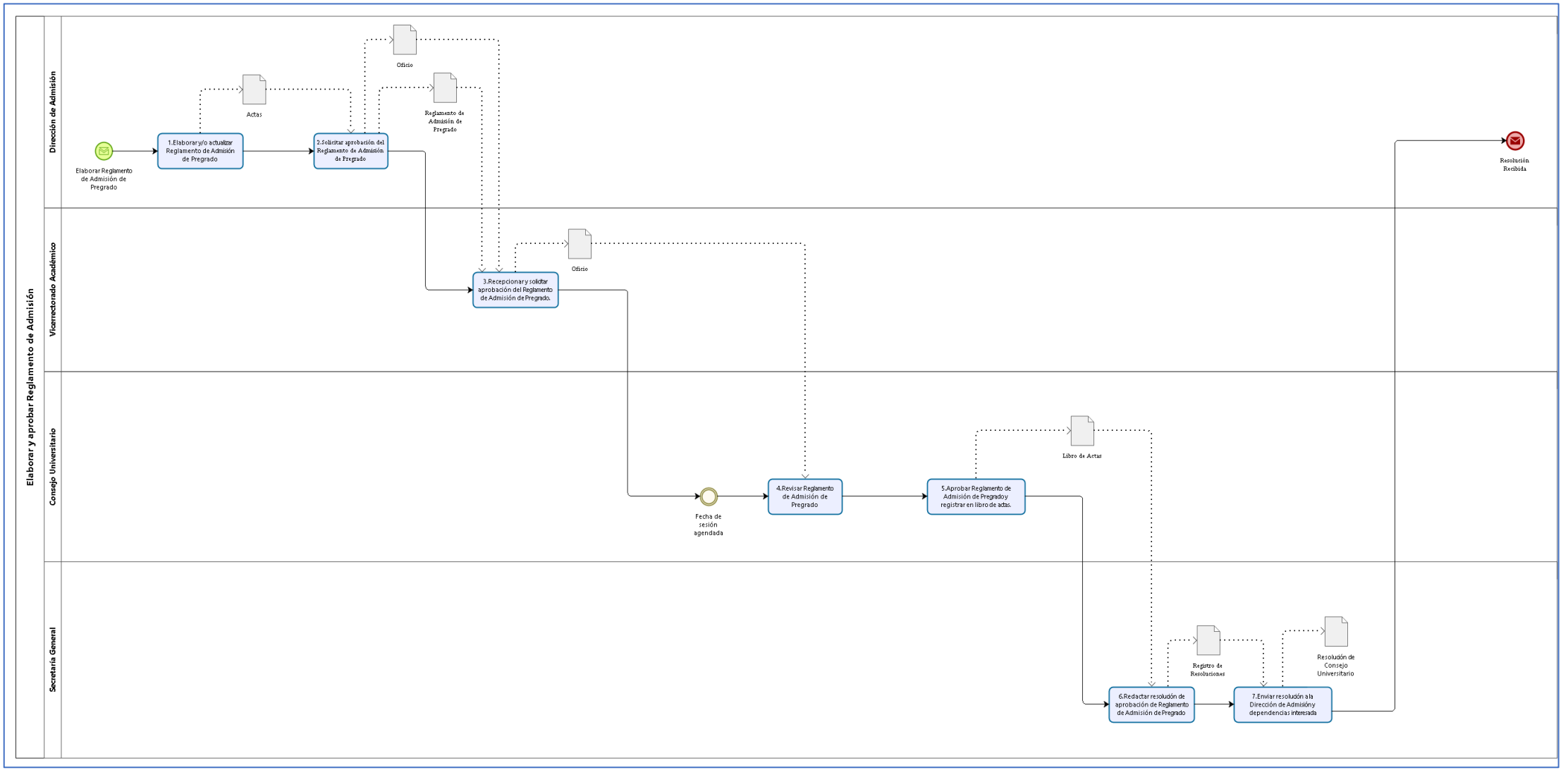


Figura N° 21: PM01.01.01.03 (Parte 1) - Diagrama BPMN 2.0

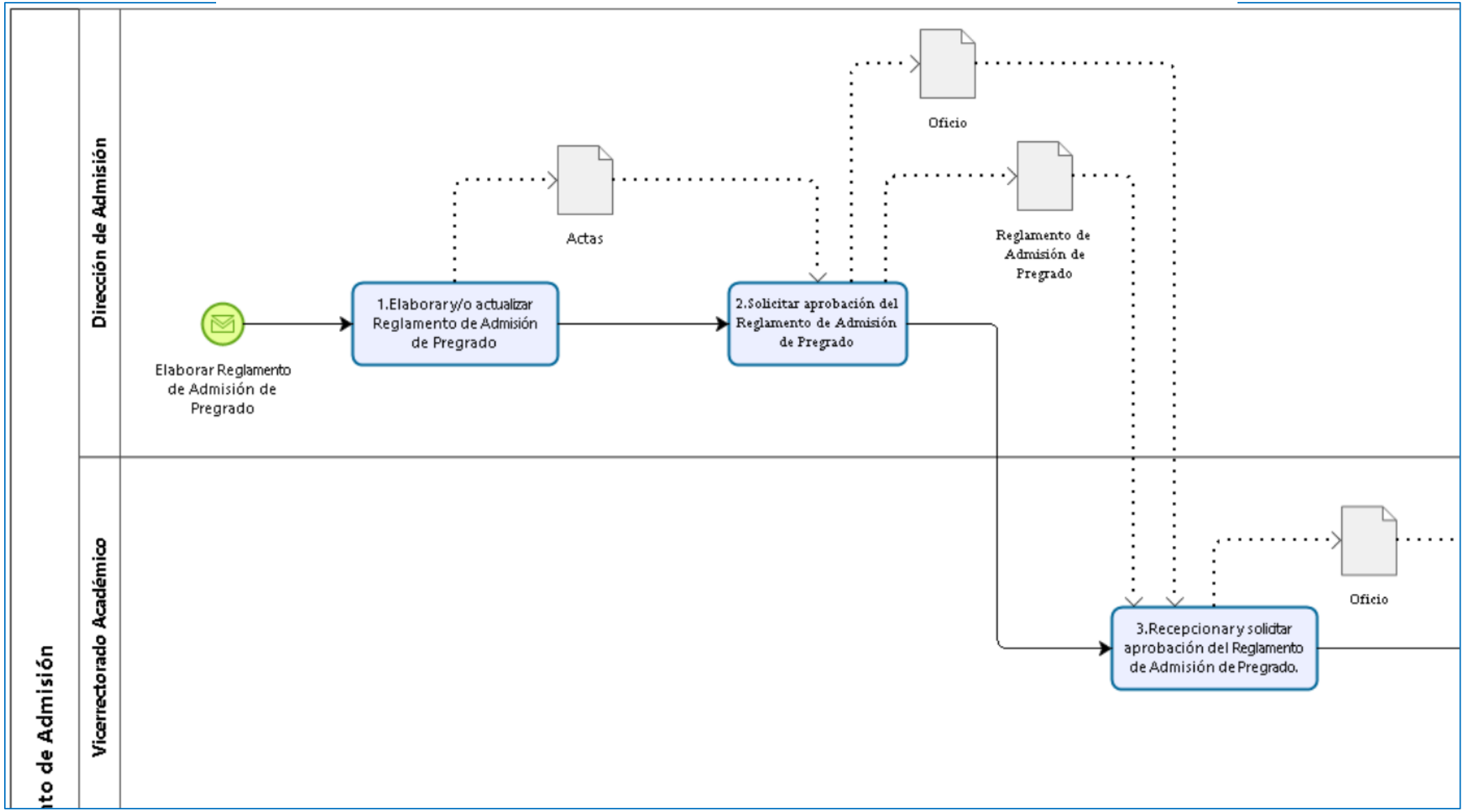


Figura N° 22: PM01.01.01.03 (Parte 2) - Diagrama BPMN 2.0

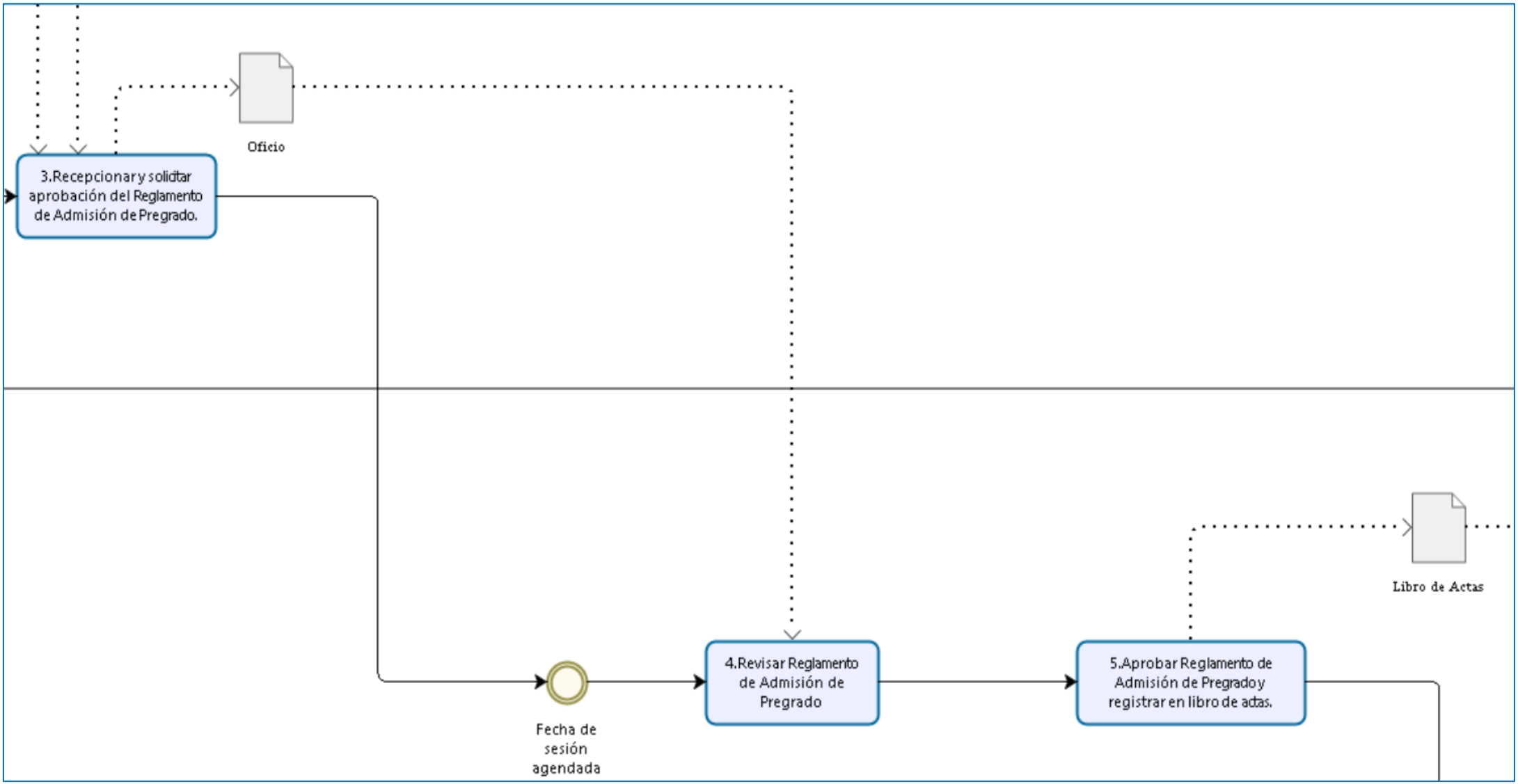


Figura N° 23: PM01.01.01.03 (Parte 3) - Diagrama BPMN 2.0

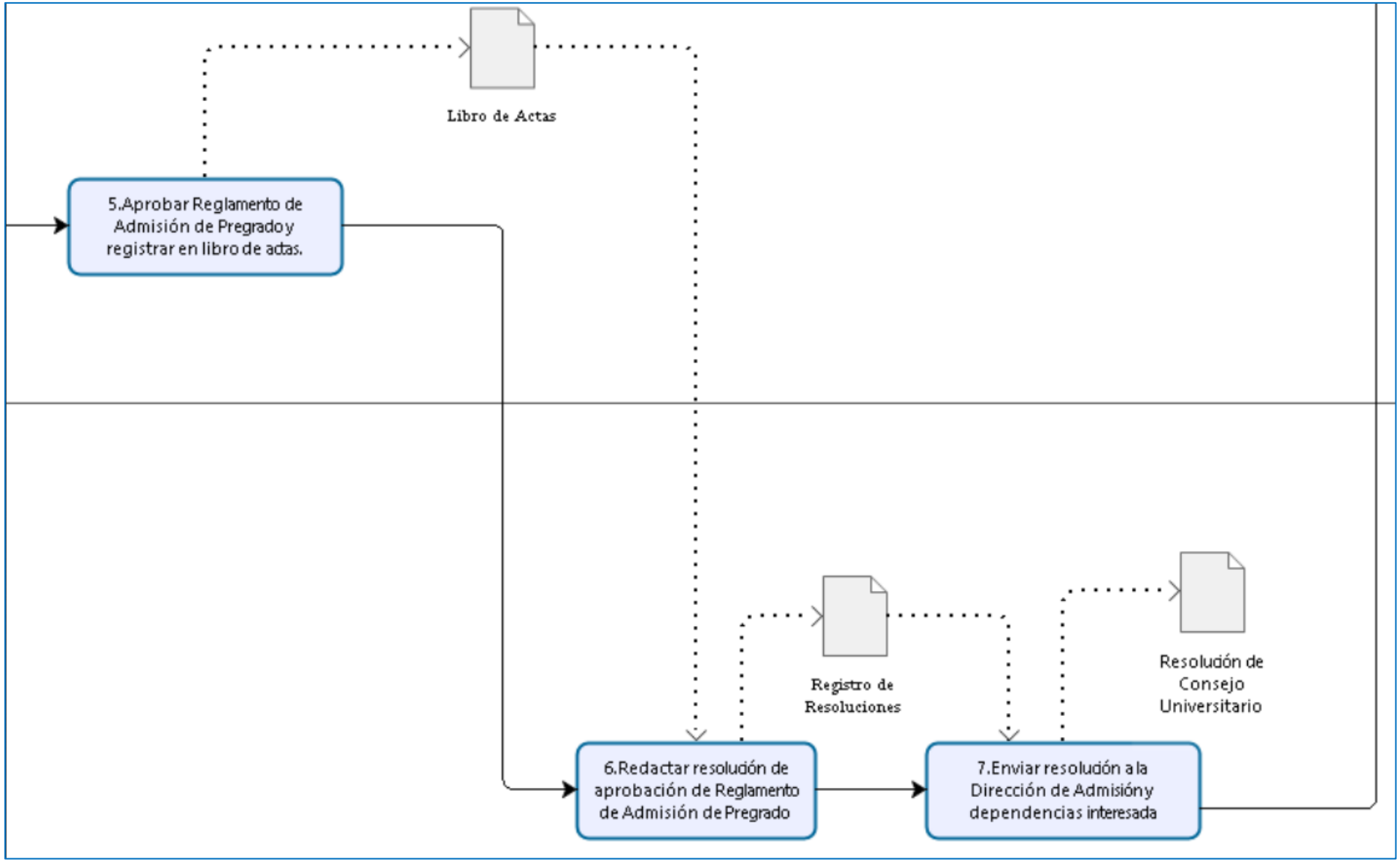


Figura N° 24: PM01.01.01.03 (Parte 4) - Diagrama BPMN 2.0

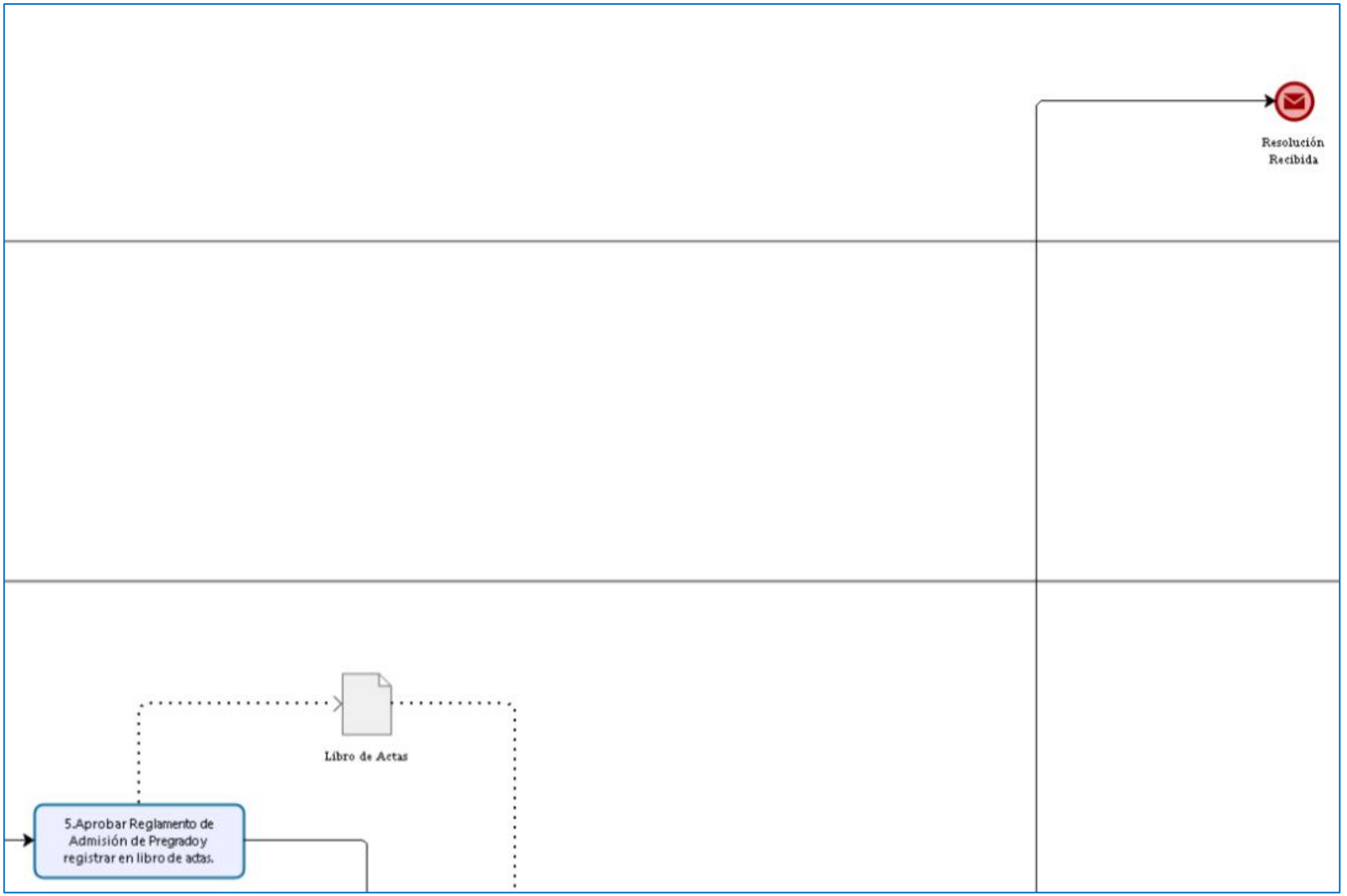


Tabla N° 11: PM01.01.01.04- Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.01.04
			Versión: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.01.Planificación del Proceso de Admisión de Pregrado
TÍTULO:	Elaboración del Prospecto de Admisión		
A. OBJETIVO:	Elaborar Prospecto de Admisión		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Revisar y actualizar cuadro de vacantes de carrera profesional por modalidad.		Dirección de Admisión	Director(a) de Admisión	Resolución de Consejo Universitario, Cuadro de Vacantes
2	Solicitar Perfil del Ingresante y Perfil del Egresado por Carrera profesional.		Dirección de Admisión	Director(a) de Admisión	Oficio
3	Recepcionar solicitud y remitir Perfil del Ingresante, Perfil del Egresado por Carrera profesional.		Dirección de Escuela	Director(a) de Escuela	Oficio
4	Recepcionar información y solicitar reunión con Directores de Escuela.		Dirección de Admisión	Director(a) de Admisión	Oficio
5	Realizar reunión para analizar cuadro de vacantes, Perfil del Ingresante, Perfil del Egresado.		Dirección de Admisión	Director(a) de Admisión	Actas
6	Consolidar cuadro de vacantes, Perfil del Ingresante, Perfil del Egresado y Reglamento de Admisión de Pregrado en un archivo.		Dirección de Admisión	Director(a) de Admisión	
7	Remitir solicitud de elaboración de prospecto de admisión y archivo vía correo electrónico.		Dirección de Admisión	Director(a) de Admisión	Oficio, Registro de Correo Electrónico
8	Revisar correo electrónico, descargar archivo y elaborar propuesta de prospecto de admisión.		Dirección de Imagen	Personal de la Dirección de Imagen	Registro de Correo Electrónico

9	Remitir oficio y archivo de prospecto de admisión vía correo electrónico.		Dirección de Imagen	Personal de la Dirección de Imagen	Oficio, Registro de Correo Electrónico
10	Revisar correo electrónico, descargar y verificar archivo de prospecto de admisión.		Dirección de Admisión	Director(a) de Admisión	Registro de Correo Electrónico
	Se cuenta con observaciones continuar, caso contrario ir al paso 12.		Dirección de Admisión	Director(a) de Admisión	
11	Retornar archivo de prospecto de admisión vía correo electrónico, ir al paso 8.		Dirección de Admisión	Director(a) de Admisión	Registro de Correo Electrónico
12	Solicitar vía orden de servicio para la impresión del archivo del prospecto de admisión mediante el aplicativo SIGA MEF para su distribución.		Dirección de Admisión	Director(a) de Admisión	Oficio, Registro de Orden de Servicio
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 25: PM01.01.01.04 (General) - Diagrama BPMN 2.0

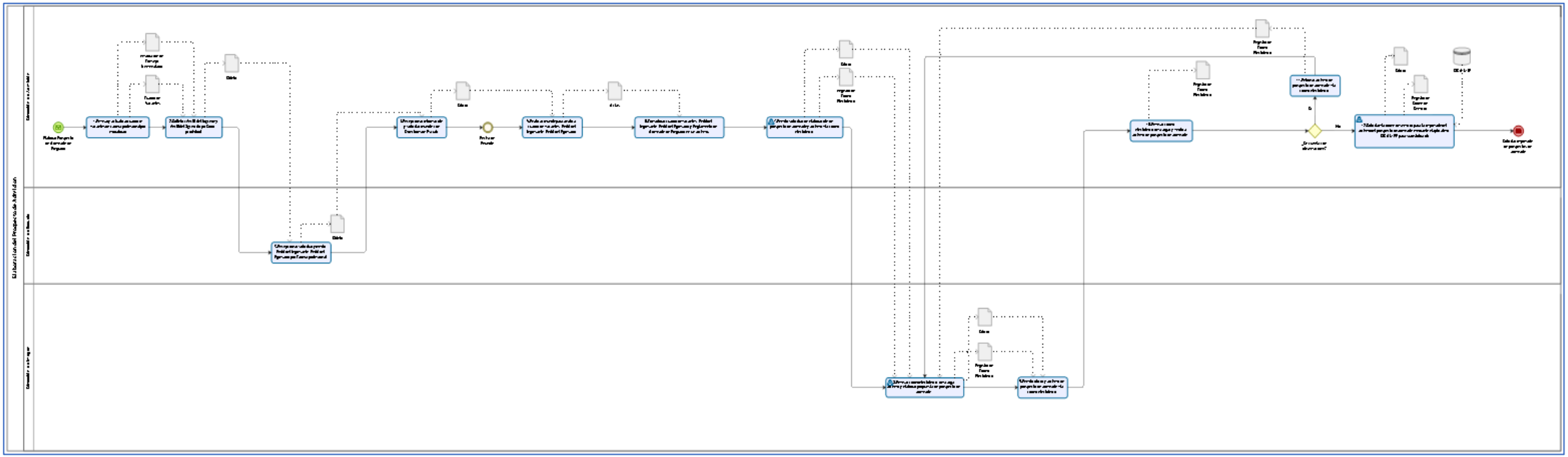


Figura N° 26: PM01.01.01.04 (Parte 1) - Diagrama BPMN 2.0

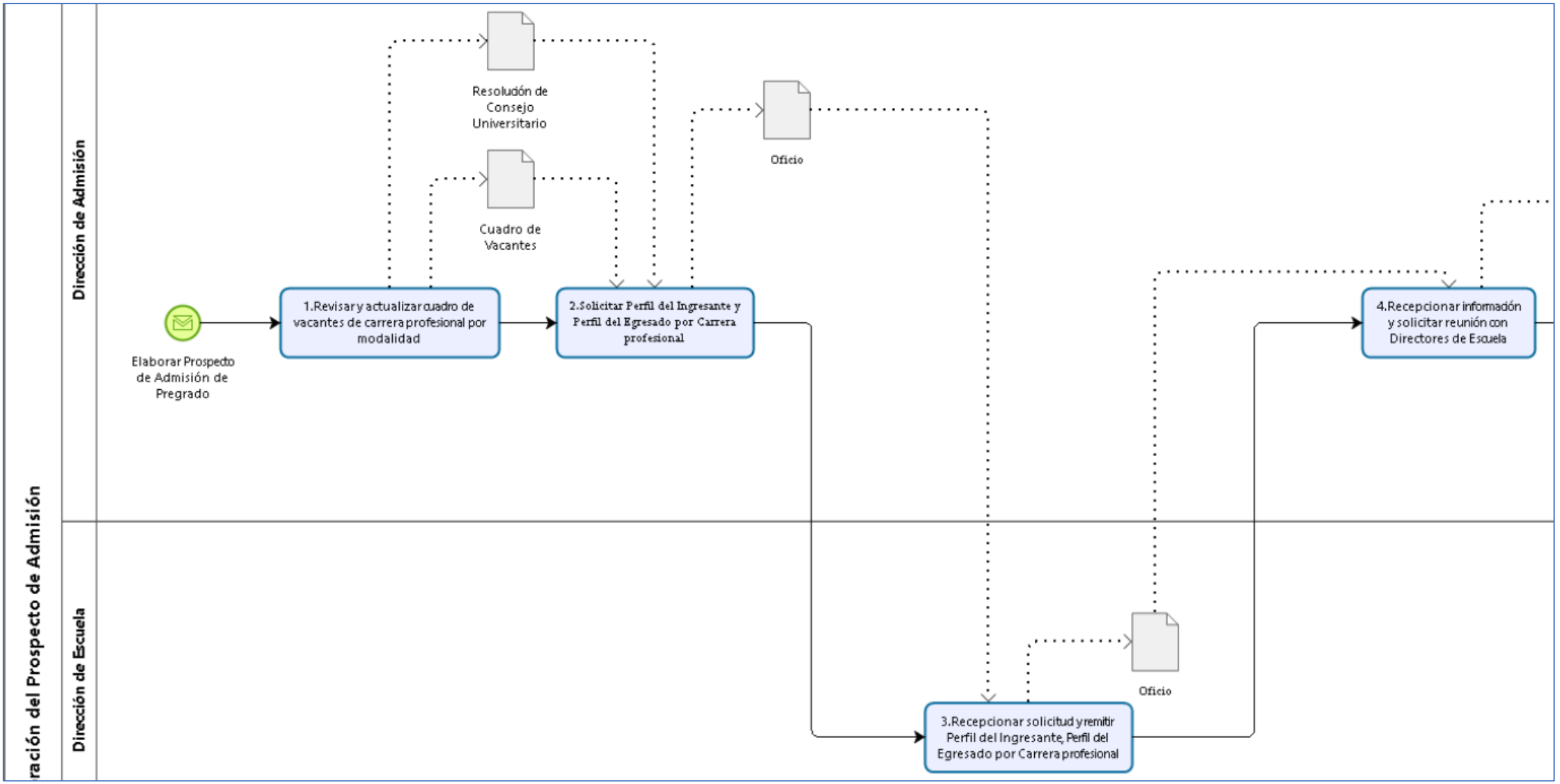


Figura N° 27: PM01.01.01.04 (Parte 2) - Diagrama BPMN 2.0

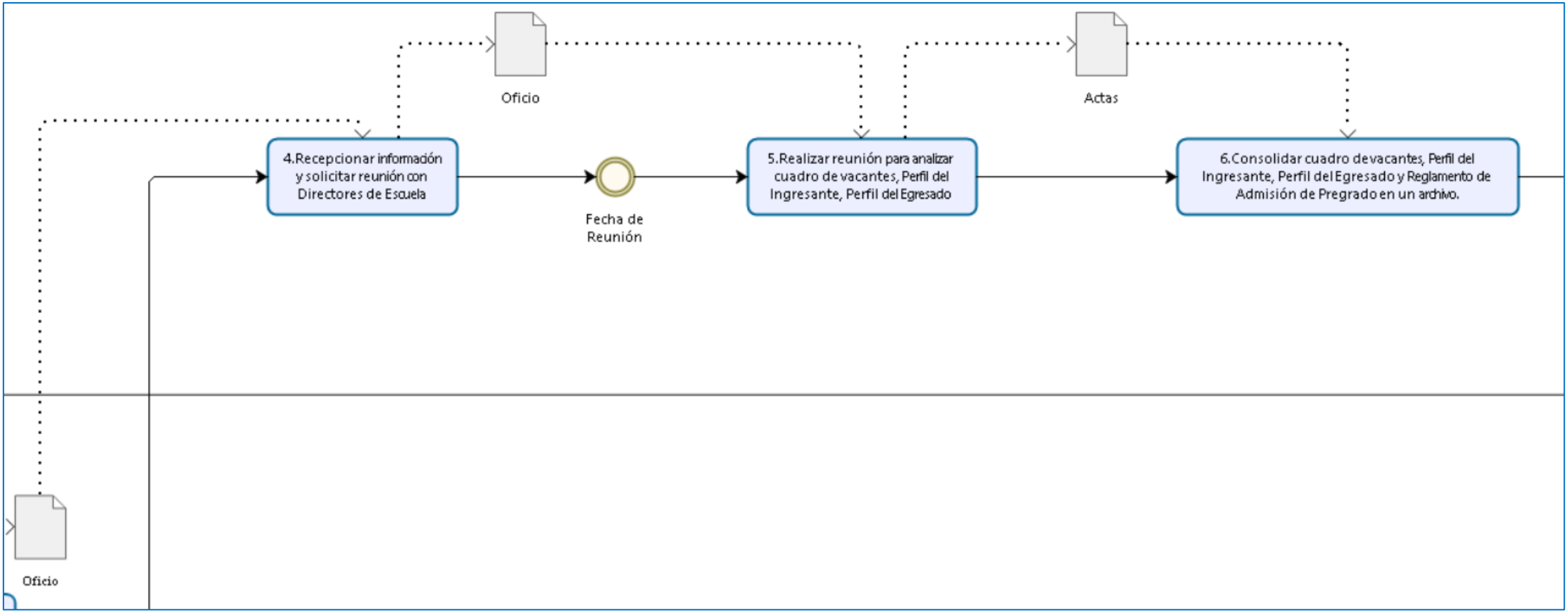


Figura N° 28: PM01.01.01.04 (Parte 3) - Diagrama BPMN 2.0

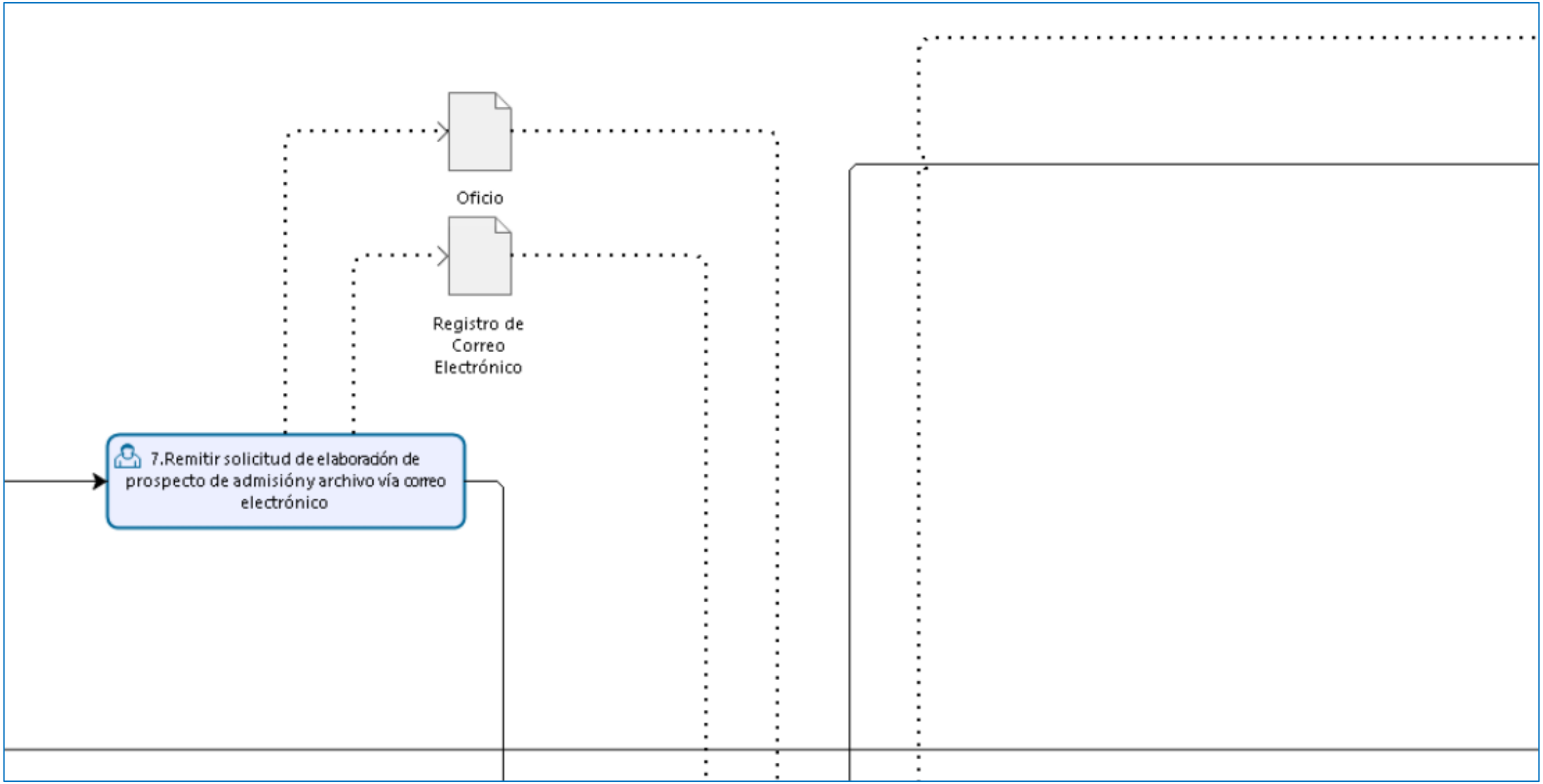


Figura N° 29: PM01.01.01.04 (Parte 4) - Diagrama BPMN 2.0

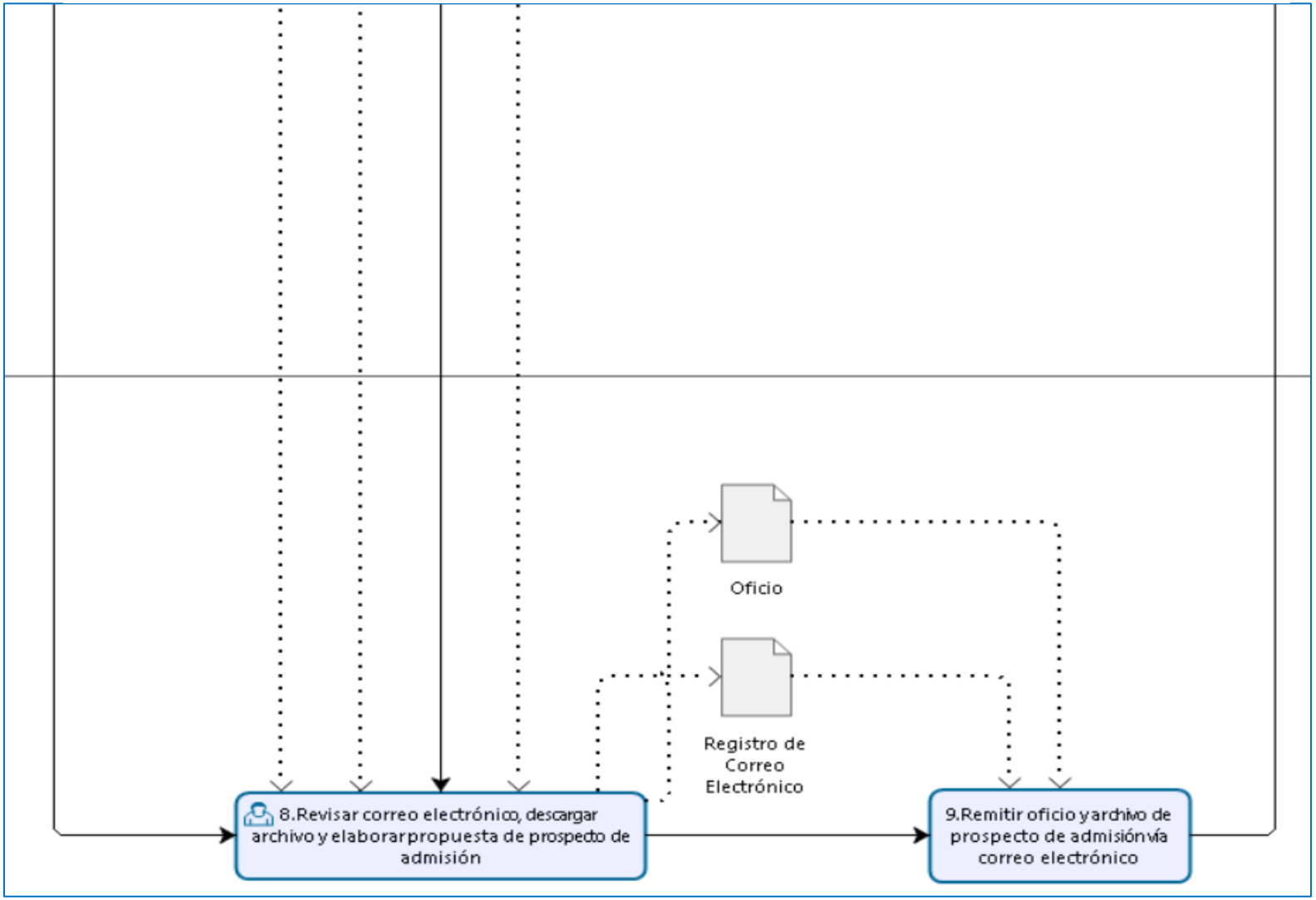


Figura N° 30: PM01.01.01.04 (Parte 5) - Diagrama BPMN 2.0

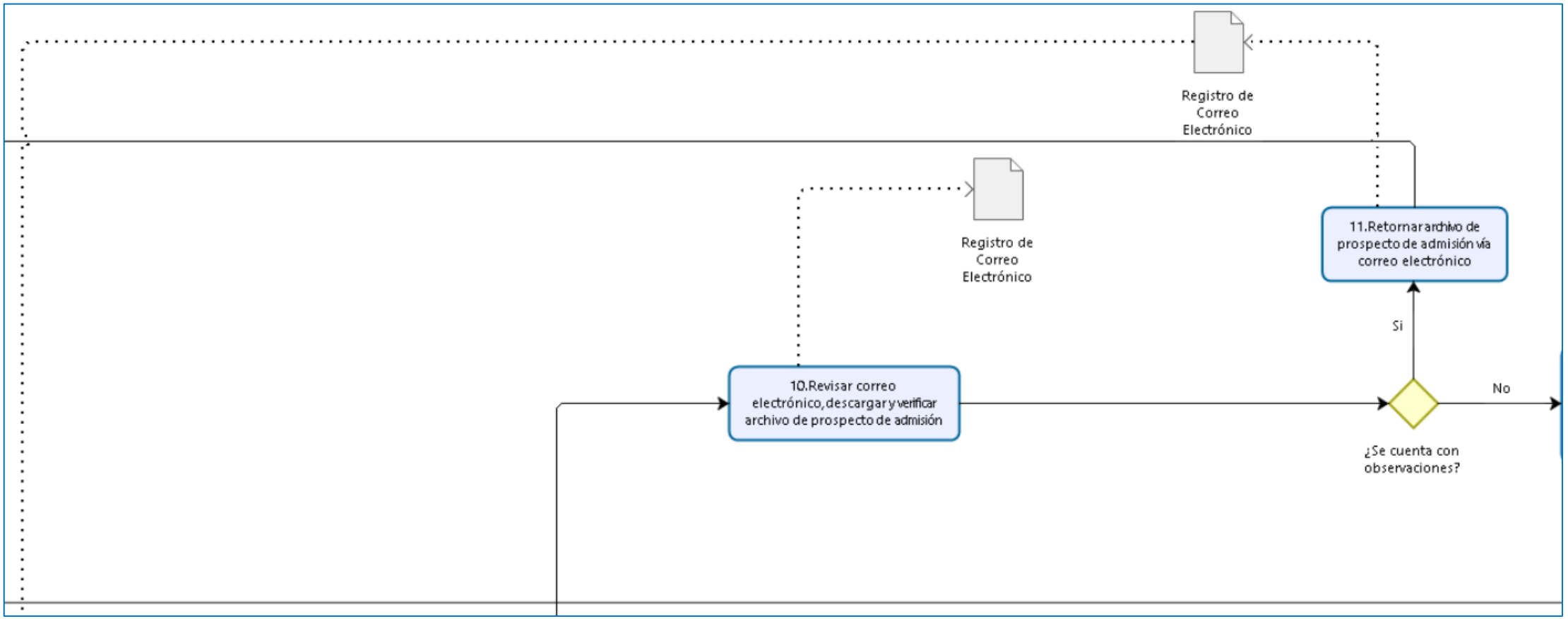


Figura N° 31: PM01.01.01.04 (Parte 6) - Diagrama BPMN 2.0

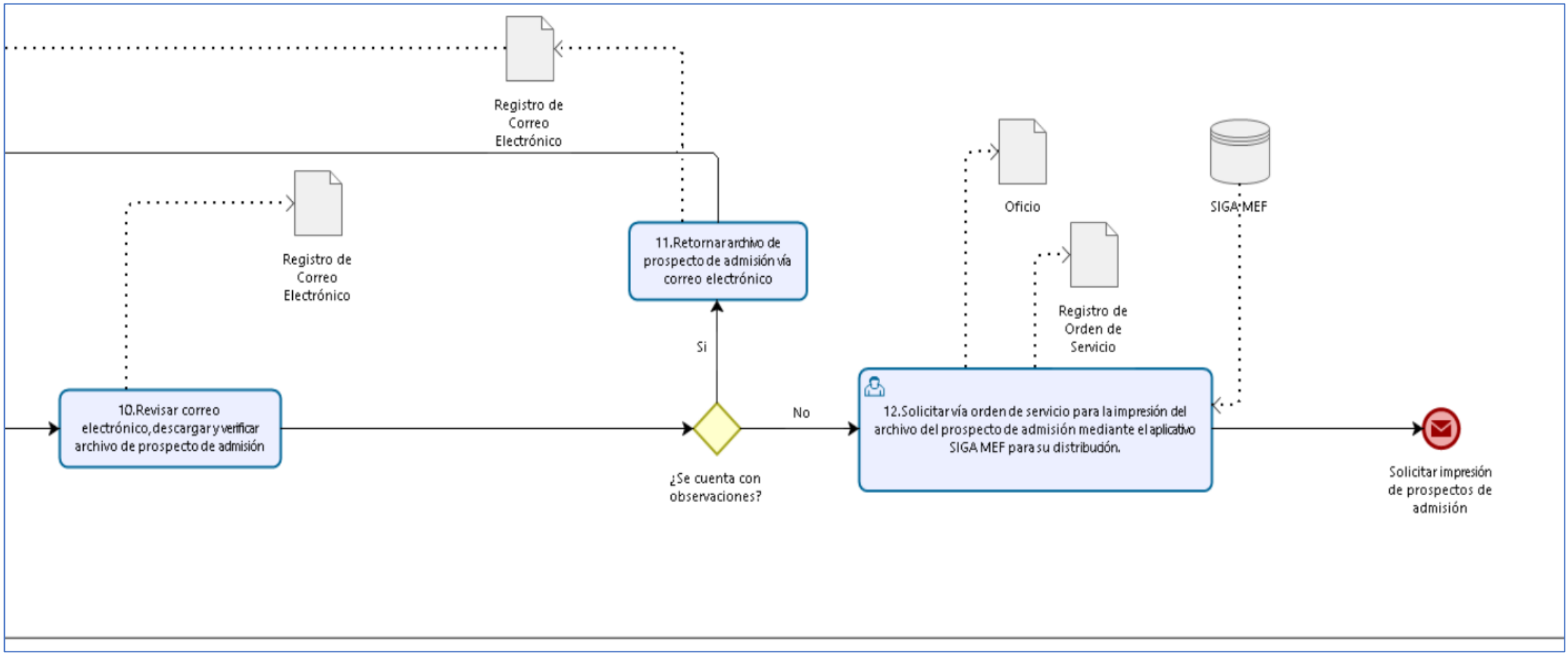


Tabla N° 12: PM01.01.02 - Ficha de Proceso

<table>
<tr><td colspan="2"></td><td colspan="3">FICHA DE PROCESO DE NIVEL 2</td><td colspan="2">Código: PM01.01.02
Versión: 1.0</td></tr>
<tr><td colspan="7">I. DATOS GENERALES DEL PROCESO</td></tr>
<tr><td>1. NOMBRE DEL PROCESO</td><td colspan="2">Difusión del Proceso de Admisión de Pregrado</td><td>2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR</td><td colspan="3">Proceso de Admisión de Programas de Pregrado</td></tr>
<tr><td>2. OBJETIVO DEL PROCESO</td><td colspan="6">Difundir las carreras profesionales de pregrado la comunidad local y nacional.</td></tr>
<tr><td rowspan="2">4. DUEÑO DEL PROCESO</td><td rowspan="2">Director de Admisión</td><td rowspan="2">5. LÍMITES DEL PROCESO</td><td>INICIO</td><td colspan="3">Convocatoria a los Directores de Escuela de las Carreras Profesionales de Pregrado</td></tr>
<tr><td>FIN</td><td colspan="3">Culmina con la presentación del informe de difusión del proceso de admisión de pregrado</td></tr>
<tr><td colspan="7">II. DESCRIPCIÓN DEL PROCESO</td></tr>
<tr><td>6. PROVEEDORES</td><td>7. INSUMOS</td><td colspan="2">8. PROCESOS DE NIVEL INFERIOR</td><td>9. CONTROLES APLICADOS</td><td>10. PRODUCTOS</td><td>11. CLIENTES</td></tr>
<tr><td>Dirección de Escuela</td><td>Currículo de las Carreras Profesionales

Plan de Difusión de Carreras Profesionales</td><td colspan="2">PM01.01.02.01.Convocatoria y reunión con Directores de Escuela</td><td>Se realiza reuniones para determinar estrategias para publicitar las carreras profesionales</td><td>Plan de Difusión por Carrera Profesional

Actas</td><td>Dirección de Admisión

Dirección de Escuela</td></tr>
<tr><td rowspan="2">Dirección de Admisión</td><td>Solicitud con descripción del spot publicitario</td><td colspan="2" rowspan="2">PM01.01.02.02.Elaboración y realización de publicidad</td><td>Se realiza reuniones para revisar el spot elaborado por la Dirección de Imagen y solicitar orden de servicio para contratar su proyección en los medios televisivos</td><td>Spot Publicitario</td><td>Dirección de Admisión

Dirección de Imagen

Dirección General de Administración

Oficina de Abastecimiento

Medio Televisivos</td></tr>
<tr><td>Solicitud para la adquisición de souvenirs</td><td>Se realiza coordinación con el proveedor encargado de la confección y compra de souvenirs</td><td>Souvenirs</td><td>Dirección de Admisión

Dirección General de Administración

Oficina de Abastecimiento</td></tr>
<tr><td>Dirección de Admisión</td><td>Solicitud de publicación del cronograma, requisitos y enlace del módulo web de inscripción</td><td colspan="2">PM01.01.02.03.Publicación de cronograma del proceso de admisión</td><td>Se realiza coordinación con la Dirección de Imagen para la publicación en el portal web institucional</td><td>Requisitos y Cronograma de Admisión en la Web

Vínculo del Módulo Web de Admisión en el Portal</td><td>Dirección de Admisión

Postulantes</td></tr>
<tr><td>Dirección de Admisión</td><td>Registro de Visitas programadas</td><td colspan="2">PM01.01.02.04.Realización de visitas locales y regionales</td><td>Se realiza visitas programadas a las instituciones educativas representativas</td><td>Registros fotográficos y audiovisuales

Actas</td><td>Dirección de Admisión

Dirección de Imagen</td></tr>
</table>

			de la localidad y la región		
Dirección de Admisión	Registros fotográficos y audiovisuales Actas	**PM01.01.02.05.Elaboración y Presentación de Informe de Difusión**	Se elabora el informe de difusión y se envía para verificación de Vicerrectorado Académico	Informe de Difusión verificado	Dirección de Admisión Vicerrectorado Académico

III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO	
12. TIPO	**13. DESCRIPCIÓN**
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica,1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas, 2 Recepcionistas, 1 Especialista de Dirección de Imagen.
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).
	Material: Material de Oficina

IV. DOCUMENTACIÓN DEL PROCESO	
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**
1. Actas de Reuniones	1. Ley Universitaria 30220
2. Registro de solicitudes de compra	2. Estatuto
3. Registros fotográficos y audiovisuales	3. Reglamento General
	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento para Pago de Subvenciones al Personal
	8. Reglamento de Admisión

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 32: PM01.01.02 (General) - Diagrama BPMN 2.0

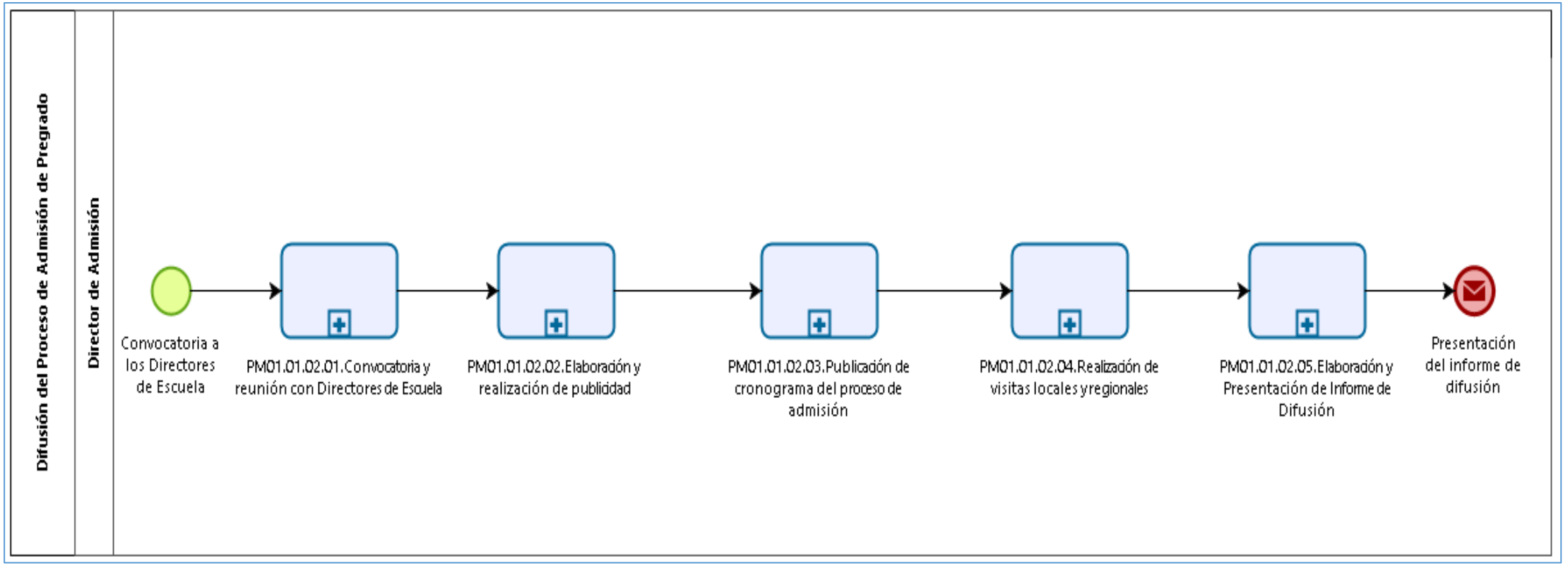


Figura N° 33: PM01.01.02 (Parte 1) - Diagrama BPMN 2.0

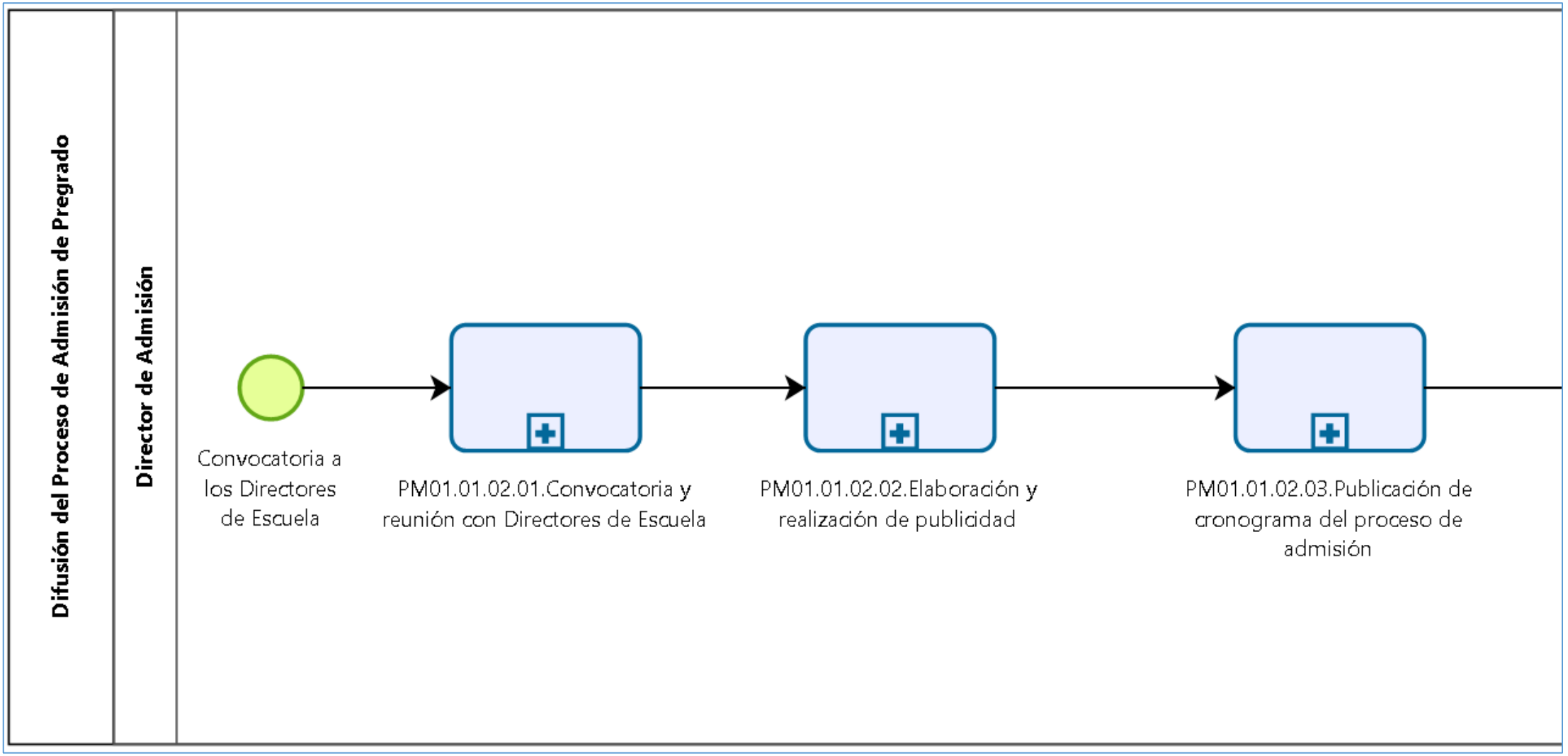


Figura N° 34: PM01.01.02 (Parte 2) - Diagrama BPMN 2.0

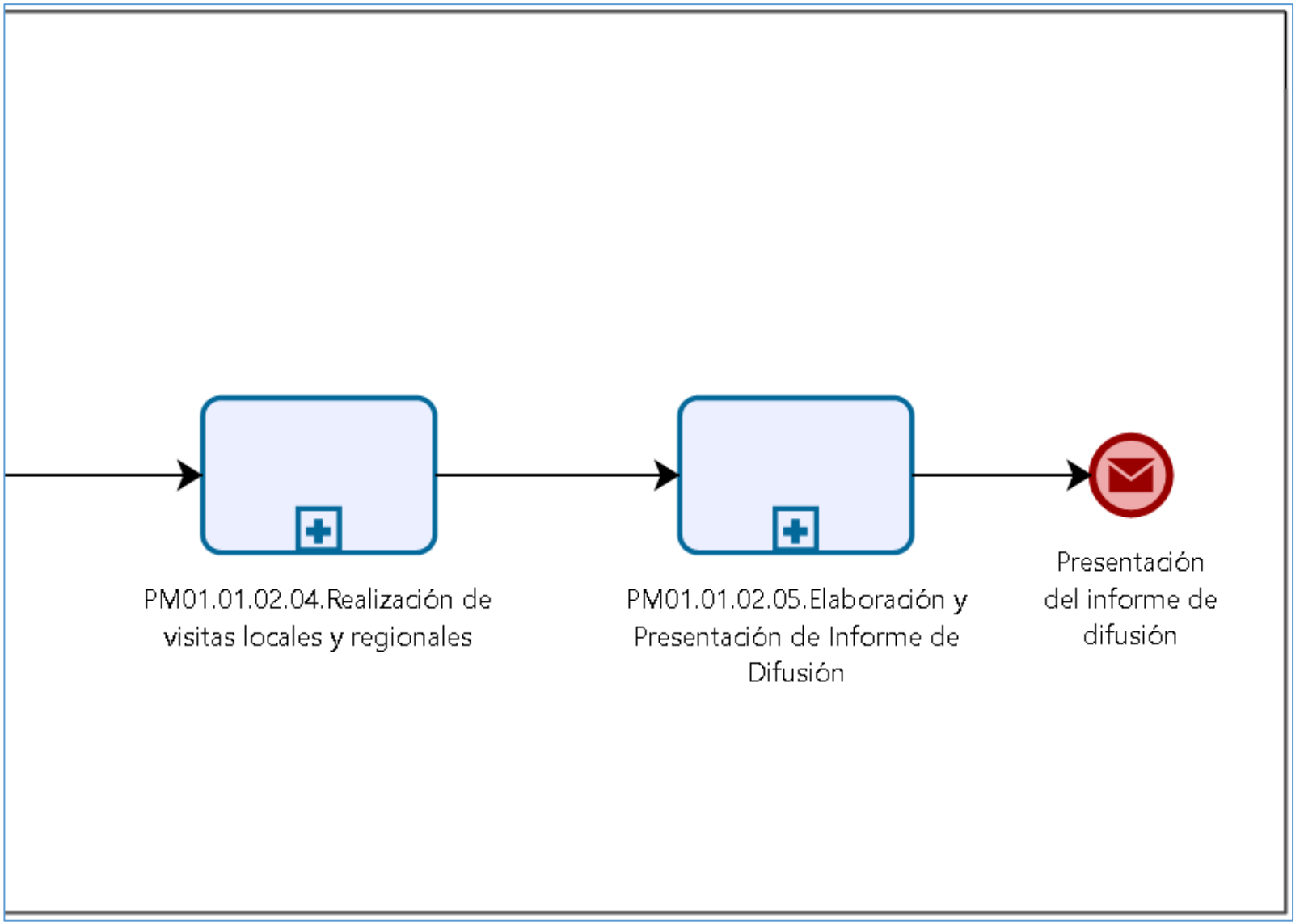


Tabla N° 13: PM01.01.02.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.02.01
			Versión: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.02.Difusión del Proceso de Admisión de Pregrado
TÍTULO:	Convocatoria y reunión con Directores de Escuela		
A. OBJETIVO:	Convocar a los Directores de Escuela para las actividades de difusión de las carreras profesionales de pregrado		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Solicitar reunión con los directores de escuela para planificar las actividades de difusión.		Dirección de Admisión	Director(a) de Admisión	Oficio
2	Realizar reunión con Directores de Escuela y determinar actividades.		Dirección de Admisión	Director(a) de Admisión	Actas
3	Elaborar cronograma de actividades de difusión.		Dirección de Admisión	Director(a) de Admisión	Cronograma de actividades de difusión
4	Remitir cronograma de actividades de difusión a los Directores de Escuela.		Dirección de Admisión	Director(a) de Admisión	Oficio, Cronograma de actividades de difusión
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Aprobado por:			
Cargo:			

Figura N° 35 : PM01.01.02.01 (General) - Diagrama BPMN 2.0

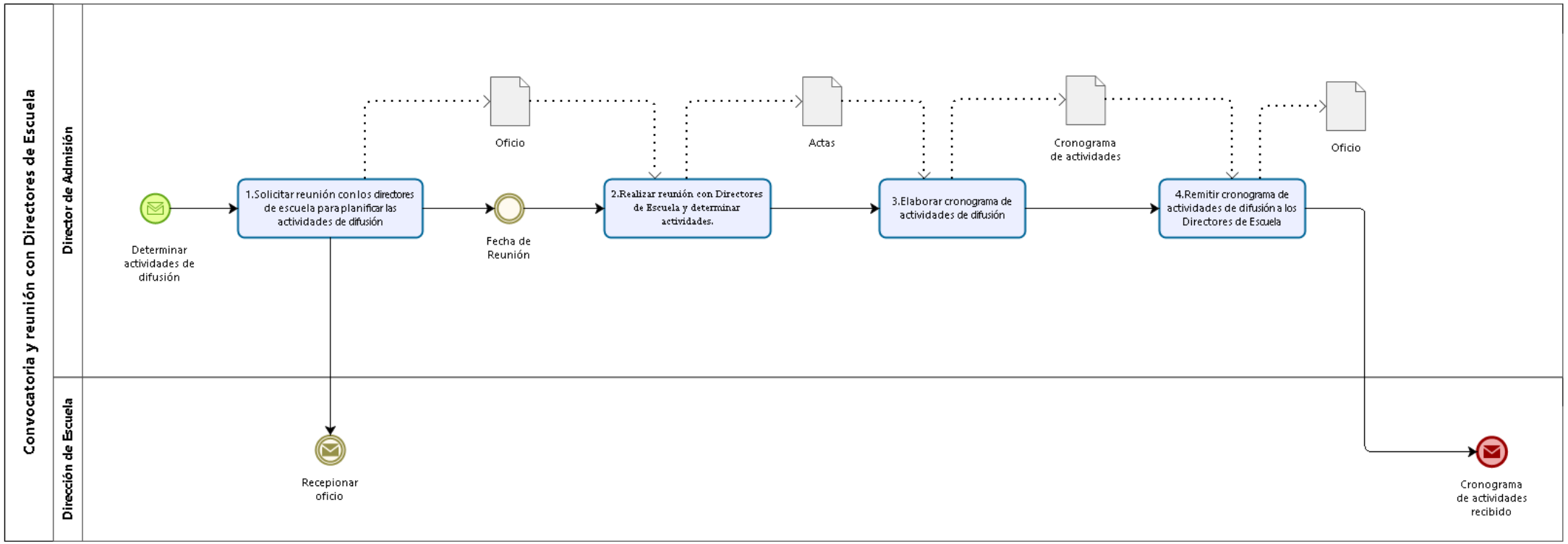


Figura N° 36: PM01.01.02.01 (Parte 1) - Diagrama BPMN 2.0

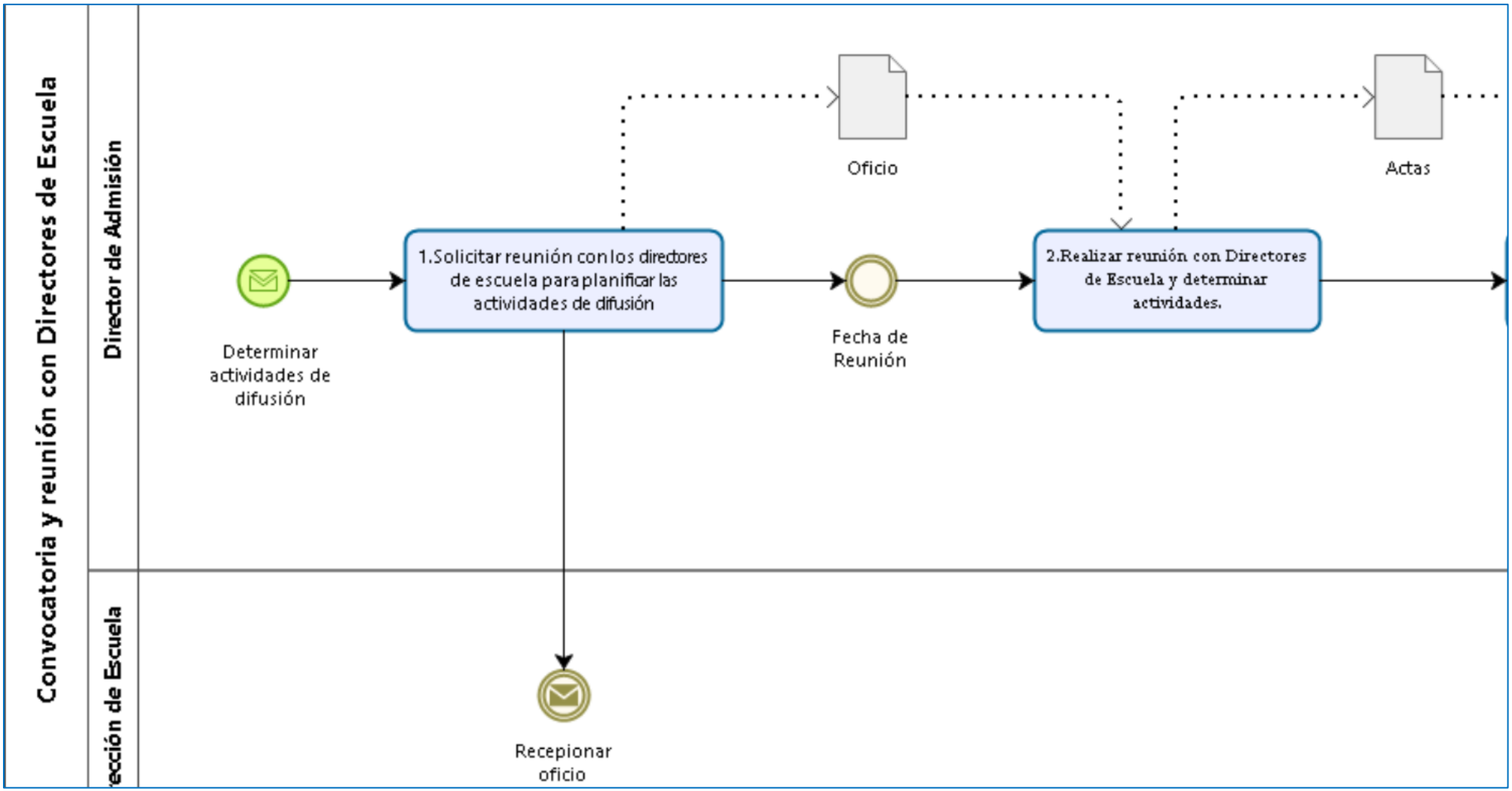


Figura N° 37: PM01.01.02.01 (Parte 2) - Diagrama BPMN 2.0

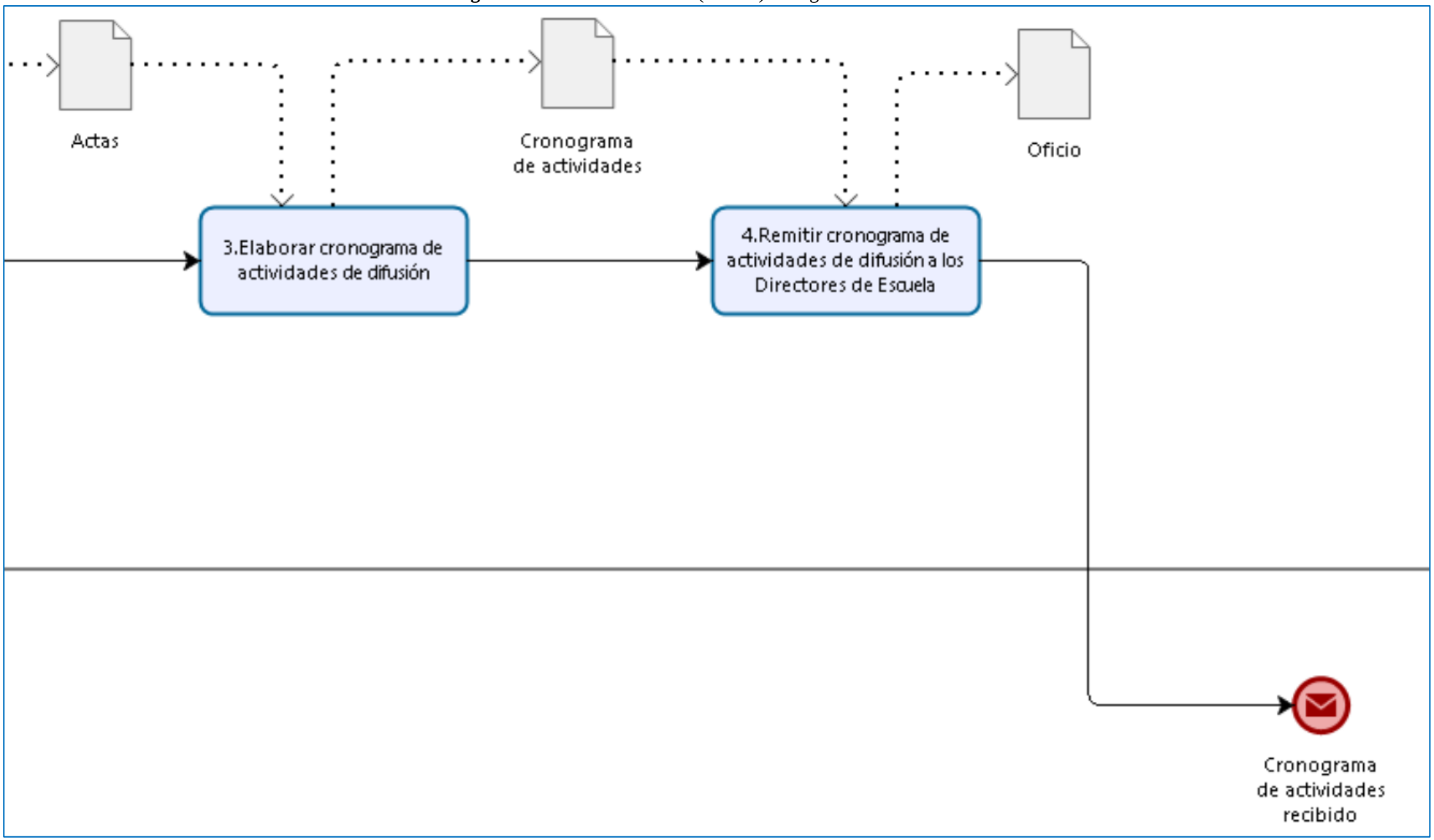


Tabla N° 14: PM01.01.02.02 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO			**Código**: PM01.01.02.02 **Versión**: 1.0	
TIPO:	PROCEDIMIENTO		**PROCESO DE NIVEL SUPERIOR:**	PM01.01.02.Difusión del Proceso de Admisión de Pregrado	
TÍTULO:	Elaboración y realización de publicidad				
A. OBJETIVO:	Elaborar la publicidad del proceso de admisión de pregrado.				
B. UNIDAD RESPONSABLE:	Dirección de Admisión				
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.				
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.				
E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Remitir solicitud de elaboración de spot publicitario y realizar envío de información vía correo electrónico.		Dirección de Admisión	Director(a) de Admisión	Oficio, Registro de Correo Electrónico
2	Revisar correo electrónico, descargar archivo y elaborar propuesta de spot publicitario.		Dirección de Imagen	Personal de la Dirección de Imagen	Registro de Correo Electrónico
3	Remitir oficio y archivo de spot publicitario vía correo electrónico.		Dirección de Imagen	Personal de la Dirección de Imagen	Oficio, Registro de Correo Electrónico
4	Revisar correo electrónico, descargar y verificar archivo de spot publicitario.		Dirección de Admisión	Director(a) de Admisión	Registro de Correo Electrónico
	Se cuenta con observaciones continuar, caso contrario ir al paso 7.		Dirección de Admisión	Director(a) de Admisión	
5	Solicitar cambios de archivo de spot publicitario, ir al paso 2.		Dirección de Admisión	Director(a) de Admisión	Registro de Correo Electrónico
6	Solicitar orden de servicio para el contrato de medios televisivos mediante el aplicativo SIGA MEF.		Dirección de Admisión	Director(a) de Admisión	Oficio, Registro de Orden de Servicio
7	Solicitar orden de servicio para la confección de suvenires para la difusión del Proceso de Admisión mediante el aplicativo SIGA MEF.		Dirección de Admisión	Director(a) de Admisión	Oficio, Registro de Orden de Servicio
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 38: PM01.01.02.02 (General) - Diagrama BPMN 2.0

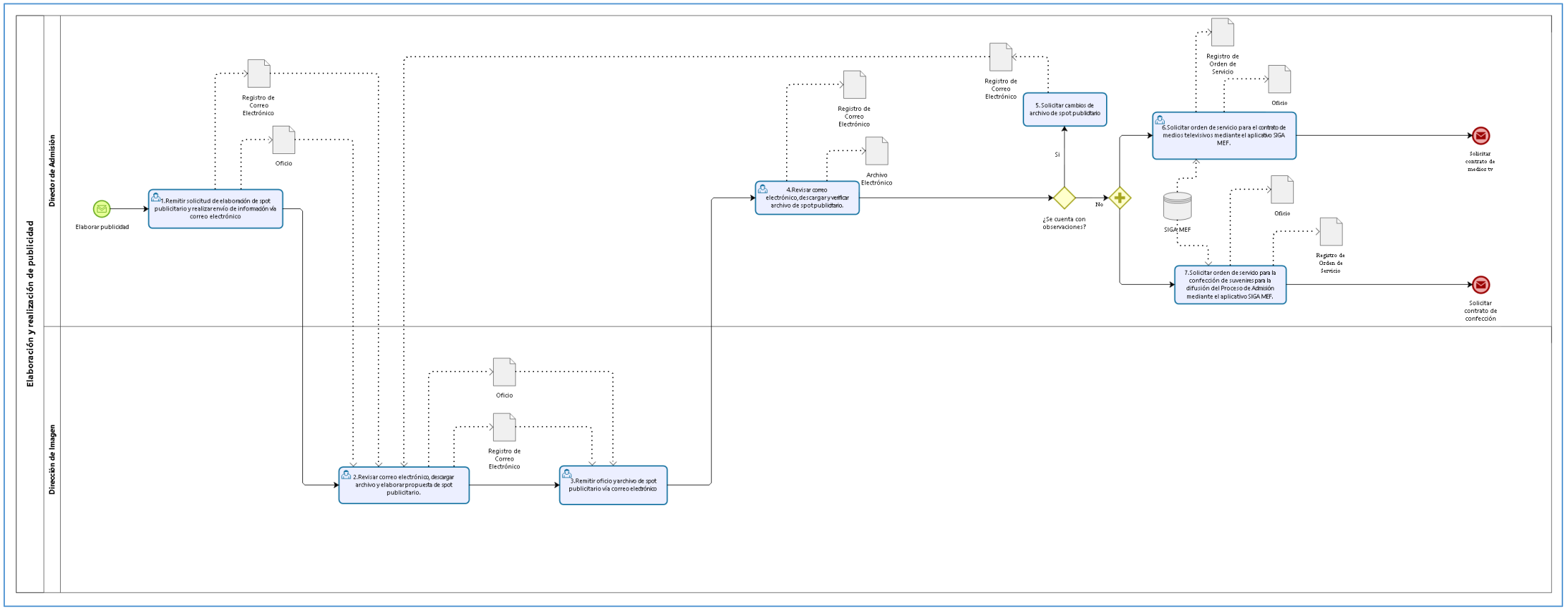


Figura N° 39: PM01.01.02.02 (Parte 1) - Diagrama BPMN 2.0

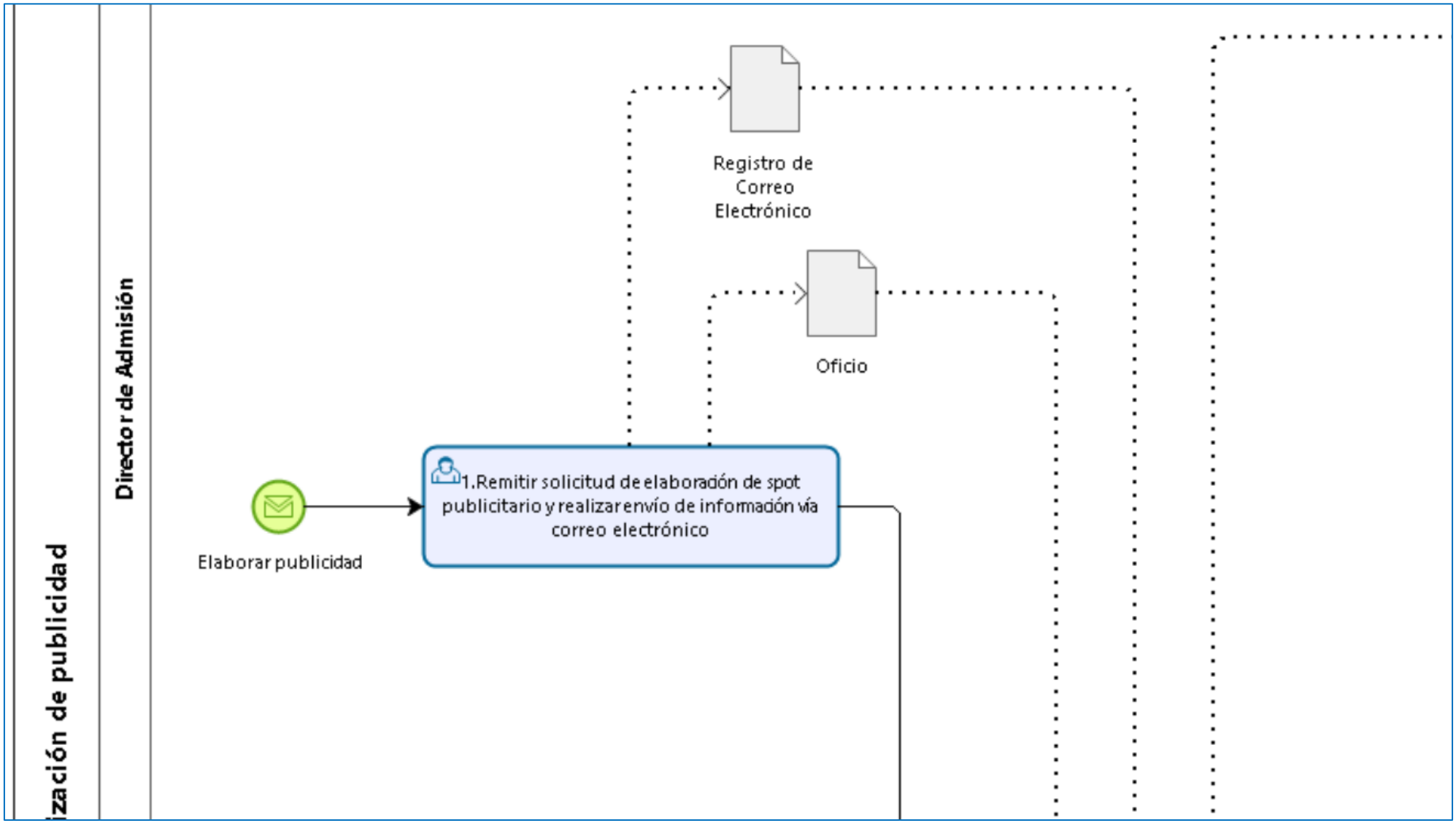


Figura N° 40: PM01.01.02.02 (Parte 2) - Diagrama BPMN 2.0

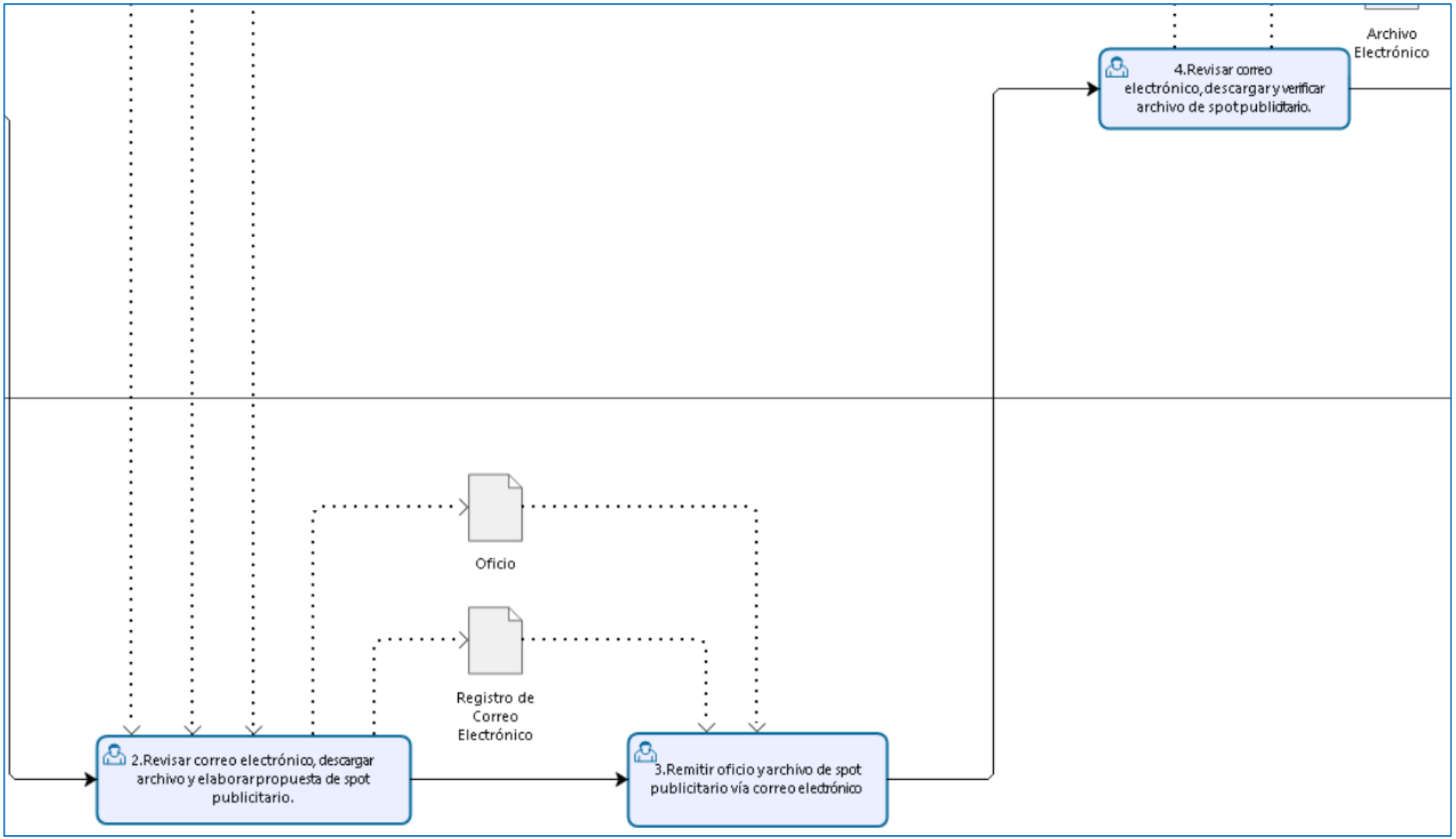


Figura N° 41: PM01.01.02.02 (Parte 3) - Diagrama BPMN 2.0

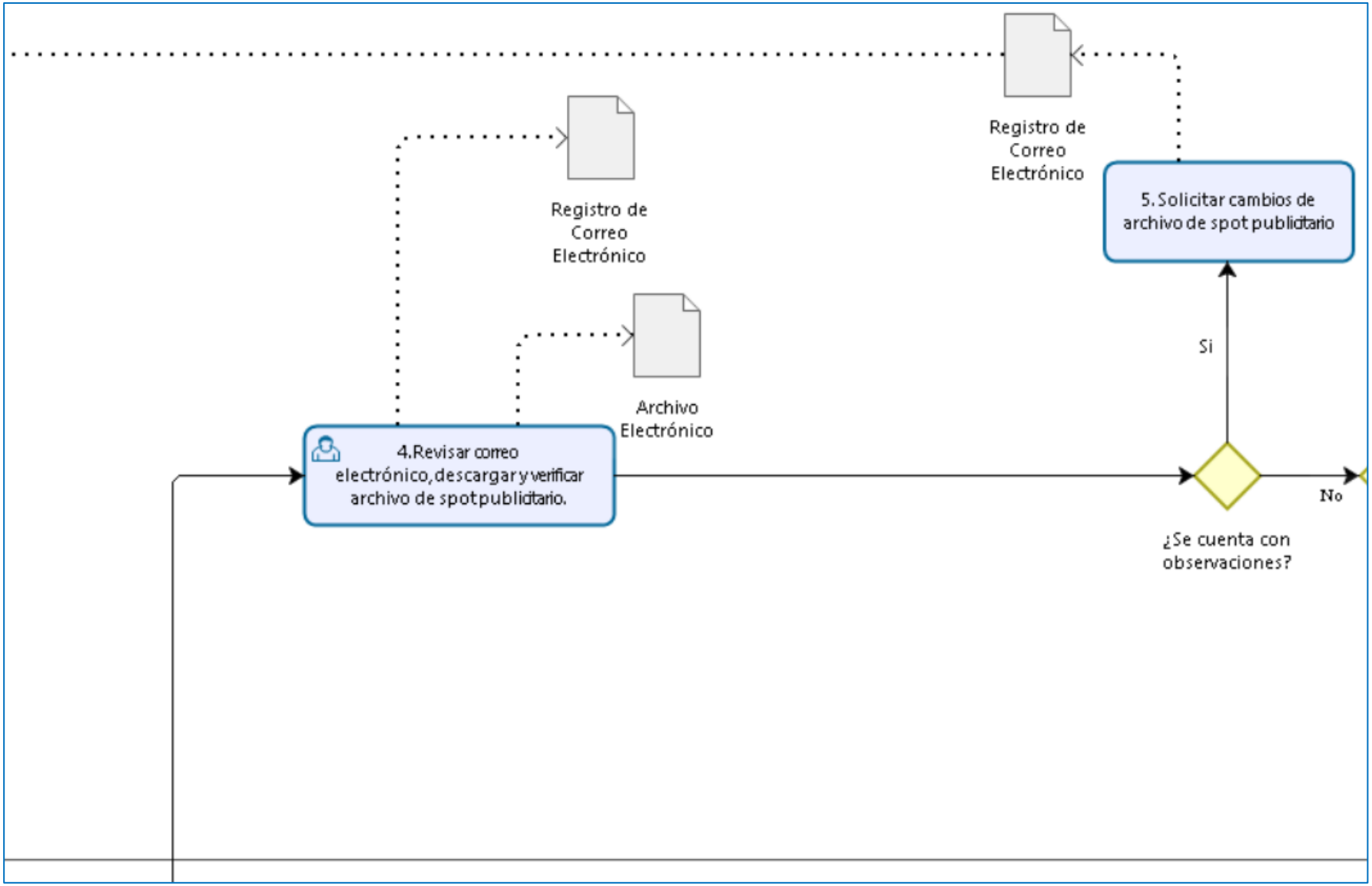


Figura N° 42: PM01.01.02.02 (Parte 4) - Diagrama BPMN 2.0

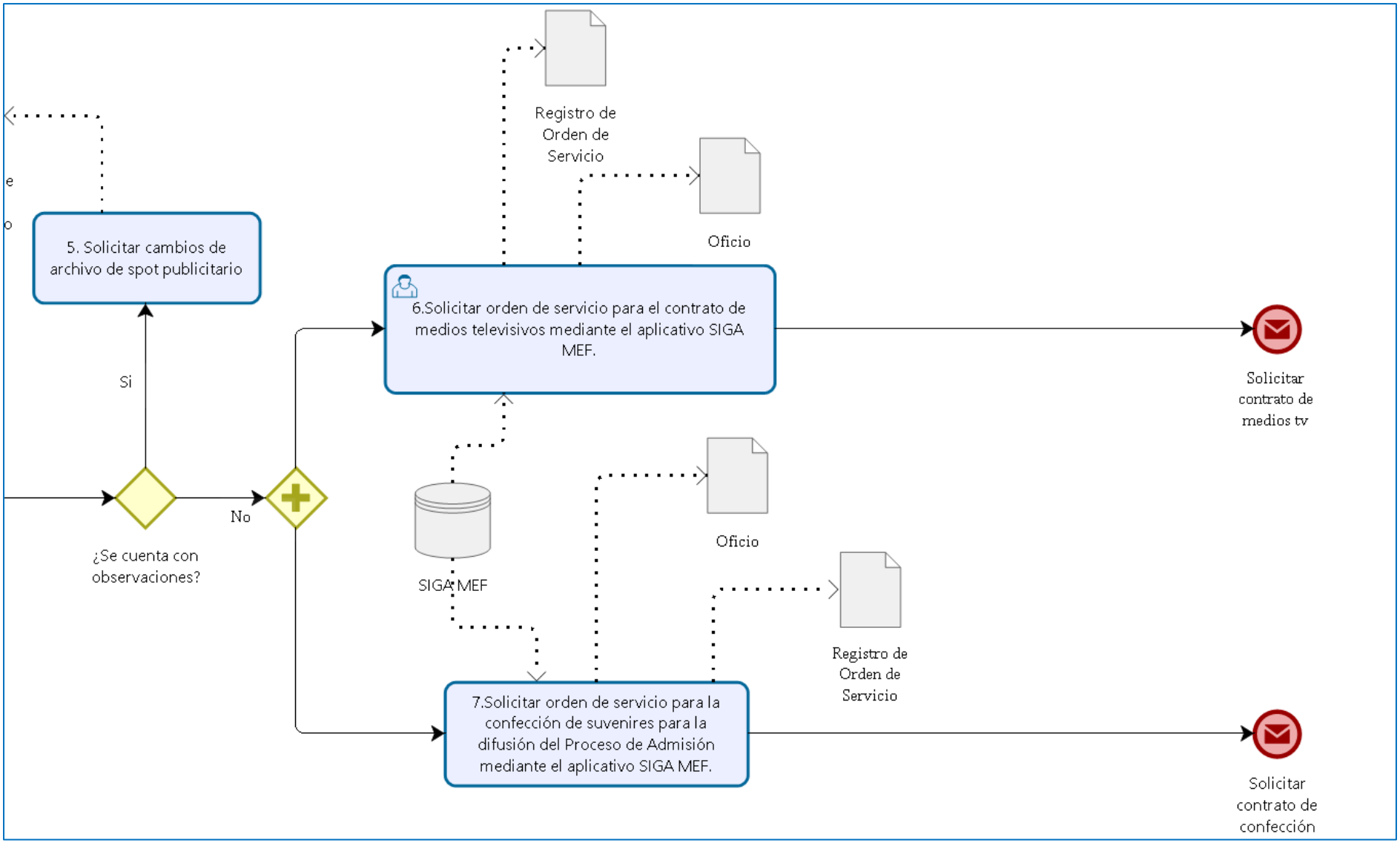


Tabla N° 15: PM01.01.02.03 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.02.03 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.02.Difusión del Proceso de Admisión de Pregrado
TÍTULO:	Publicación de cronograma del proceso de admisión		
A. OBJETIVO:	Publicar cronograma del proceso de admisión en el portal institucional		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Solicitar a la Dirección de Información y Documentación actualización en el sistema web del proceso de admisión.		Dirección de Admisión	Director(a) de Admisión	Oficio
2	Recepcionar oficio, realizar actualización y testeo de funcionalidades implementadas en el sistema web del proceso de admisión.		Dirección de Información y Documentación	Director de Información y Documentación	Oficio, Registro de control de cambios
3	Elaborar y remitir informe de cambios realizados en el sistema web del proceso de admisión.		Dirección de Información y Documentación	Director de Información y Documentación	Oficio
4	Verificar informe de cambios y realizar pruebas de funcionalidad.		Dirección de Admisión	Director(a) de Admisión	Oficio
5	Remitir solicitud de publicación del cronograma, prospecto y enlace del sistema web del proceso de admisión.		Dirección de Admisión	Director(a) de Admisión	Oficio
6	Recepcionar solicitud y realizar publicación del cronograma, prospecto y enlace del sistema web del proceso de admisión.		Dirección de Imagen	Personal de la Dirección de Imagen	Oficio, Registro del Portal Web Institucional
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 43: PM01.01.02.03 (General) - Diagrama BPMN 2.0

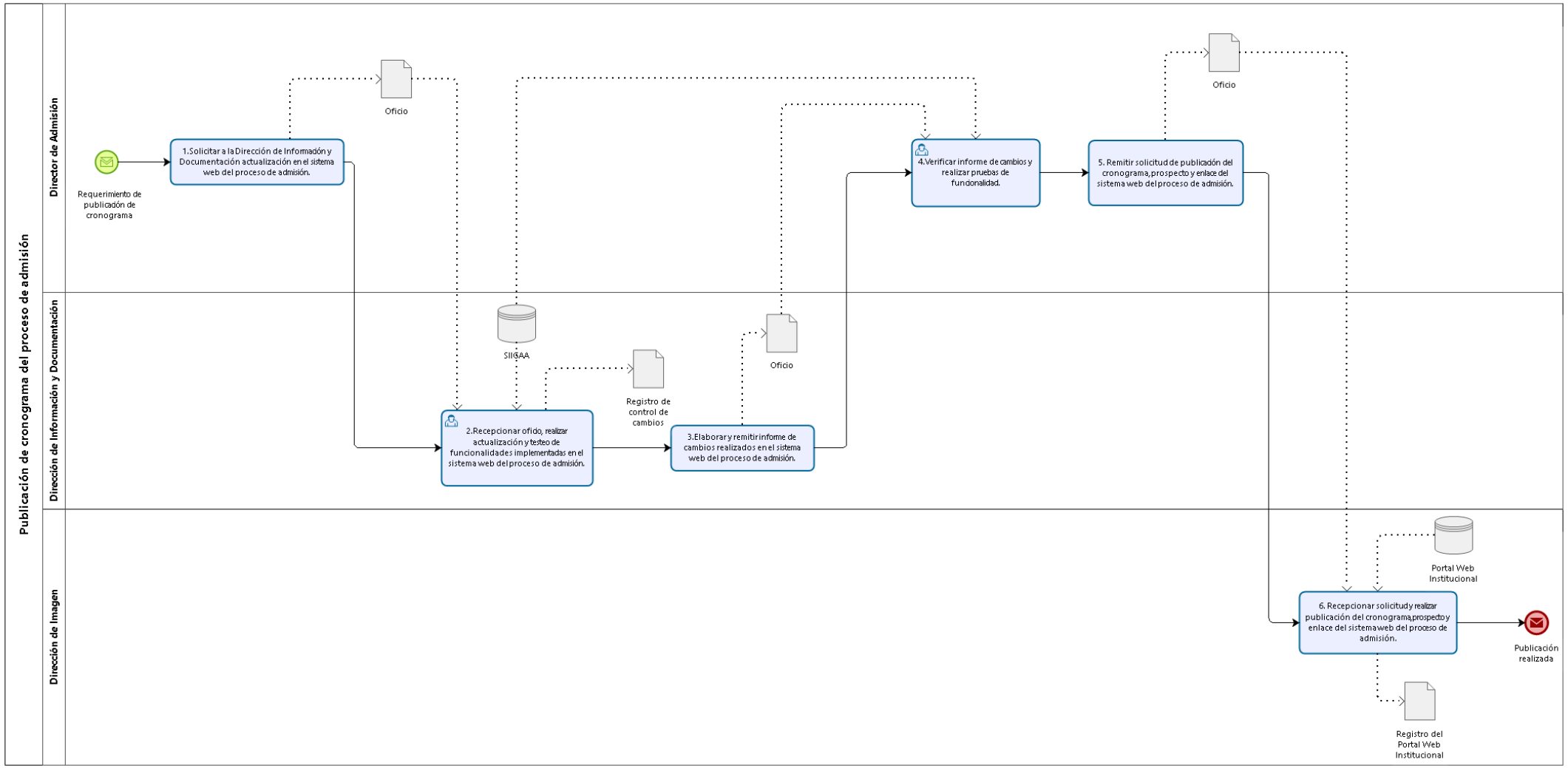


Figura N° 44: PM01.01.02.03 (Parte 1) - Diagrama BPMN 2.0

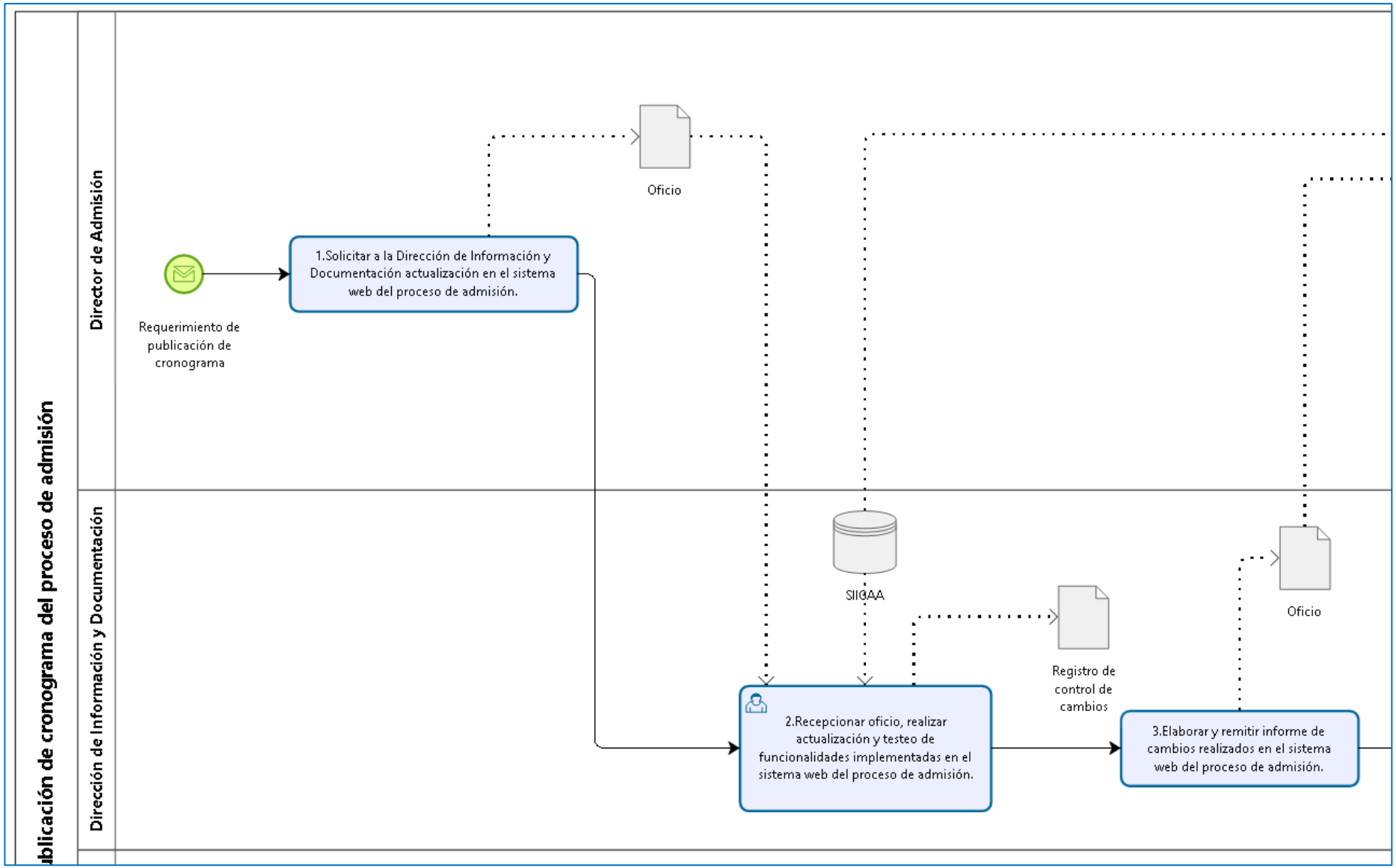


Figura N° 45: PM01.01.02.03 (Parte 2) - Diagrama BPMN 2.0

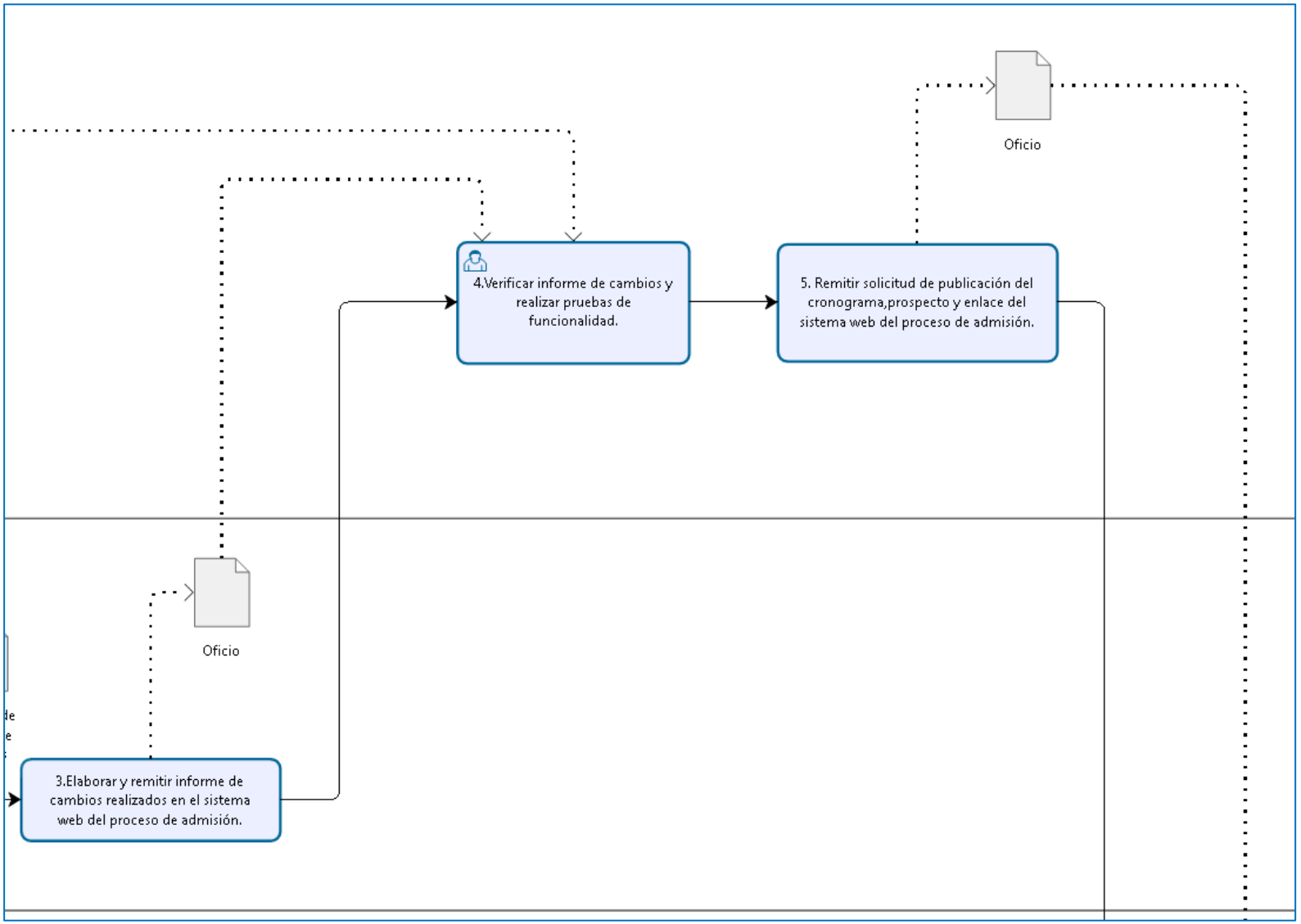


Figura N° 46: PM01.01.02.03 (Parte 3) - Diagrama BPMN 2.0

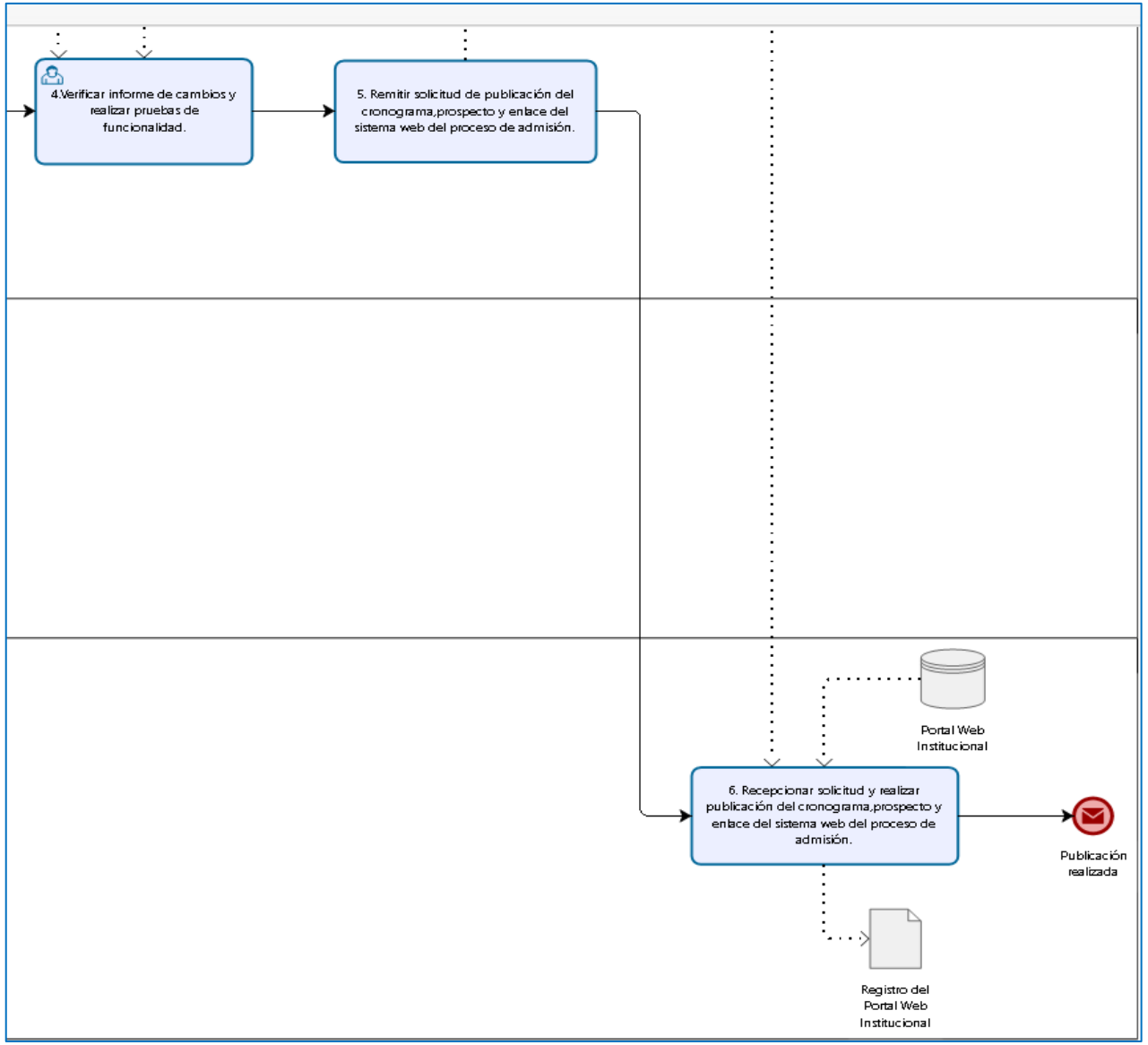


Tabla N° 16: PM01.01.02.04 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.02.04 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.02.Difusión del Proceso de Admisión de Pregrado
TÍTULO:	Realización de visitas locales y regionales		
A. OBJETIVO:	Realizar embajadas culturales en la Universidad y en las localidades de la provincia y la región.		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF ,Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Elaborar agenda de visitas guiadas a las instalaciones de la Universidad.		Dirección de Admisión	Director(a) de Admisión	Actas
2	Remitir invitaciones a los centros educativos más representativos de la provincia y la región.		Dirección de Admisión	Director(a) de Admisión	Oficio
3	Realizar embajadas culturales a estudiantes de los últimos años escolares a las instalaciones de la Universidad.		Dirección de Admisión	Director(a) de Admisión	Registro de escolares, Registros fotográficos y audiovisuales
4	Realizar charlas vocacionales a los centros educativos locales y regionales.		Dirección de Admisión	Director(a) de Admisión	Registro de visitas, Registro de escolares, Registros fotográficos y audiovisuales
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 47: PM01.01.02.04 (General) - Diagrama BPMN 2.0

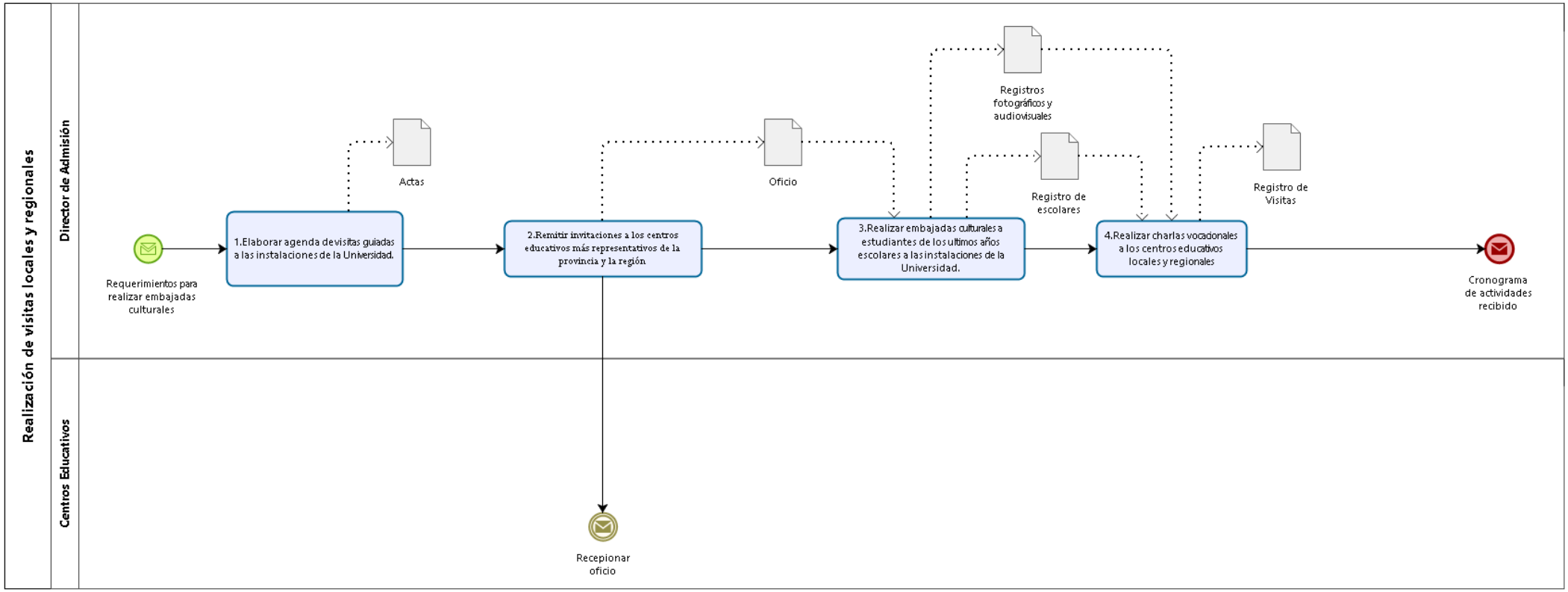


Figura N° 48: PM01.01.02.04 (Parte 1) - Diagrama BPMN 2.0

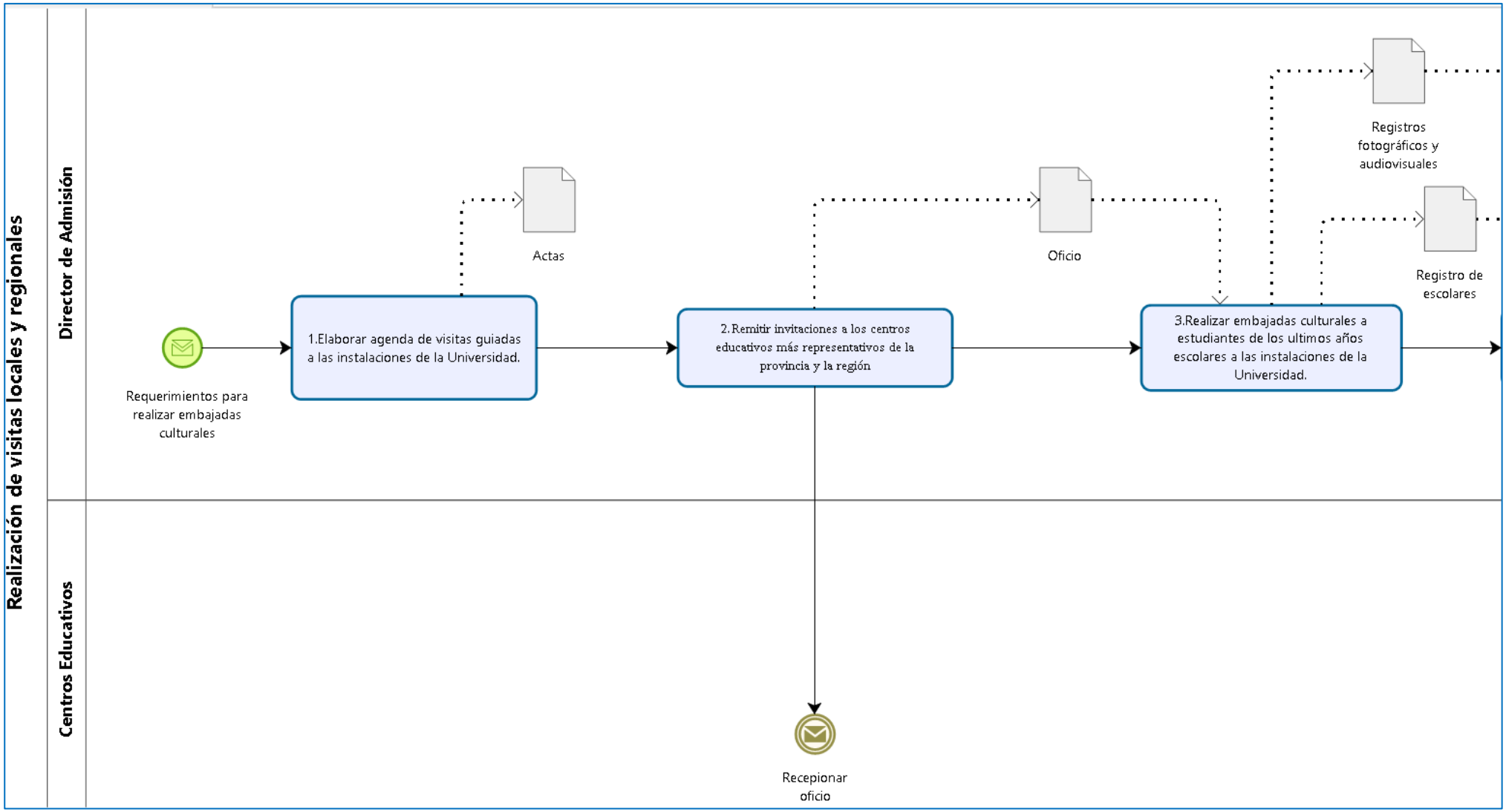


Figura N° 49: PM01.01.02.04 (Parte 2) - Diagrama BPMN 2.0

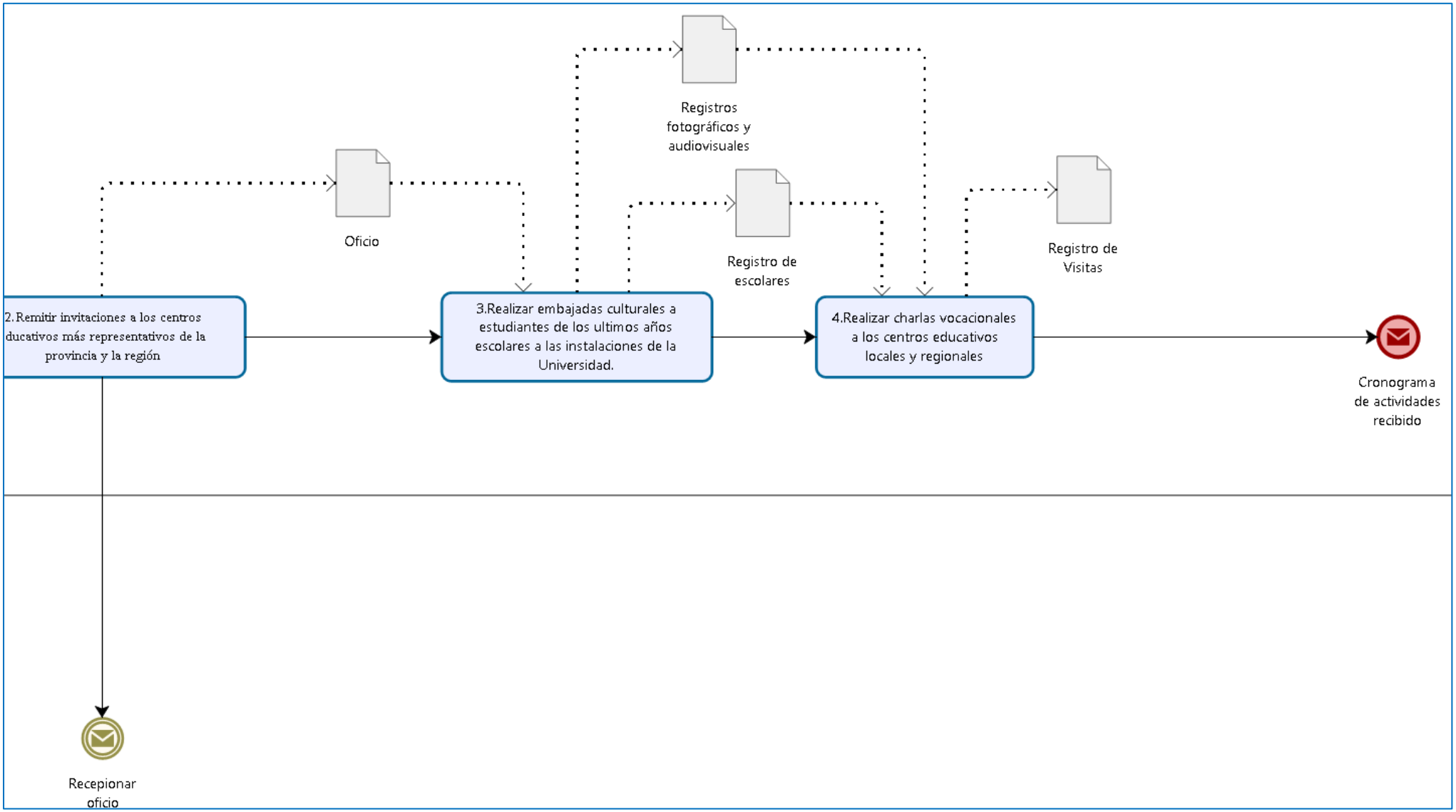


Tabla N° 17: PM01.01.02.05 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.02.05 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.02.Difusión del Proceso de Admisión de Pregrado
TÍTULO:	Elaboración y Presentación de Informe de Difusión		
A. OBJETIVO:	Presentar Informe de Difusión del Proceso de Admisión de Pregrado		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Elaborar Informe de Difusión del Proceso de Admisión.		Dirección de Admisión	Director(a) de Admisión	Informe de Difusión
2	Remitir Informe de Difusión del Proceso de Admisión.		Dirección de Admisión	Director(a) de Admisión	Oficio, Informe de Difusión
3	Recepcionar y evaluar Informe de Difusión del Proceso de Admisión.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio, Informe de Difusión

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 50: PM01.01.02.05 (General) - Diagrama BPMN 2.0

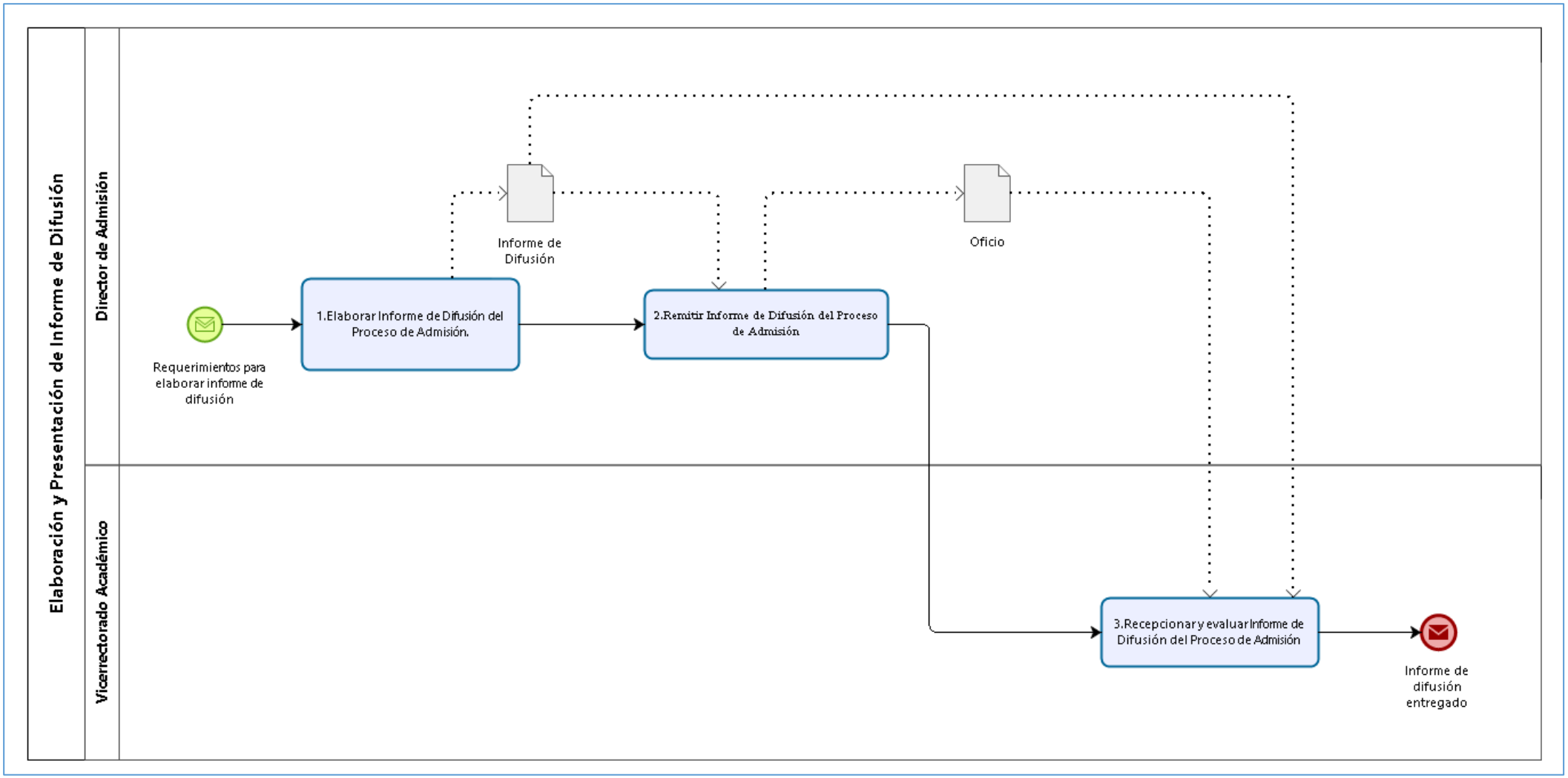


Figura N° 51: PM01.01.02.05 (Parte 1) - Diagrama BPMN 2.0

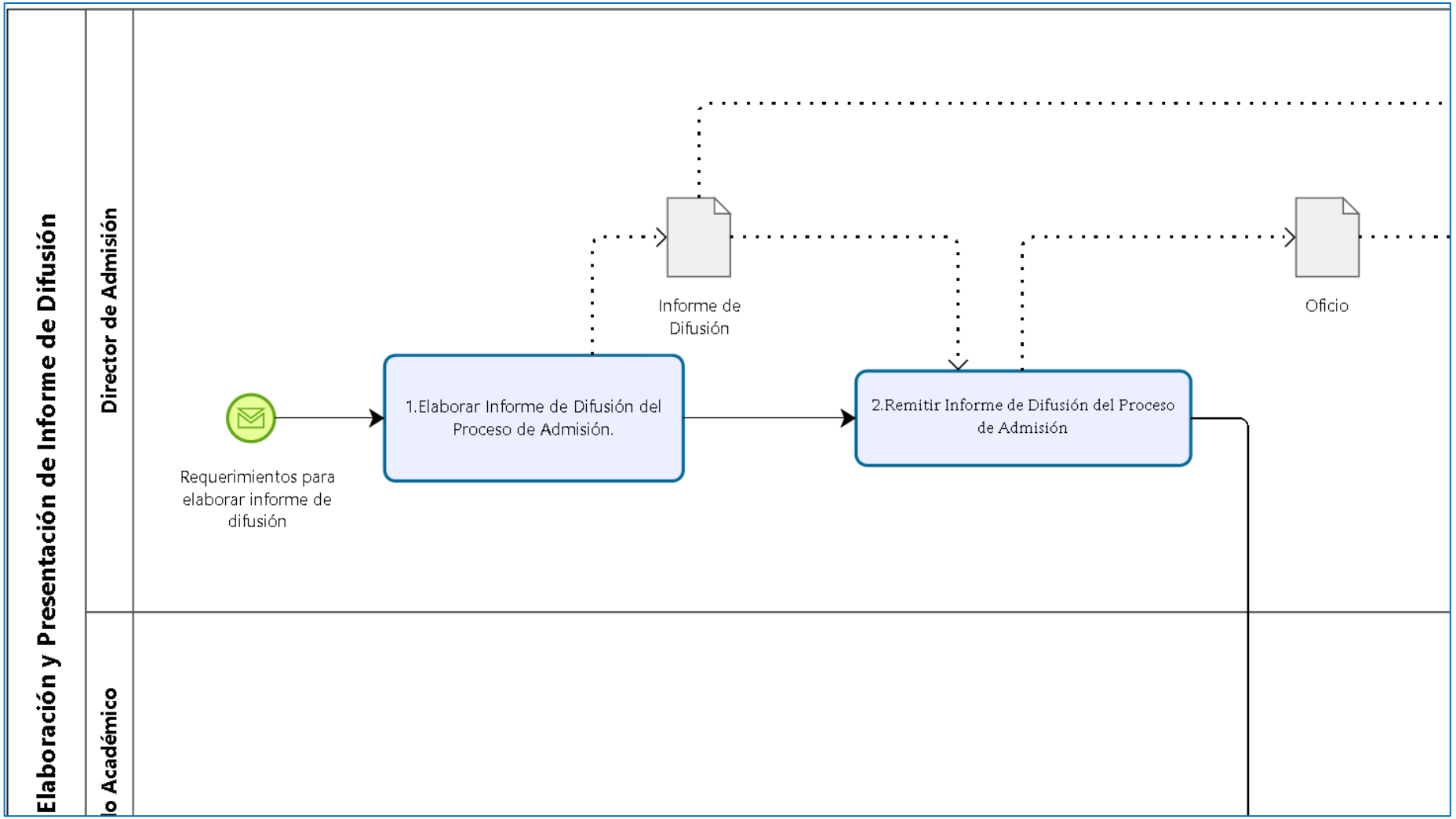


Figura N° 52: PM01.01.02.05 (Parte 2) - Diagrama BPMN 2.0

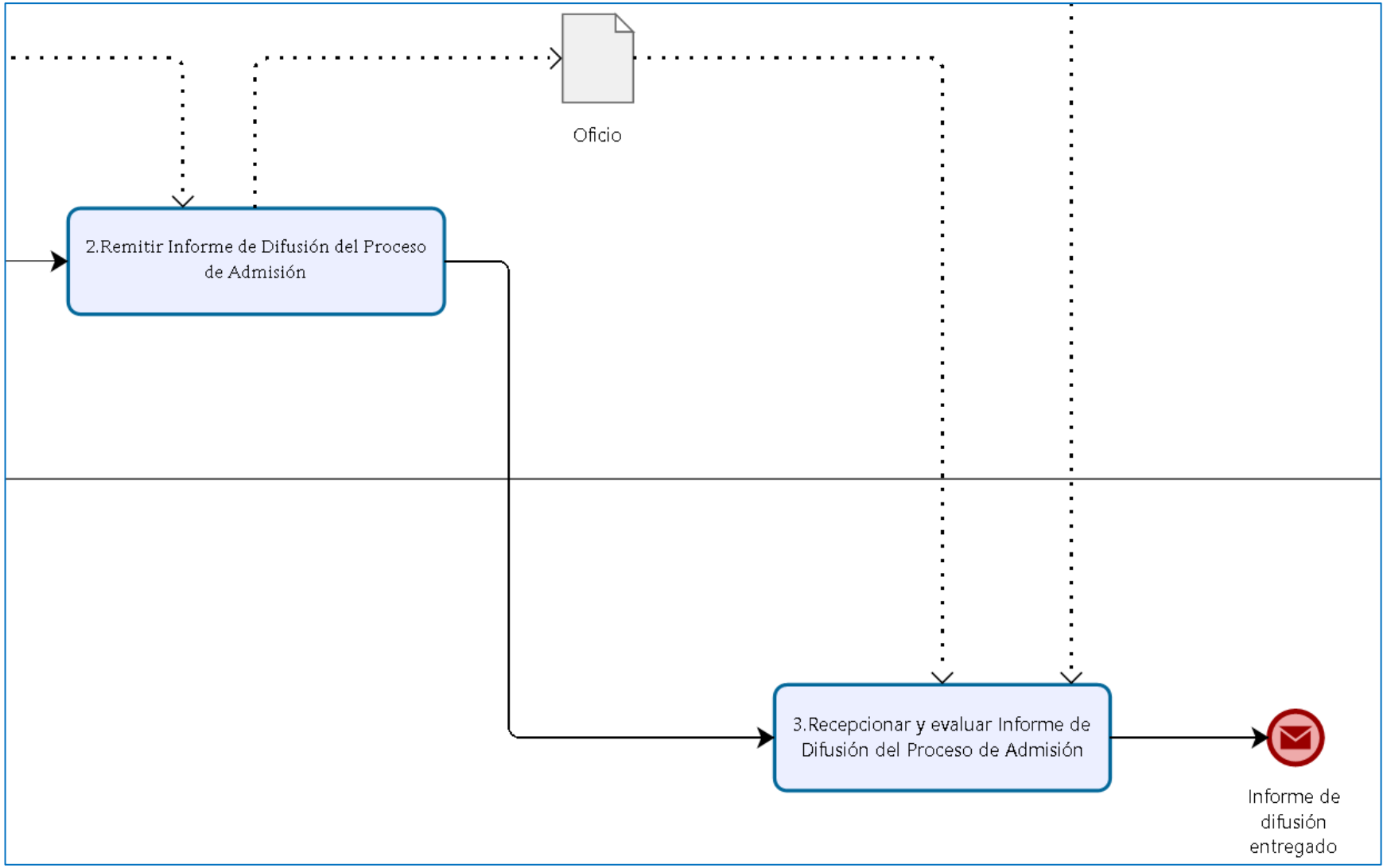


Tabla N° 18: PM01.01.02.05 - Ficha de Proceso

	FICHA DE PROCESO DE NIVEL 2				**Código:** PM01.01.03 **Versión:** 1.0
I. DATOS GENERALES DEL PROCESO					
1. NOMBRE DEL PROCESO	Inscripción al Proceso de Admisión de Pregrado	**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Proceso de Admisión de Programas de Pregrado	
2. OBJETIVO DEL PROCESO	Inscribir a los postulantes a las carreras profesionales de pregrado.				
4. DUEÑO DEL PROCESO	Director de Admisión	**5. LÍMITES DEL PROCESO**	**INICIO**	El pago de requisitos por derecho de inscripción del postulante a las carreras profesionales de pregrado	
			FIN	Con el envío de expedientes de voucher de los inscritos a la Dirección General de Administración	
II. DESCRIPCIÓN DEL PROCESO					
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**	**9. CONTROLES APLICADOS**	**10. PRODUCTOS**	**11. CLIENTES**
Dirección de Admisión Banco de la Nación	Cuenta y Código de Pago por derecho de inscripción Voucher de Pago por inscripción	**PM01.01.03.01.Inscripción a las modalidades de Admisión a las Carreras Profesionales de Pregrado**	Postulante realiza pago y se inscribe en módulo web de admisión	Registro de Inscripción del Postulante	Dirección de Admisión Postulante
Postulante	Requisitos documentarios especificados en el Reglamento de Admisión tales como: DNI, Voucher de Pago original, Ficha de inscripción, Acuerdo de Privacidad de Protección de Datos Personales, Ficha socioeconómica.	**PM01.01.03.02.Presentación y validación de requisitos de inscripción**	Se verifica los requisitos y se realiza la toma de fotografía	Carné del Postulante Carpeta del Postulante	Postulante Dirección de Admisión
Dirección de Admisión	Vouchers Registro de Inscritos	**PM01.01.03.03.Control de las inscripciones**	Se realiza consolidación de vouchers e inscritos	Expediente del Postulante	Dirección de Admisión Dirección General de Administración Oficina de Fondos Oficina de Contabilidad

III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO	
12. TIPO	**13. DESCRIPCIÓN**
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica, 1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas, 2 Recepcionistas.
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).
	Material: Material de Oficina

IV. DOCUMENTACIÓN DEL PROCESO	
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**
1. Registro de postulantes inscritos	1. Ley Universitaria 30220
2. Registro de expedientes de postulantes	2. Estatuto
	3. Reglamento General
	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento para Pago de Subvenciones al Personal
	8. Reglamento de Admisión

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 53: PM01.01.03 - Ficha de Proceso

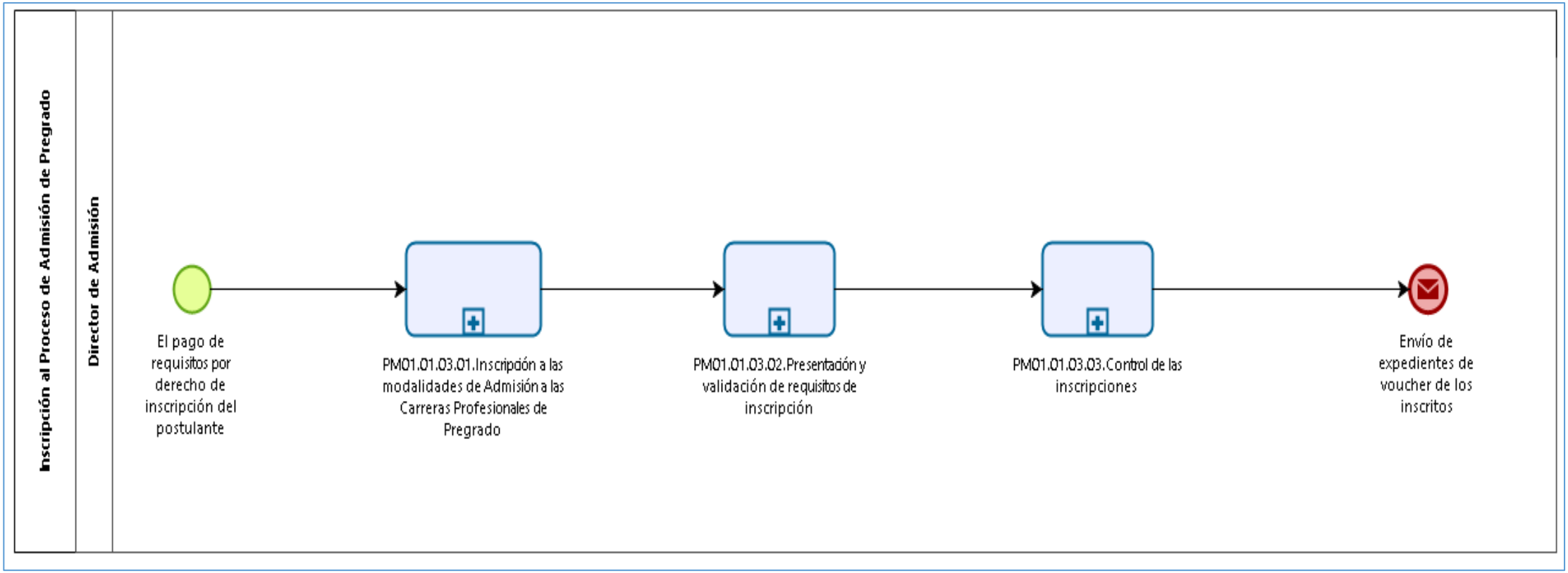


Tabla N° 19: PM01.01.03.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.03.01 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.03.Inscripción al Proceso de Admisión de Pregrado
TÍTULO:	Inscripción a las modalidades de Admisión para Pregrado		
A. OBJETIVO:	Inscribirse vía web para postular al Proceso de Admisión de Pregrado		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF ,Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Brindar informes a interesados respecto a los requisitos para la inscripción al proceso de admisión.		Dirección de Admisión	Recepcionista	Fichas Informativas
2	Realizar pago por derecho de examen de admisión (indicar el número de DNI del postulante) según modalidad respectiva a la cuenta de la UNS del Banco de la Nación.		Postulante	Postulante	Voucher
3	Realizar inscripción a través del sistema (SIIGAA) web de Admisión según modalidad a la que postula.		Postulante	Postulante	Registro del SIIGAA, Voucher
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 54: PM01.01.03.01 (General) - Diagrama BPMN 2.0

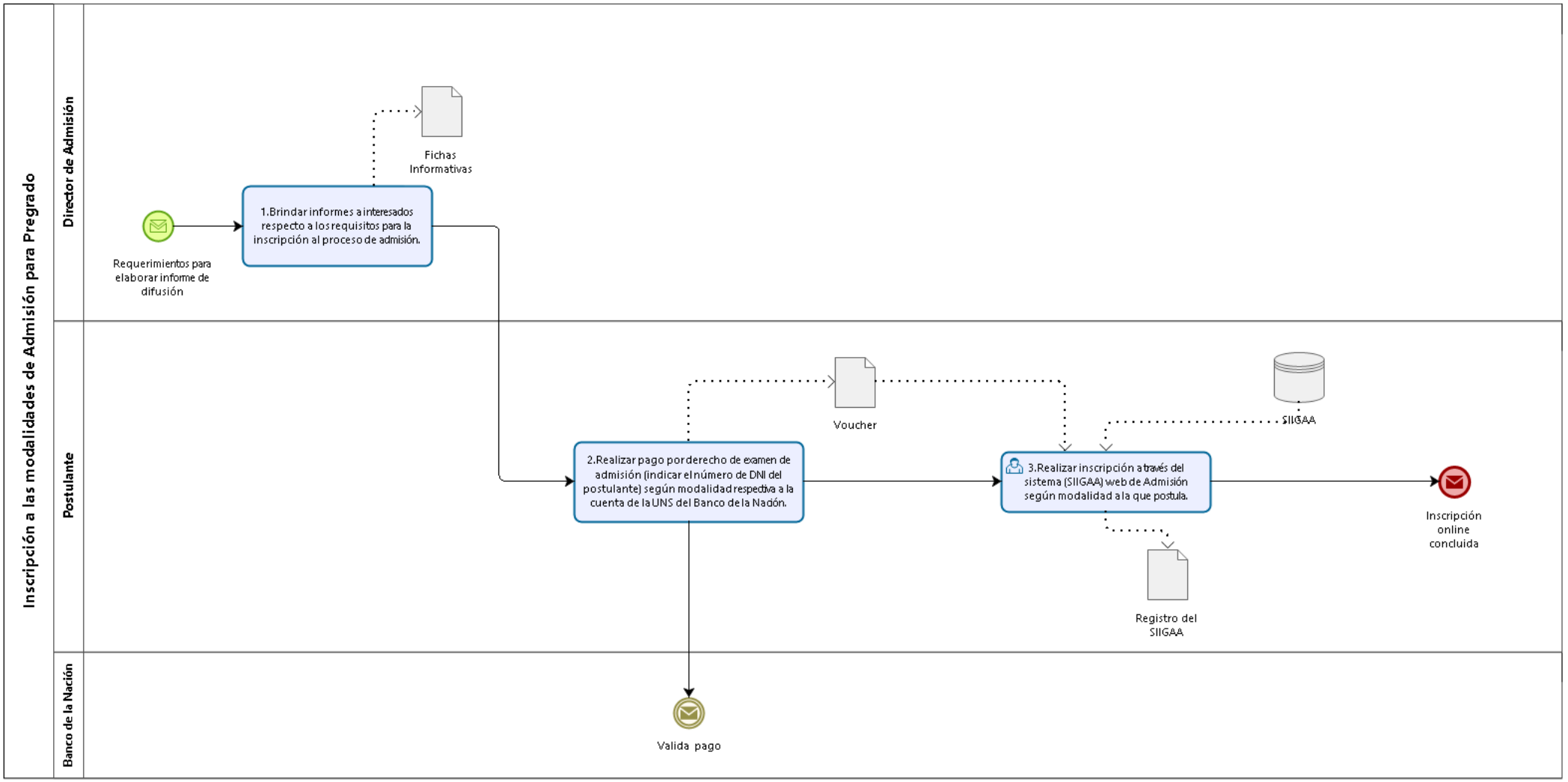


Figura N° 55: PM01.01.03.01 (Parte 1) - Diagrama BPMN 2.0

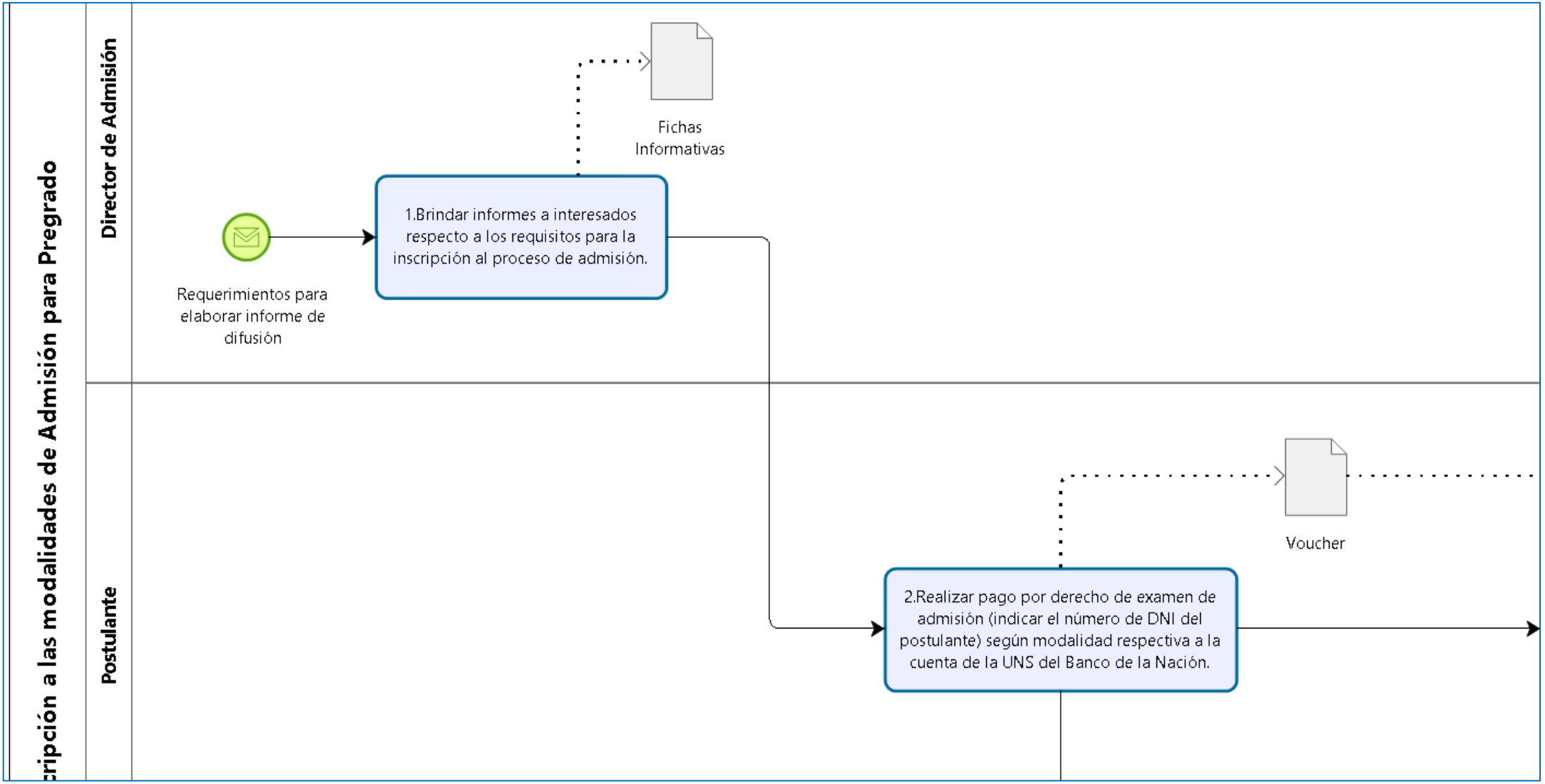


Figura N° 56: PM01.01.03.01 (Parte 2) - Diagrama BPMN 2.0

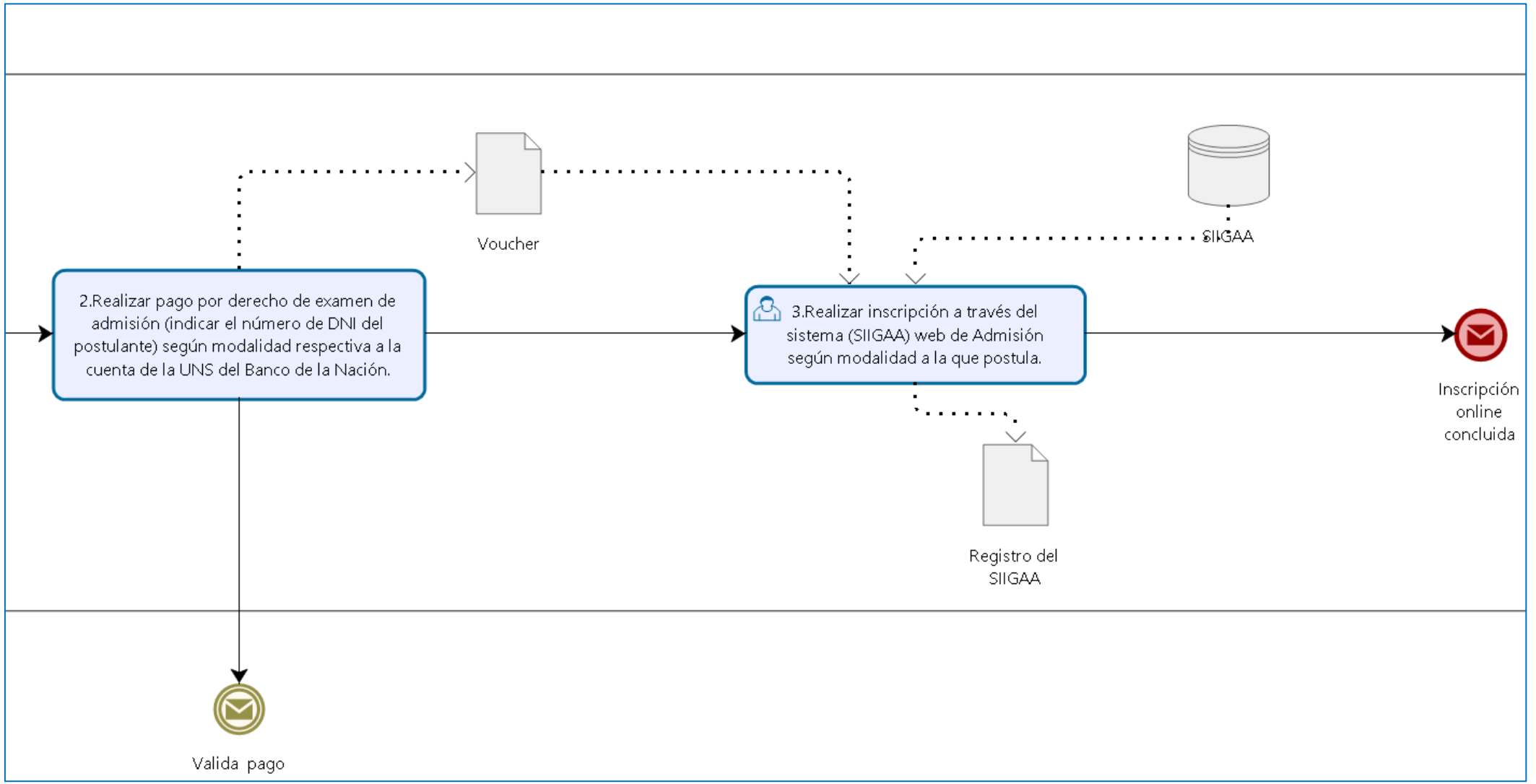


Tabla N° 20: PM01.01.03.02 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.03.02 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.03.Inscripción al Proceso de Admisión de Pregrado
TÍTULO:	Presentación y validación de requisitos de inscripción		
A. OBJETIVO:	Validar requisitos de inscripción al Proceso de Admisión de Pregrado		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF ,Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Presentar requisitos documentarios (DNI, Voucher de Pago del Banco de la Nación, Ficha de inscripción, Ficha socioeconómica, Acuerdo de Privacidad de Protección de Datos Personales) para completar inscripción según modalidad y el Reglamento de Admisión.		Dirección de Admisión	Postulante	Requisitos documentarios
2	Recepcionar, verificar y validar requisitos documentarios y derivar para toma de fotografía.		Dirección de Admisión	Recepcionista	Expediente del Postulante
3	Realizar toma, edición de fotografía y elaborar carnés de postulantes según modalidad.		Dirección de Admisión	Especialista de Sistemas	Registro de Carnés, Expediente del Postulante
4	Solicitar firma y huella digital para conformidad de la inscripción.		Dirección de Admisión	Especialista de Sistemas	Registro de inscripción conforme del postulante
5	Entregar carpeta del postulante (prospecto de admisión, copia de ficha de inscripción, copia de acuerdo de privacidad de protección de datos personales, folder, carné y fichas informativas).		Dirección de Admisión	Especialista de Sistemas	Registro de inscripción conforme del postulante, Carpeta del postulante
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			

Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 57: PM01.01.03.02 (General) - Diagrama BPMN 2.0

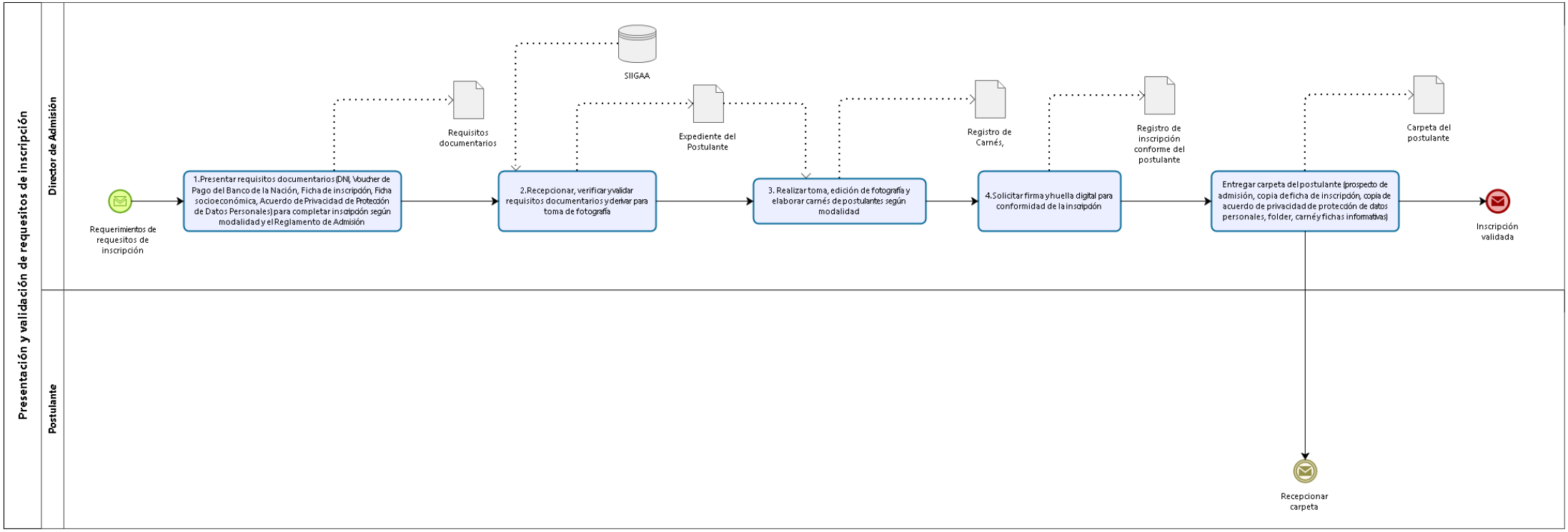


Figura N° 58: PM01.01.03.02 (Parte 1) - Diagrama BPMN 2.0

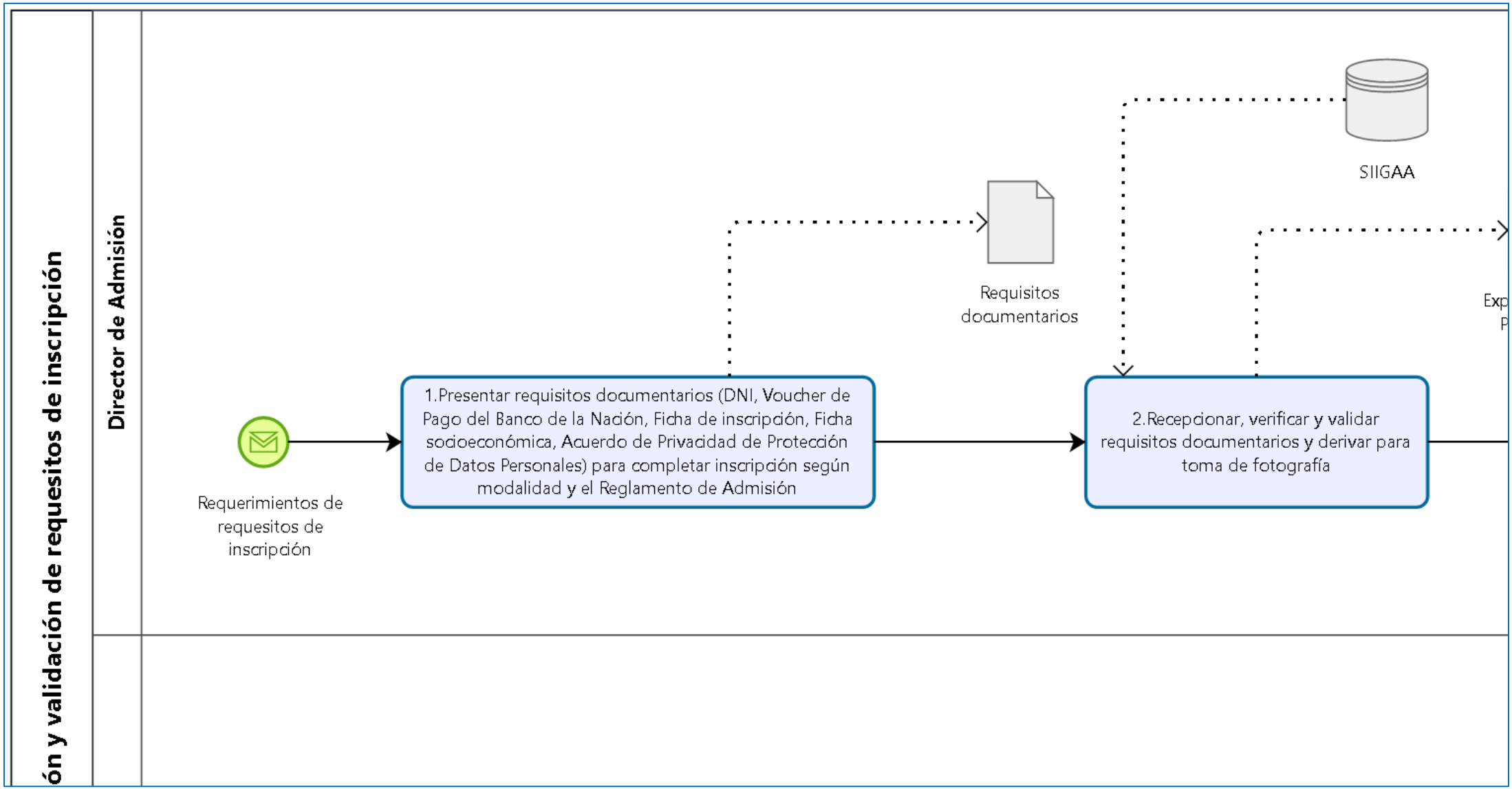


Figura N° 59: PM01.01.03.02 (Parte 2) - Diagrama BPMN 2.0

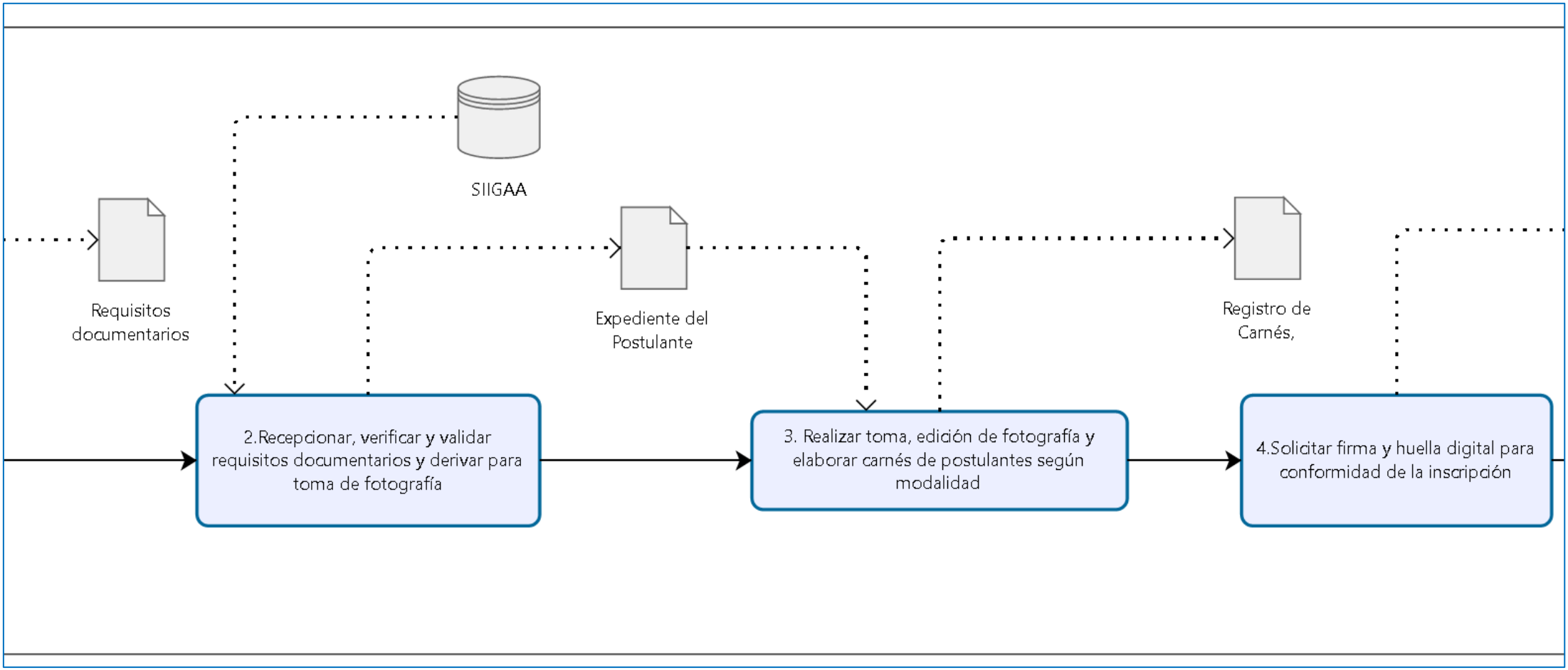


Figura N° 60: PM01.01.03.02 (Parte 3) - Diagrama BPMN 2.0

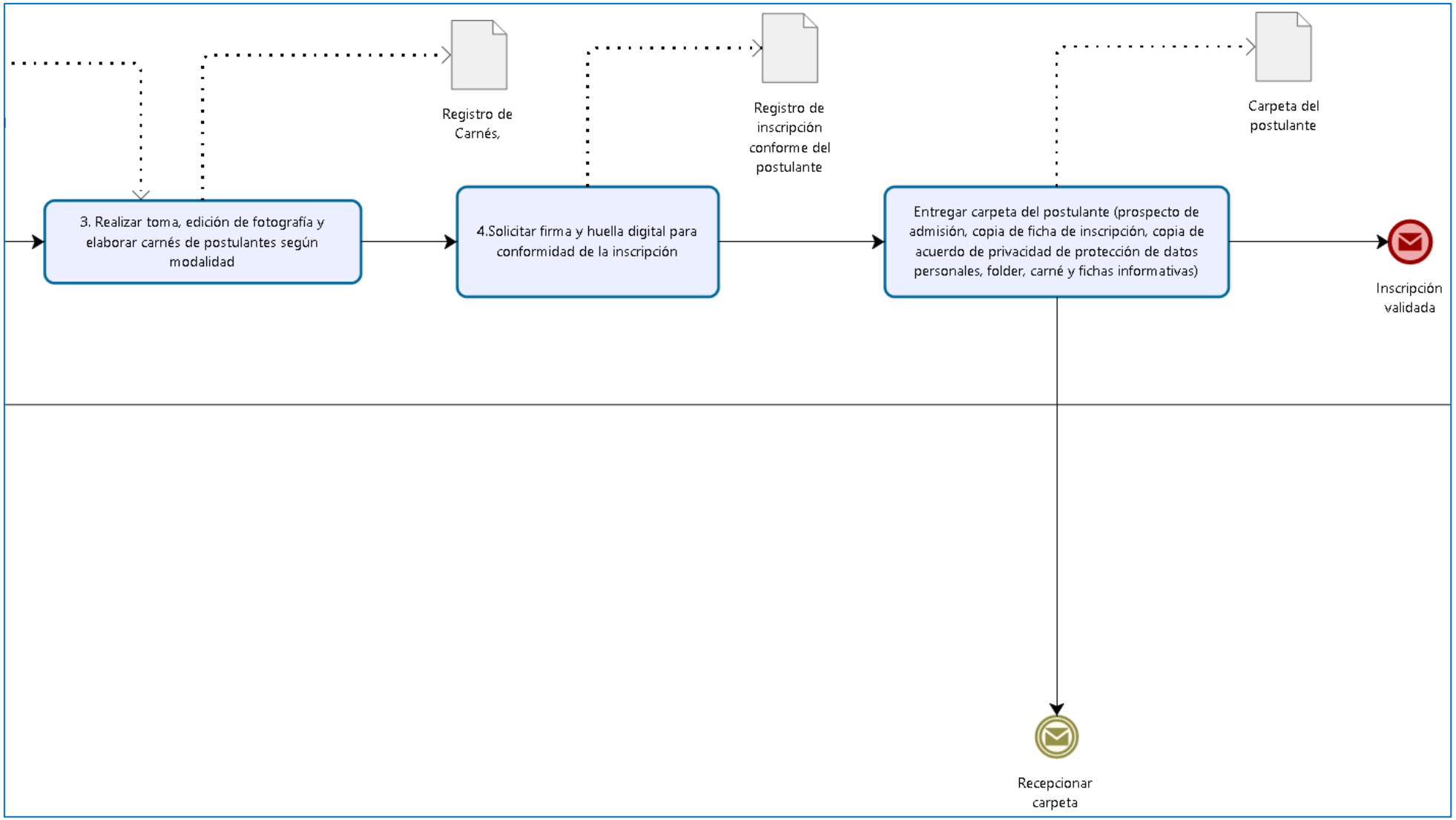


Tabla N° 21: PM01.01.03.03 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.03.03 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.03.Inscripción al Proceso de Admisión de Pregrado
TÍTULO:	Control de las inscripciones		
A. OBJETIVO:	Realizar control de los ingresos del Proceso de Admisión		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Verificar diariamente que la cantidad de postulantes y de vouchers mantengan una relación correcta.		Dirección de Admisión	Especialista de Sistemas	Registro de ficha de inscripción de postulante, Registro de vouchers
2	Elaborar y remitir informe semanal de control del Proceso de Admisión para la revisión de expedientes de los postulantes (fichas, vouchers y cartas de renuncia de ser el caso).		Dirección de Admisión	Especialista de Sistemas	Oficio, Informe semanal de control del Proceso de Admisión, Expedientes de Postulantes
3	Recepcionar y verificar informe semanal de control del Proceso de Admisión y remitir a Vicerrectorado Académico.		Dirección de Admisión	Director(a) de Admisión	Oficio, Informe semanal de control del Proceso de Admisión, Expedientes de Postulantes
4	Recepcionar y remitir informe semanal de control del Proceso de Admisión a la Dirección General de Administración.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio, Informe semanal de control del Proceso de Admisión, Expedientes de Postulantes
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 61: PM01.01.03.03 - Diagrama BPMN 2.0

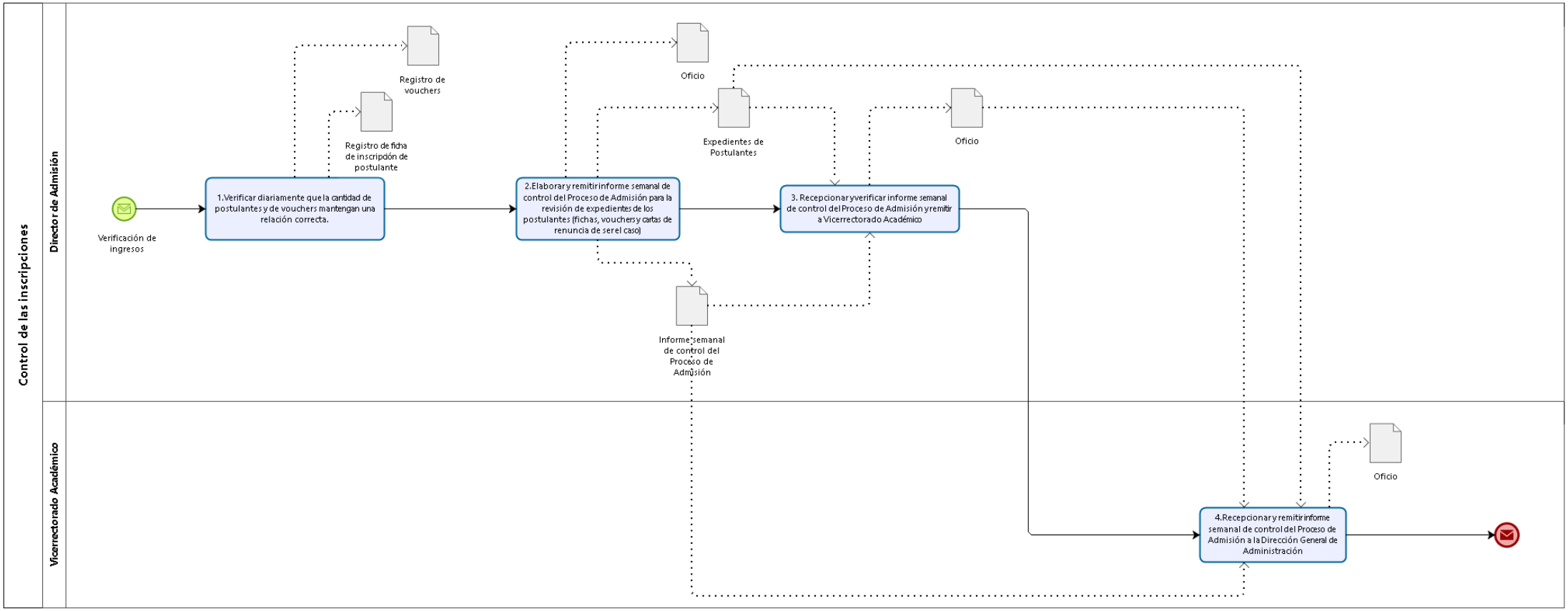


Figura N° 62: PM01.01.03.03 (Parte 1) - Diagrama BPMN 2.0

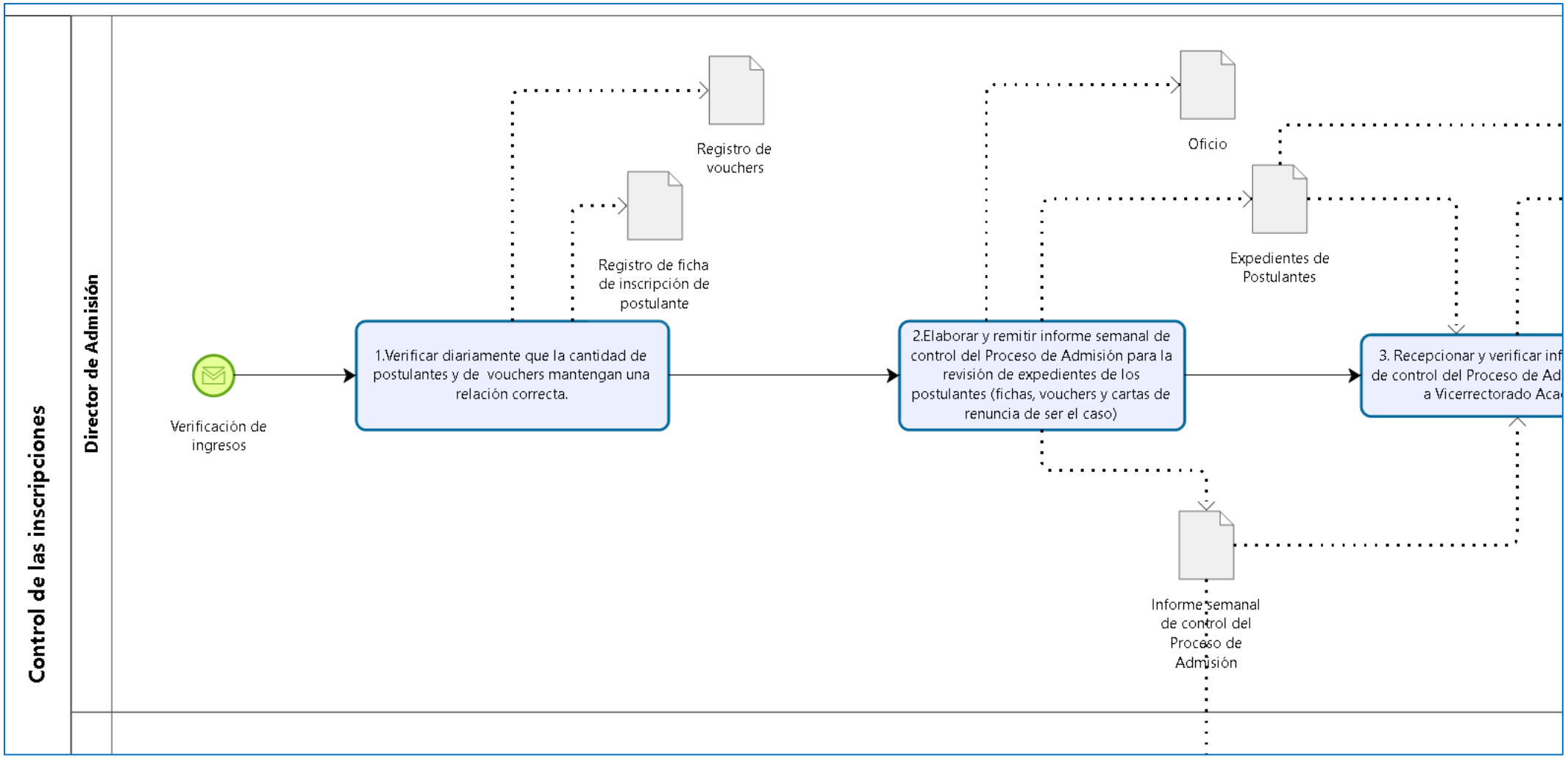


Figura N° 63: PM01.01.03.03 (Parte 2) - Diagrama BPMN 2.0

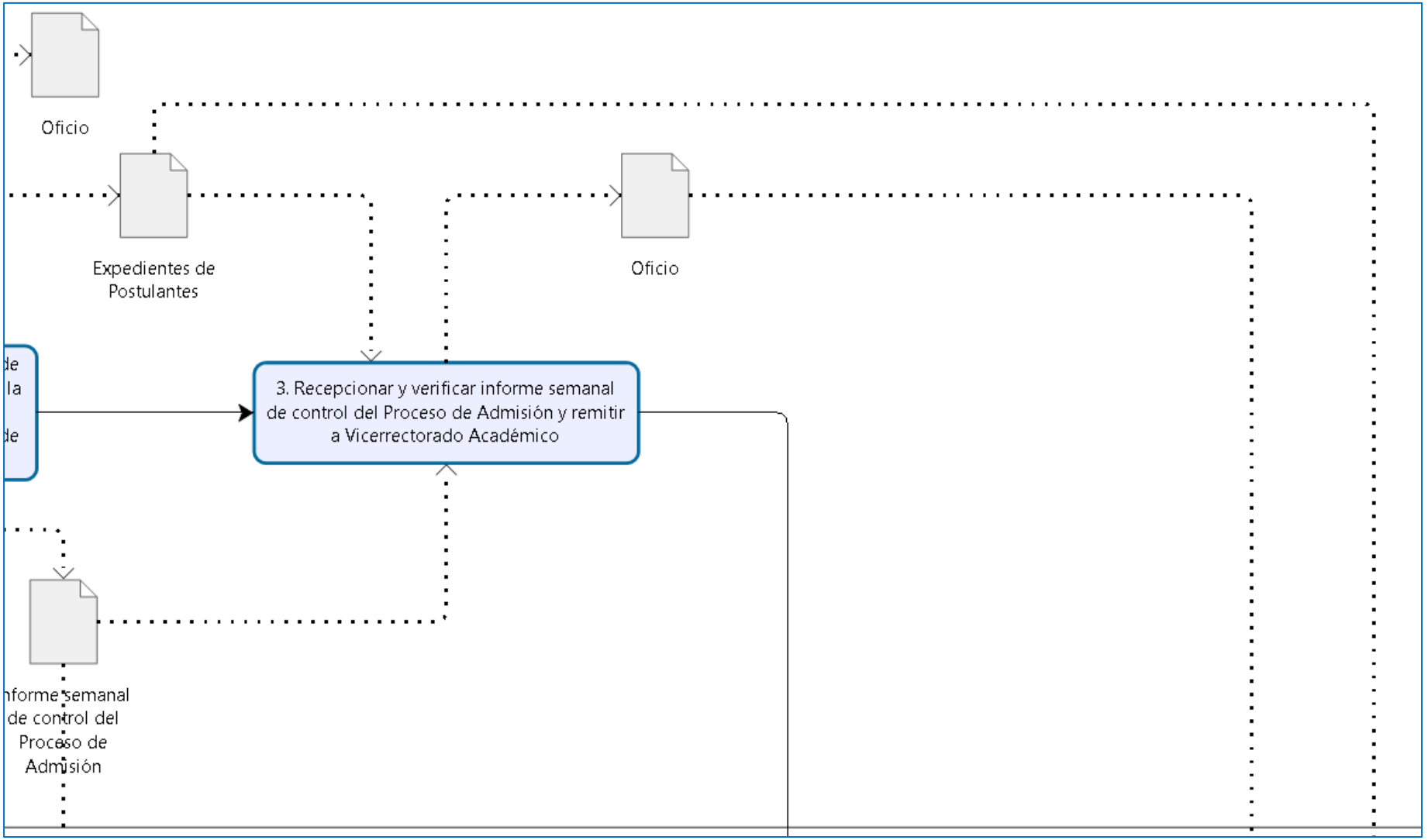


Figura N° 64: PM01.01.03.03 (Parte 3) - Diagrama BPMN 2.0

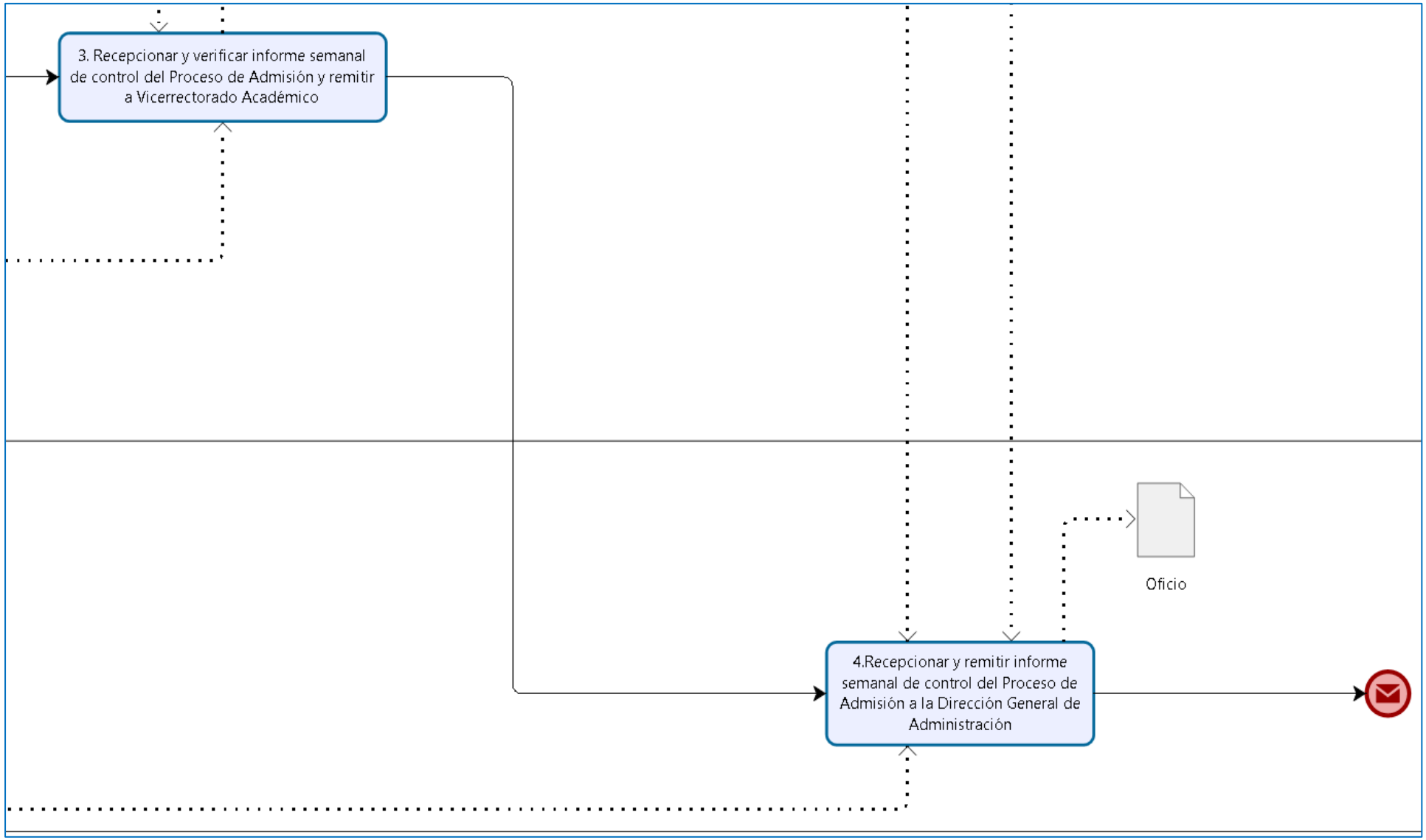


Tabla N° 22: PM01.01.04 - Ficha de Proceso

	FICHA DE PROCESO DE NIVEL 2				**Código:** PM01.01.04 **Versión:** 1.0
I. DATOS GENERALES DEL PROCESO					
1. NOMBRE DEL PROCESO	Gestión de Exámenes del Proceso de Admisión de Pregrado	**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Proceso de Admisión de Programas de Pregrado	
2. OBJETIVO DEL PROCESO	Gestionar la elaboración y aplicación eficiente de los Exámenes del Proceso de Admisión de Pregrado.				
4. DUEÑO DEL PROCESO	Director de Admisión	**5. LÍMITES DEL PROCESO**	**INICIO**	Reunión para la actualización del banco de preguntas para los exámenes de admisión de pregrado	
			FIN	Publicación de los resultados del Proceso de Admisión de Pregrado	

II. DESCRIPCIÓN DEL PROCESO					
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**	**9. CONTROLES APLICADOS**	**10. PRODUCTOS**	**11. CLIENTES**
Dirección de Admisión	Ítems de Preguntas	**PM01.01.04.01.Elaboración y actualización de ítems del banco de preguntas**	Se elabora e incorpora nuevos ítems	Banco de Preguntas	Dirección de Admisión
Dirección de Admisión	Formulario de inscripción	**PM01.01.04.02.Selección de integrantes para las Subcomisiones del Proceso de Admisión**	Se realiza un sorteo para determinar los integrantes de las subcomisiones y se solicita su oficialización ante Consejo Universitario	Acuerdo de Consejo Universitario de integrantes de las subcomisiones	Dirección de Admisión Dirección General de Administración
Dirección de Admisión	Esquema axial de preguntas por canal	**PM01.01.04.03.Elaboración de los Exámenes del Proceso de Admisión**	Se realiza la selección de ítems y digitalización de los exámenes	Exámenes por Canal	Dirección de Admisión
Dirección de Admisión	Exámenes por Canal Hojas Ópticas en blanco	**PM01.01.04.04.Aplicación de los Exámenes del Proceso de Admisión**	Se realiza el recojo, procesamiento y validación de los resultados del proceso de admisión de pregrado	Reporte de Postulantes e ingresantes por orden de mérito Reporte de Postulantes e ingresantes por escuela profesional Formatos de Control registrados Hojas Ópticas registradas	Dirección de Admisión

Dirección de Admisión	Reporte de Postulantes e ingresantes por orden de mérito Reporte de Postulantes e ingresantes por escuela profesional	**PM01.01.04.05.Aprobación y Publicación de resultados del Proceso de Admisión**	Se realiza la aprobación de los resultados del proceso por Consejo Universitario y se solicita su publicación en el Portal y redes sociales oficiales	Registro de Resultados del Proceso de Admisión en el Portal y Redes Sociales Resolución de Consejo Universitario de los resultados del Proceso de Admisión	Dirección de Admisión Dirección de Imagen Ingresantes

III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO	
12. TIPO	**13. DESCRIPCIÓN**
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica,1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas, 2 Recepcionistas, Comisiones para el Proceso de Admisión.
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).
	Material: Material de Oficina

IV. DOCUMENTACIÓN DEL PROCESO	
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**
1. Actas	1. Ley Universitaria 30220
2. Registro de Postulantes e ingresantes por orden de mérito	2. Estatuto
3. Registro de Postulantes e ingresantes por escuela profesional	3. Reglamento General
	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento para Pago de Subvenciones al Personal
	8. Reglamento de Admisión

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 65: PM01.01.04 (General) - Diagrama BPMN 2.0

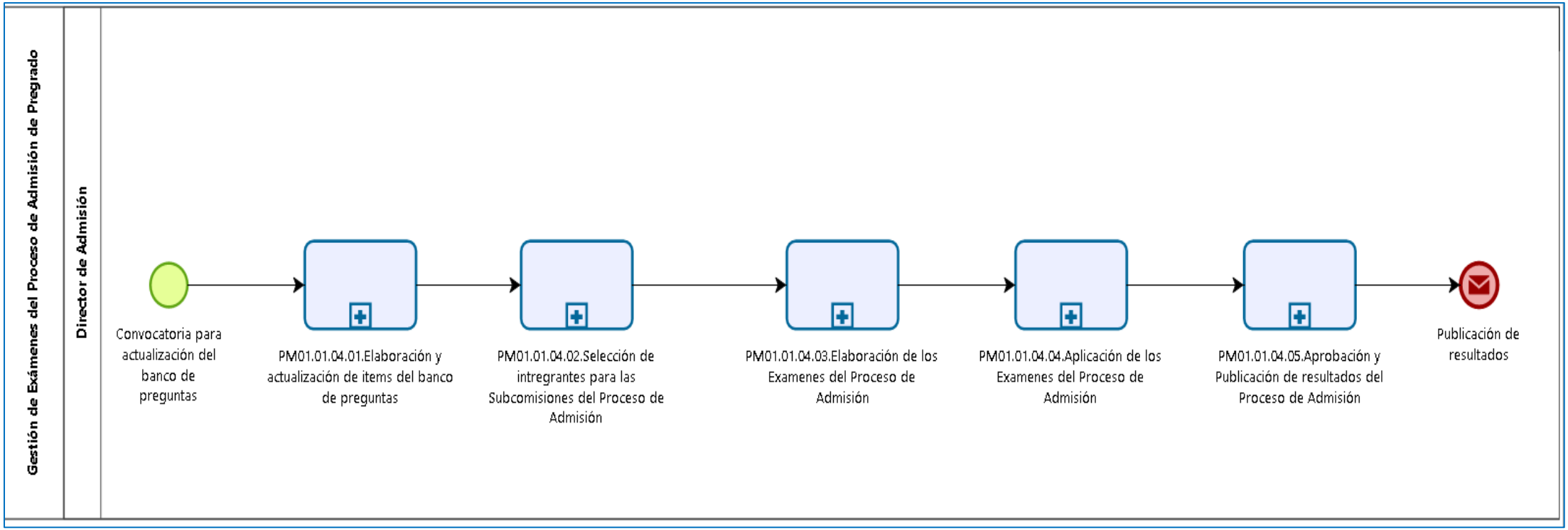


Figura N° 66: PM01.01.04 (Parte 1) - Diagrama BPMN 2.0

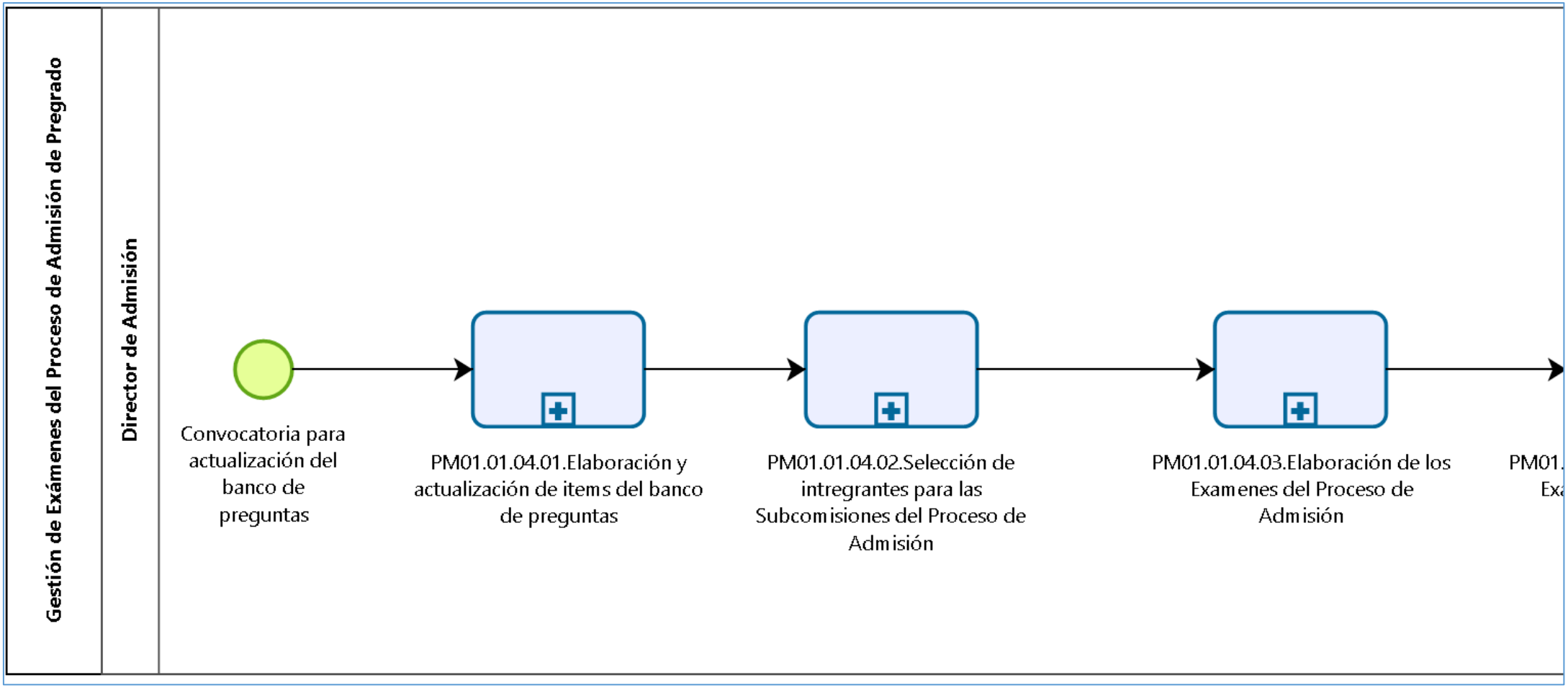


Figura N° 67: PM01.01.04 (Parte 2) - Diagrama BPMN 2.0

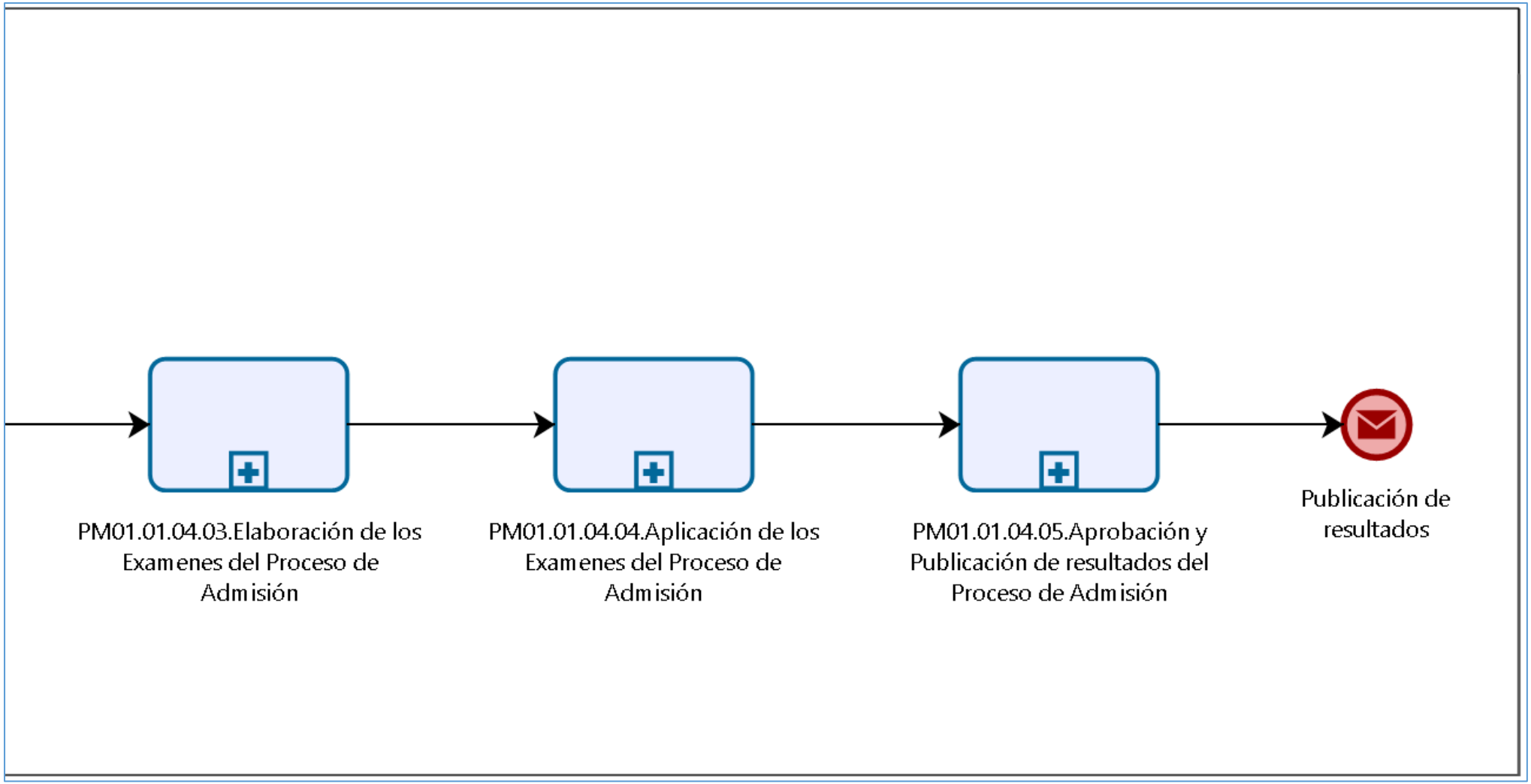


Tabla N° 23: PM01.01.04.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.04.01 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.04.Gestión de Exámenes del Proceso de Admisión de Pregrado
TÍTULO:	Elaboración y actualización de ítems del banco de preguntas		
A. OBJETIVO:	Elaborar y actualizar ítems del banco de preguntas para los exámenes de admisión		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Revisar ítems del banco de preguntas para cada asignatura del Examen ordinario.		Dirección de Admisión	Director(a) de Admisión	Registro de ítems
2	Elaborar nuevos ítems para el banco de preguntas para cada asignatura del Examen ordinario.		Dirección de Admisión	Director(a) de Admisión	Registro de ítems
3	Incorporar y actualizar ítems al banco de preguntas para cada asignatura del Examen ordinario.		Dirección de Admisión	Director(a) de Admisión	Acta, Registro de ítems
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:		Suma de duraciones			

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 68: PM01.01.04.01 - Diagrama BPMN 2.0

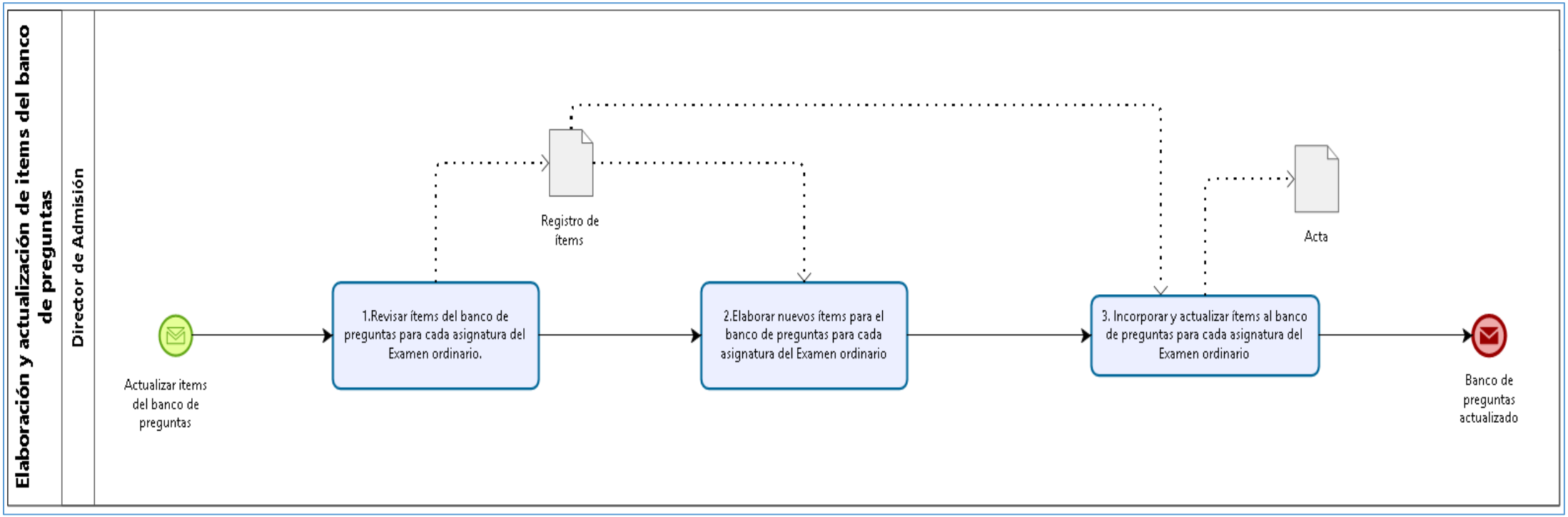


Figura N° 69: PM01.01.04.01 (Parte 1) - Diagrama BPMN 2.0

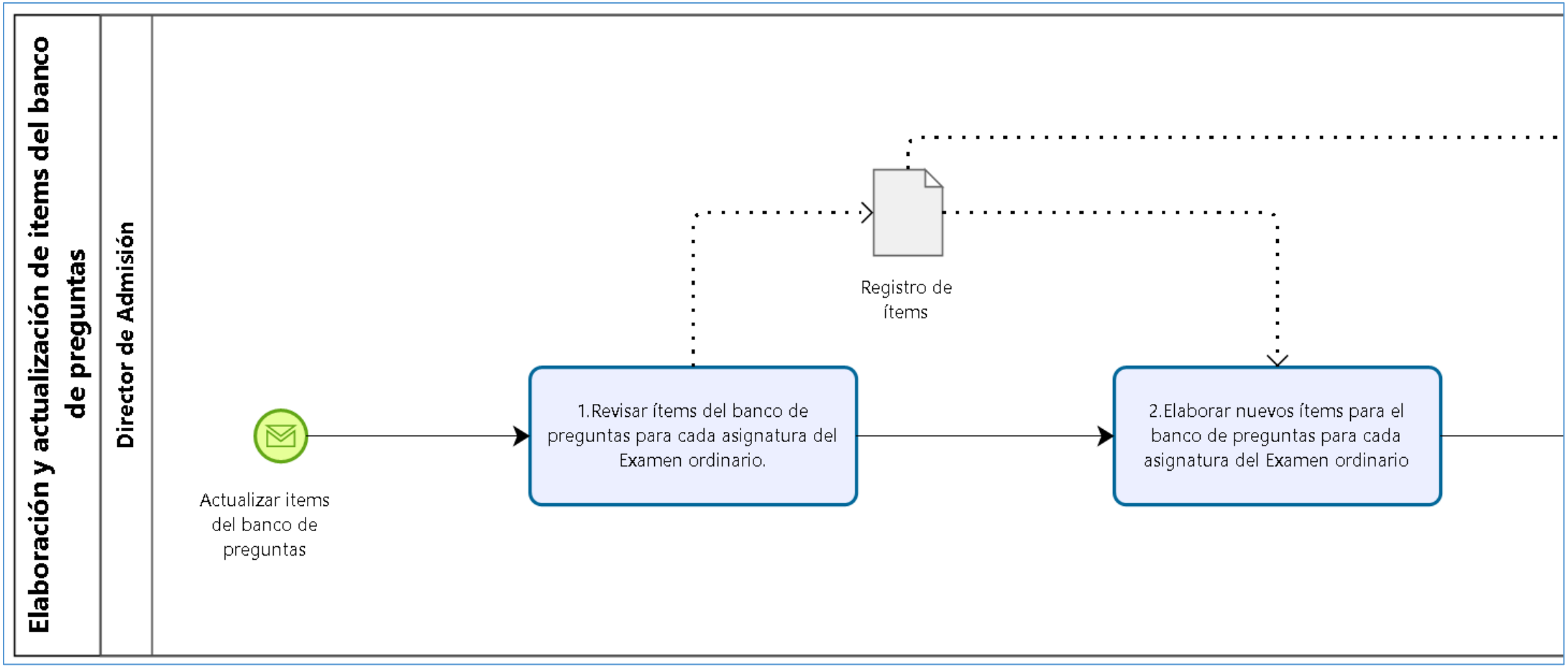


Figura N° 70: PM01.01.04.01 (Parte 1) - Diagrama BPMN 2.0

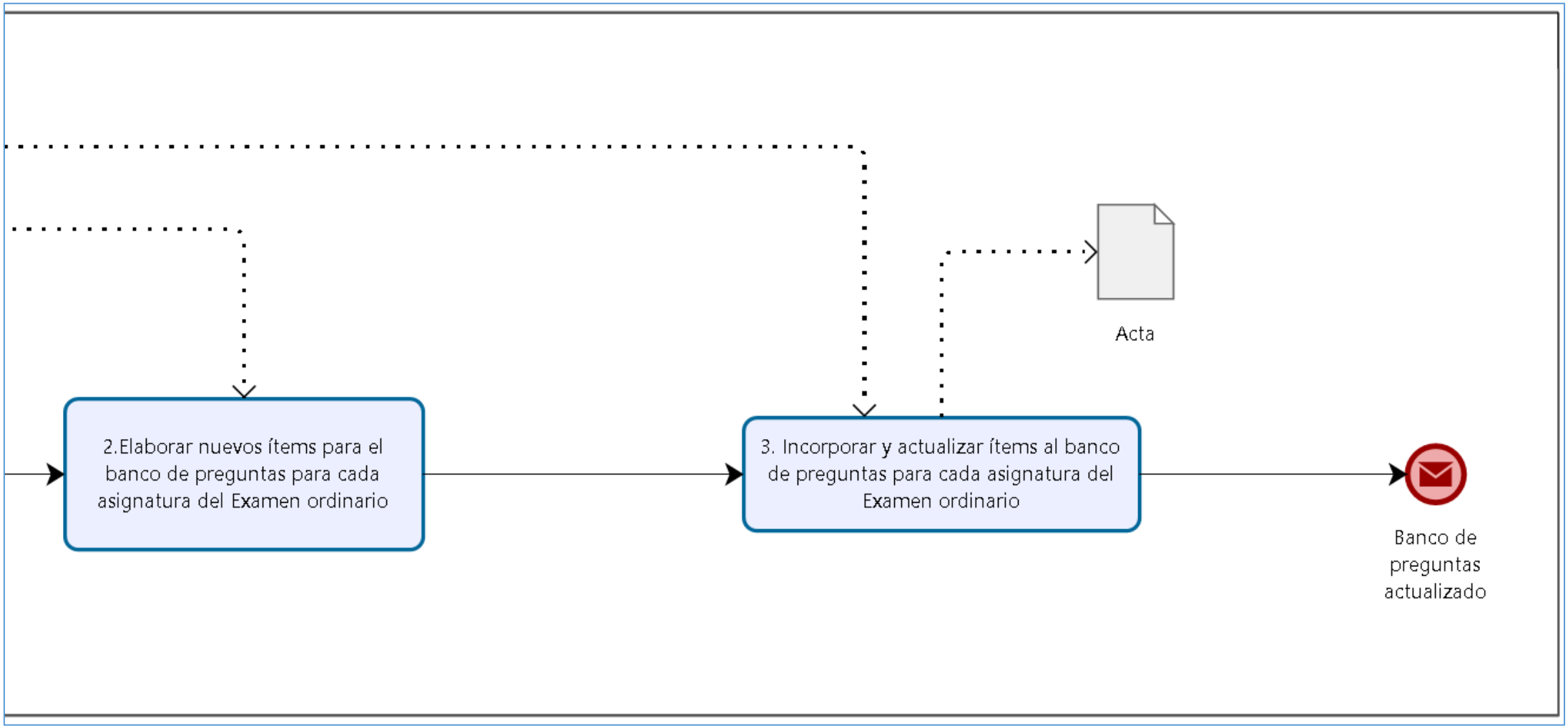


Tabla N° 24: PM01.01.04.02 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.04.02 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.04.Gestión de Exámenes del Proceso de Admisión de Pregrado
TÍTULO:	Selección de integrantes para las Subcomisiones del Proceso de Admisión		
A. OBJETIVO:	Seleccionar a los integrantes para las para las Subcomisiones del Proceso de Admisión		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Publicar convocatoria a través de un formulario de inscripción (voluntaria) en la primera puerta del Campus Universitario para la participación del personal Administrativo.		Dirección de Admisión	Director(a) de Admisión	Formulario de inscripción
2	Remitir convocatoria a través de un formulario de inscripción (voluntaria) a los Departamentos Académicos para la participación del personal Docente.		Dirección de Admisión	Director(a) de Admisión	Oficio, Formulario de inscripción
3	Remitir convocatoria a través de un formulario de inscripción (voluntaria) a las escuelas para la participación de los estudiantes de pregrado en el Examen Ordinario de admisión.		Dirección de Admisión	Director(a) de Admisión	Oficio, Formulario de inscripción
4	Realizar sorteo de administrativos, docentes y alumnos inscritos para determinar participantes para el Examen Ordinario de admisión.		Dirección de Admisión	Director(a) de Admisión	Registro de participantes del examen de admisión
5	Realizar propuesta de seleccionados (docentes, estudiantes y administrativos) para integrar las Subcomisiones del Examen Ordinario y remitir para su aprobación a Consejo Universitario.		Dirección de Admisión	Director(a) de Admisión	Oficio
6	Recepcionar y remitir propuesta de las Subcomisiones del Examen Ordinario de admisión para su aprobación.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio

7	Revisar propuesta de las Subcomisiones para la ejecución del examen de admisión.		Consejo Universitario	Consejo Universitario	Oficio
	Se cuenta con observaciones continuar, caso contrario ir al paso 10.		Consejo Universitario	Consejo Universitario	
8	Retornar propuesta, ir al paso 5.		Consejo Universitario	Consejo Universitario	Acuerdo
9	Aprobar propuesta y registrar en libro de actas.		Consejo Universitario	Secretario(a) General	Libro de Actas
10	Redactar acuerdo de aprobación de Subcomisiones del Examen Ordinario de admisión.		Secretaría General	Secretario(a) General	Oficio de Secretaría General
11	Enviar acuerdo a la Dirección de Admisión y dependencias interesadas.		Secretaría General	Secretario(a) General	Oficio de Secretaría General
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 71:PM01.01.04.02 - Diagrama BPMN 2.0

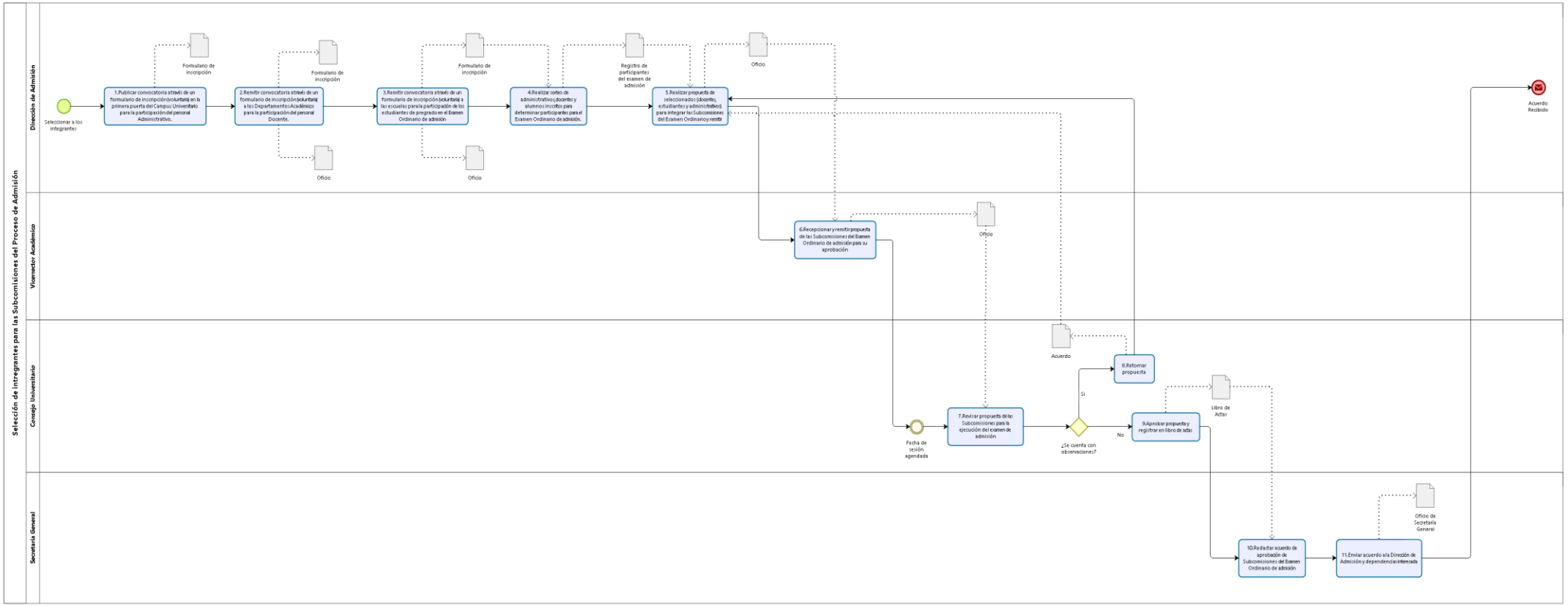


Figura N° 72: PM01.01.04.02 (Parte 1) - Diagrama BPMN 2.0

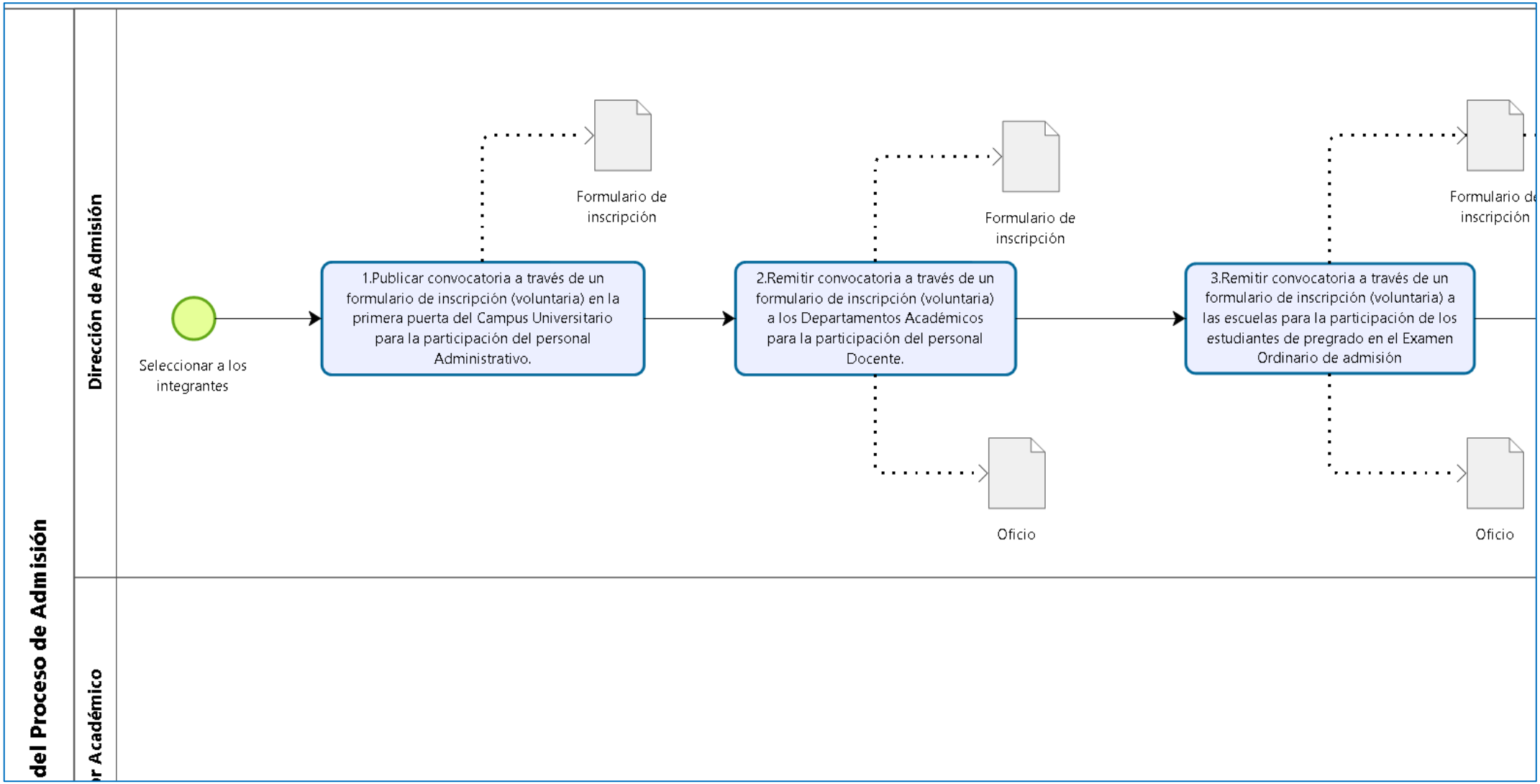


Figura N° 73: PM01.01.04.02 (Parte 1) - Diagrama BPMN 2.0

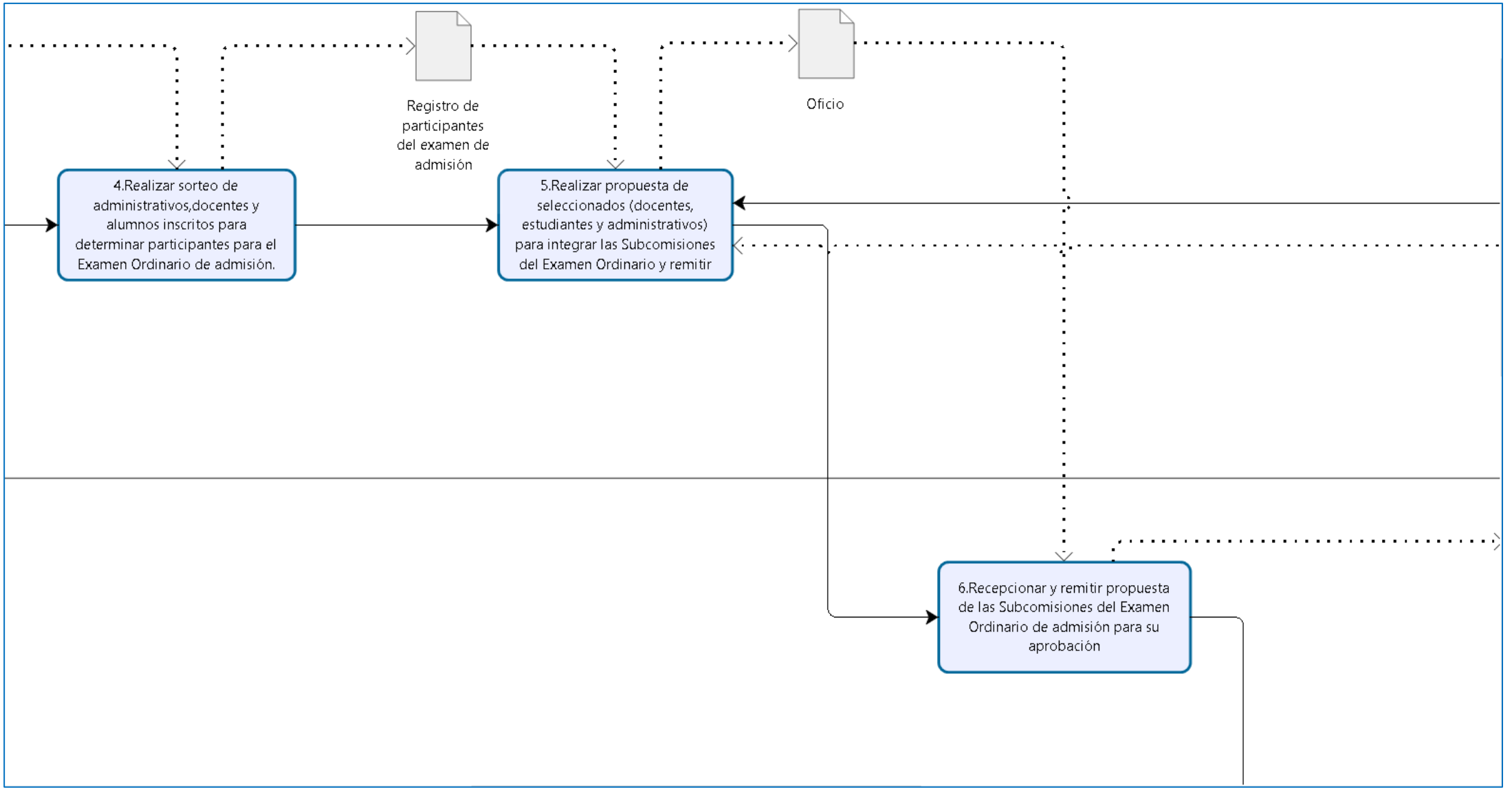


Figura N° 74: PM01.01.04.02 (Parte 2) - Diagrama BPMN 2.0

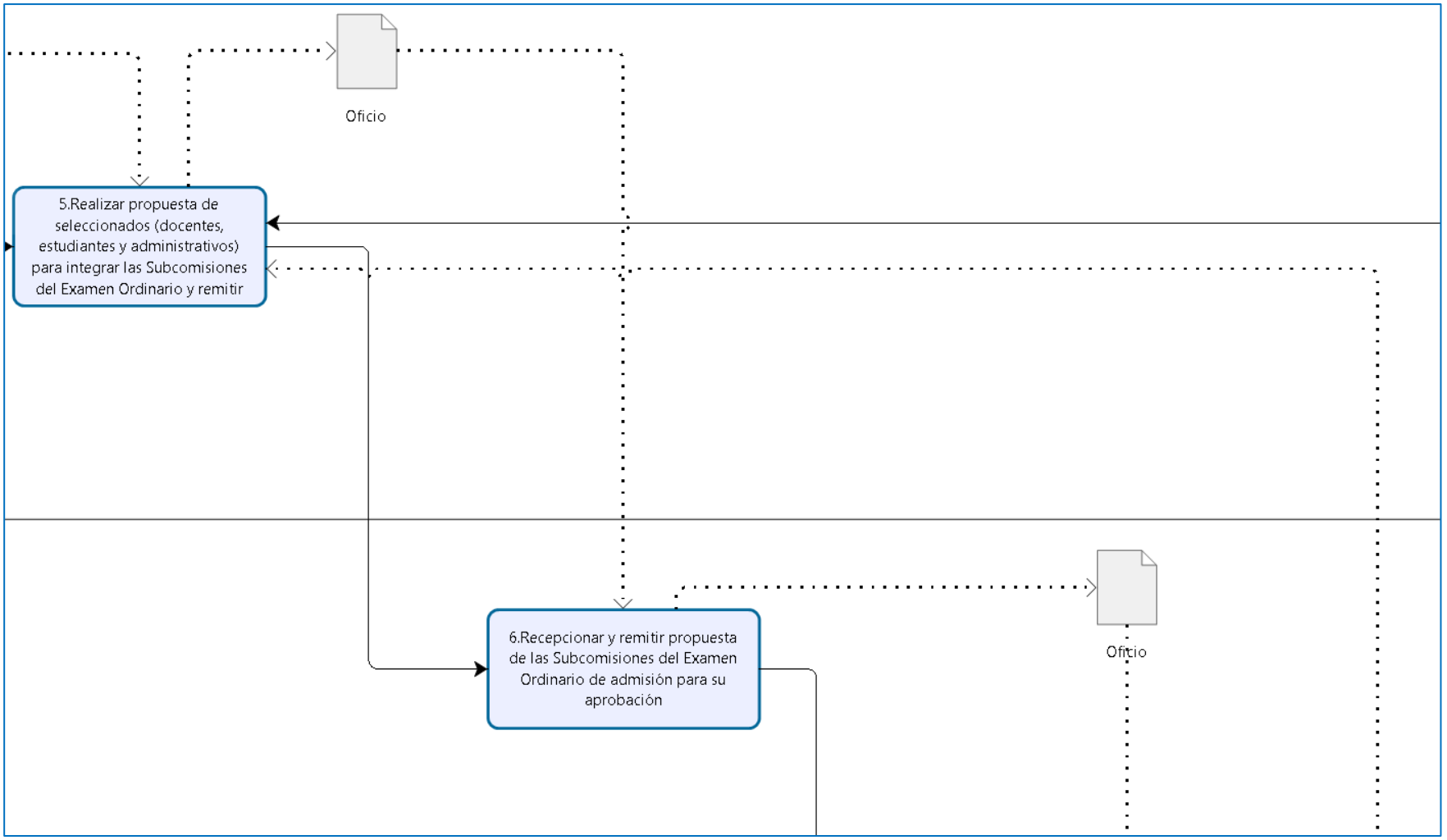


Figura N° 75: PM01.01.04.02 (Parte 3) - Diagrama BPMN 2.0

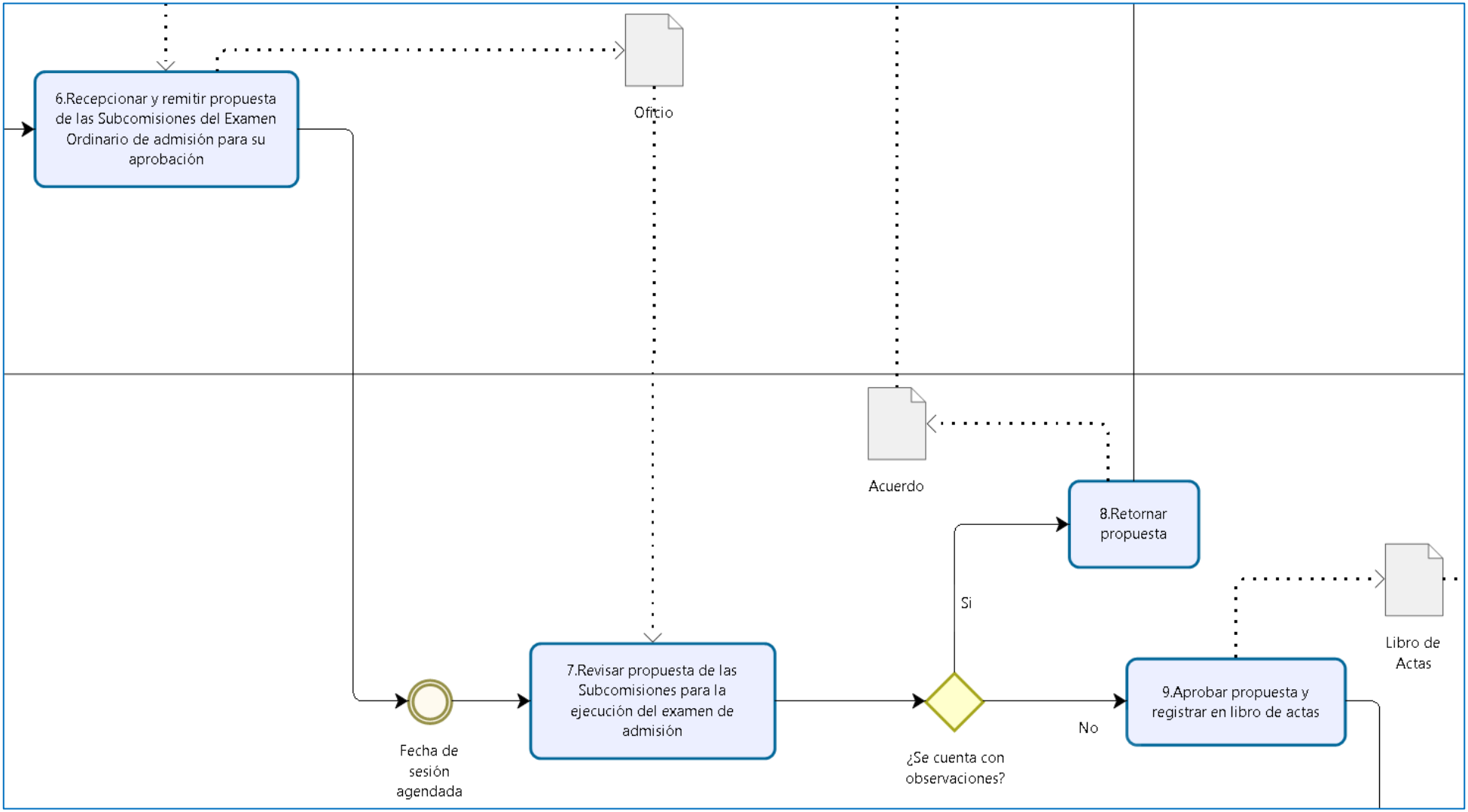


Figura N° 76: PM01.01.04.02 (Parte 4) - Diagrama BPMN 2.0

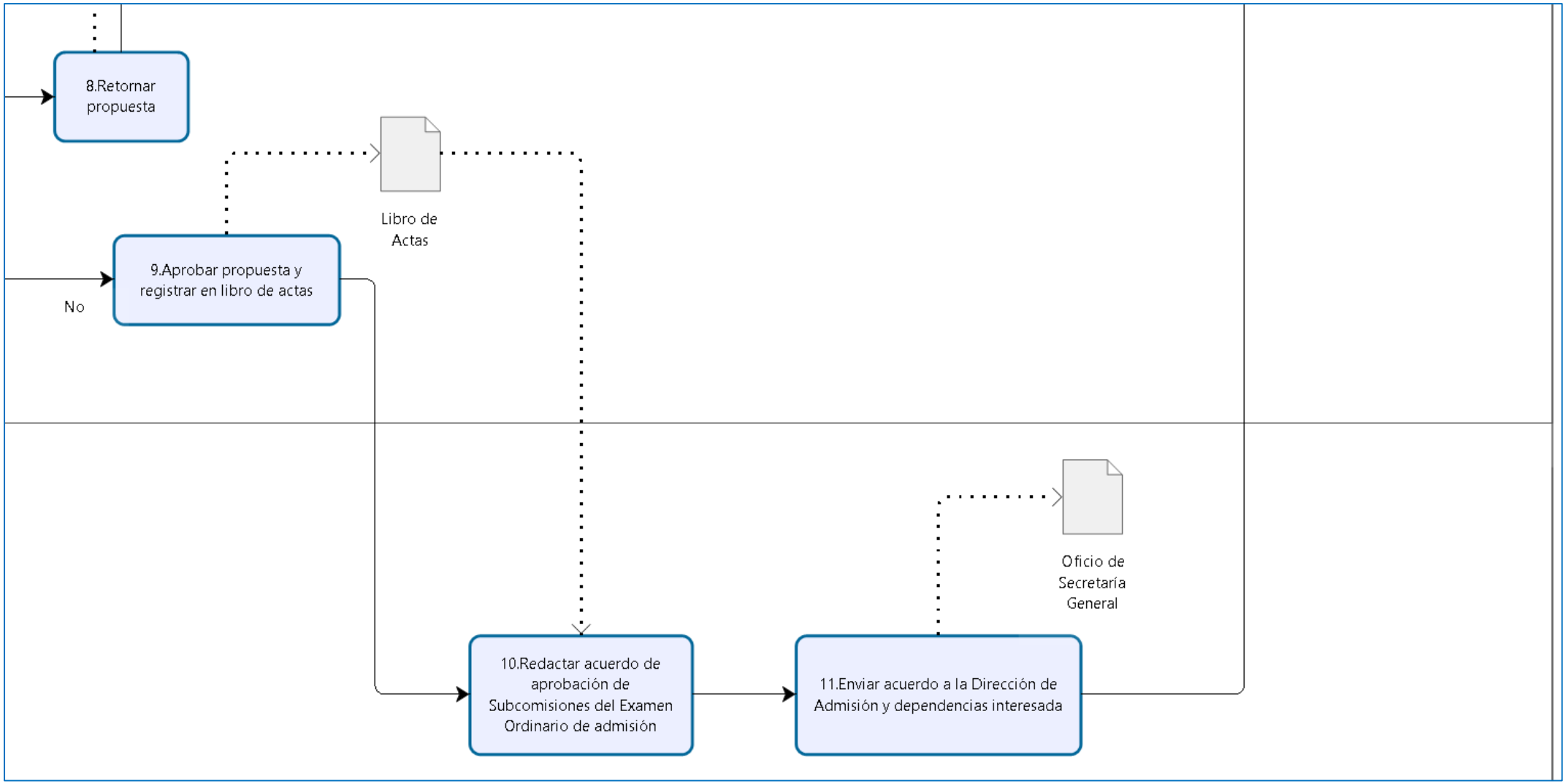


Figura N° 77: PM01.01.04.02 (Parte 5) - Diagrama BPMN 2.0

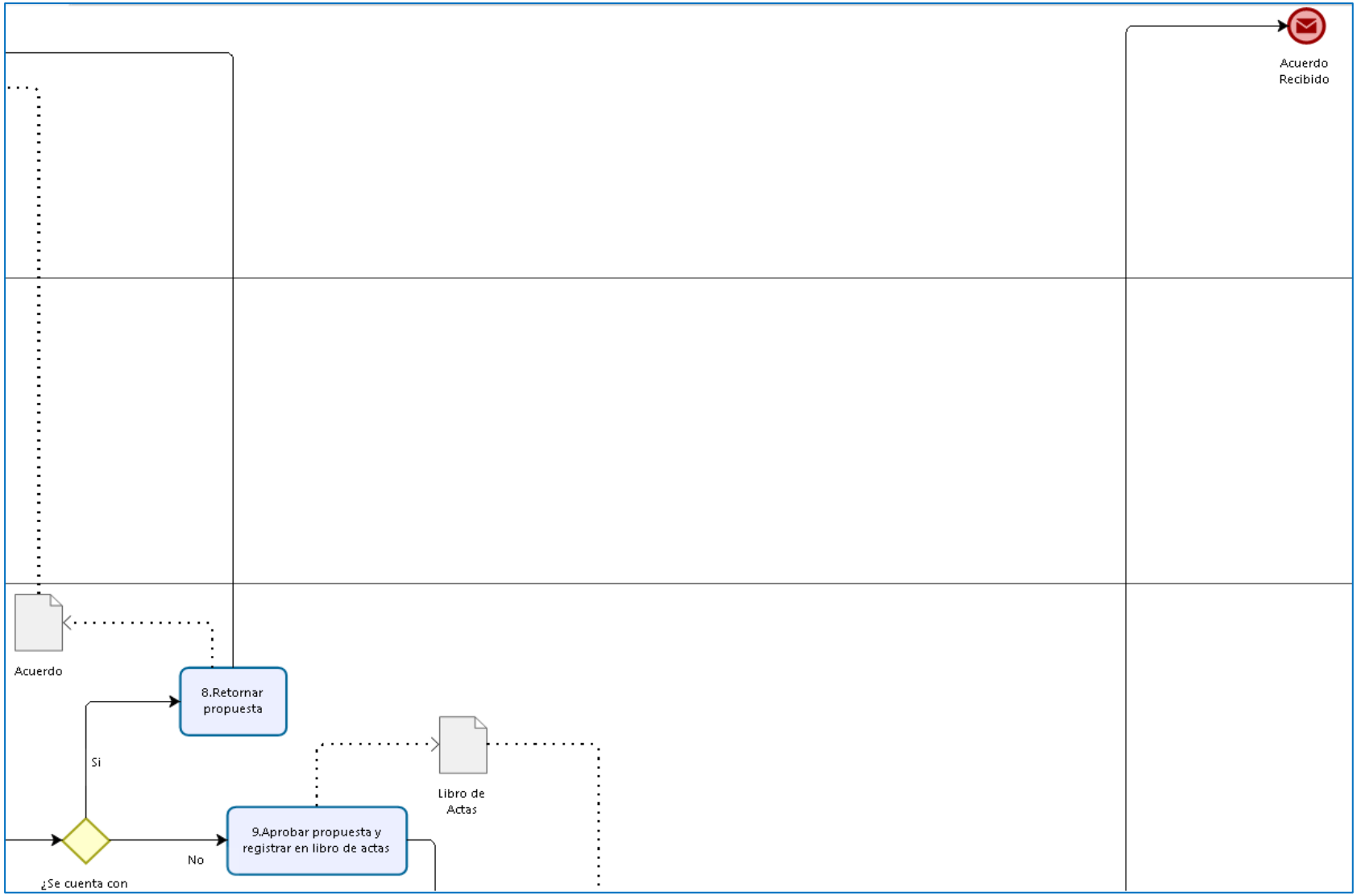


Tabla N° 25: PM01.01.04.03 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.04.03 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.04.Gestión de Exámenes del Proceso de Admisión de Pregrado
TÍTULO:	Elaboración de los Exámenes del Proceso de Admisión		
A. OBJETIVO:	Elaborar los Exámenes del Proceso de Admisión		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF ,Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

	E. DESCRIPCIÓN DEL PROCEDIMIENTO:	**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Convocar a los integrantes de las Subcomisiones.		Dirección de Admisión	Director(a) de Admisión	Oficio, Registro de llamadas
2	Instalar la Subcomisión de Elaboración del Examen a cargo de Vicerrector(a) Académico(a).		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Acta
3	Elaborar y determinar el esquema axial para el examen propuesto.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Esquema Axial
4	Seleccionar al azar de ítems para el examen de acuerdo al esquema axial y canales.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Esquema Axial, Registro de ítems
5	Realizar revisión y corrección de ítems estableciendo un esquema y numeración.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Tarjeta de ítems y solución
6	Realizar digitalización e impresión de ítems.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Tarje de ítems y solución
7	Imprimir exámenes por canal.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Exámenes por Canal
8	Colocar materiales y/o útiles, exámenes, hojas ópticas, padrón de postulantes dentro de una caja lacrada identificada con por canal y aula.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Registro de Hojas Ópticas, Registro de Exámenes por canal
9	Entregar a la Subcomisión de Recepción y Traslado del Examen, las cajas lacradas identificadas por canal y aula.		Dirección de Admisión	Subcomisión de Elaboración del Examen	Formato de Entrega/Recepción
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				

I. ANEXOS:			
ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 78: PM01.01.04.03 - Diagrama BPMN 2.0

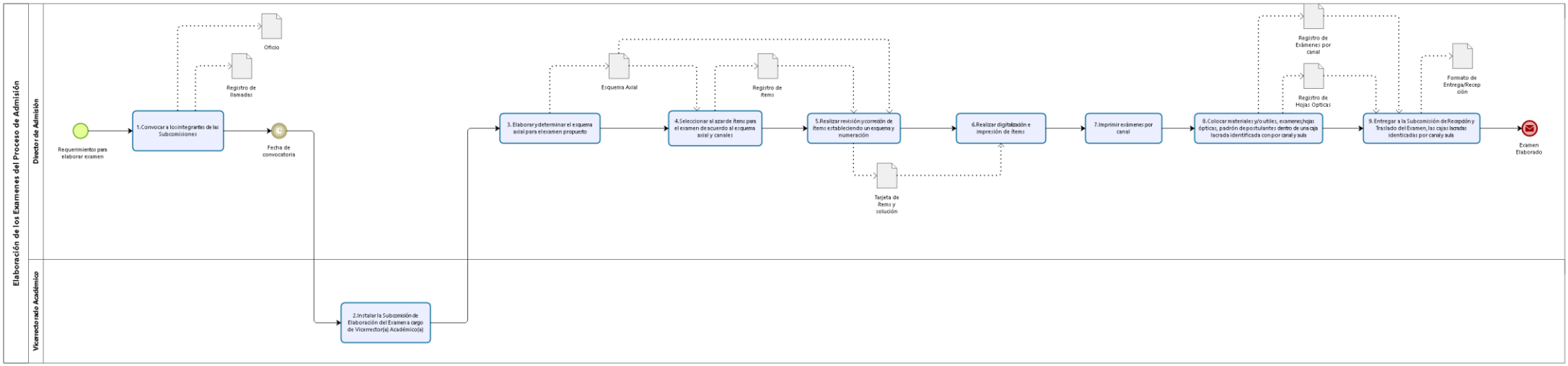


Figura N° 79: PM01.01.04.03 (Parte 1) - Diagrama BPMN 2.0

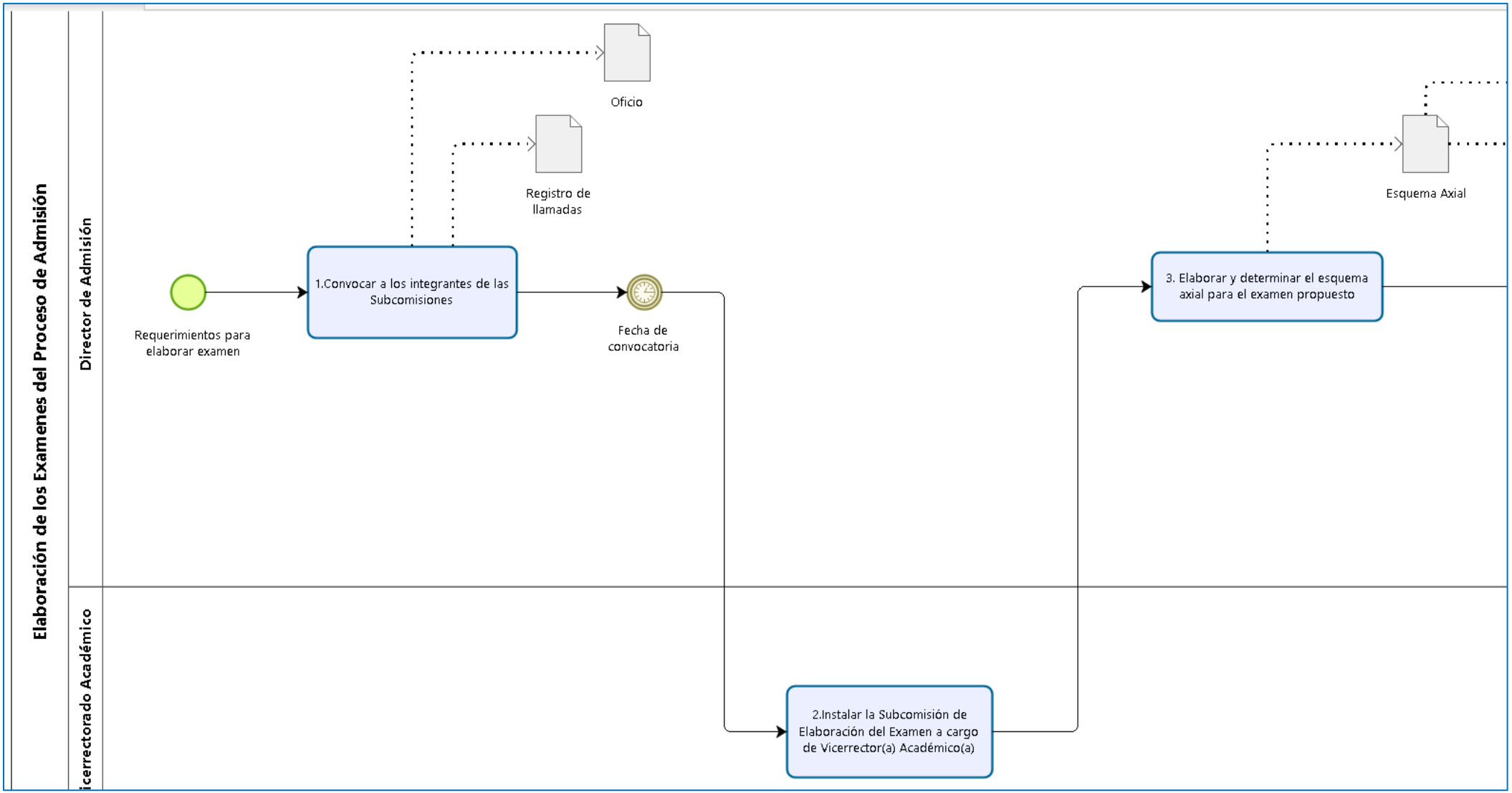


Figura N° 80: PM01.01.04.03 (Parte 2) - Diagrama BPMN 2.0

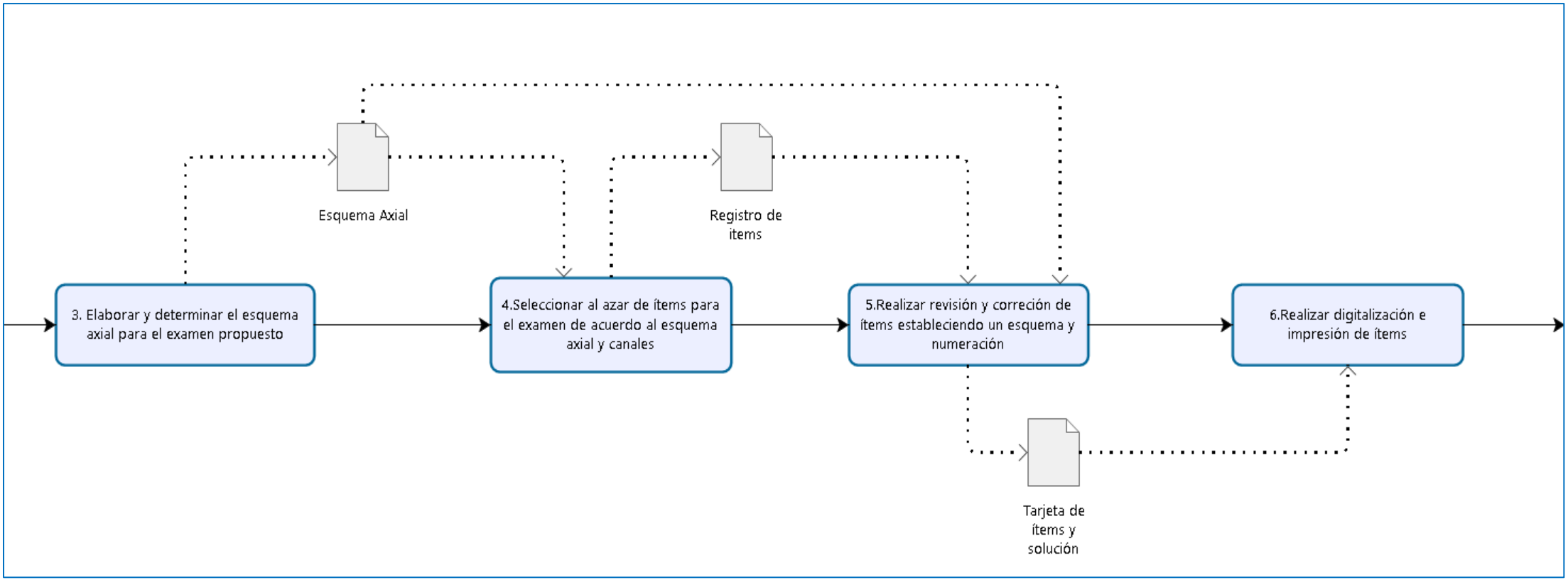


Figura N° 81: PM01.01.04.03 (Parte 3) - Diagrama BPMN 2.0

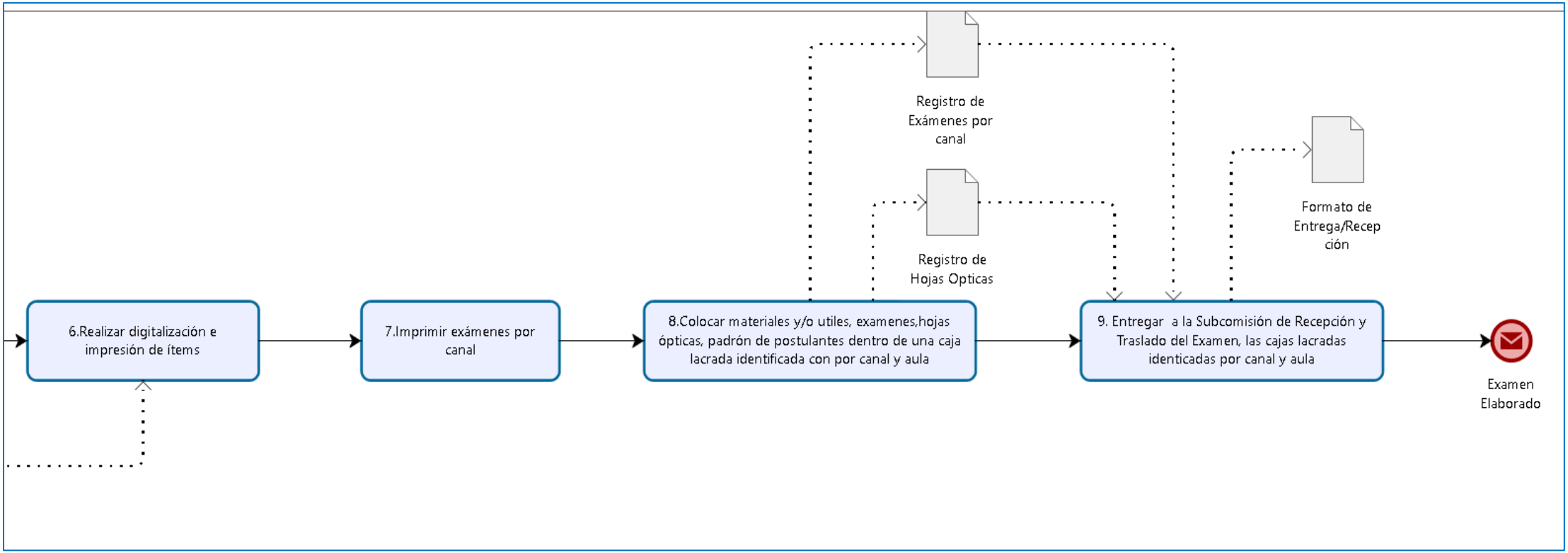


Tabla N° 26: PM01.01.04.04 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.04.04 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.04.Gestión de Exámenes del Proceso de Admisión de Pregrado
TÍTULO:	Aplicación de los Exámenes del Proceso de Admisión (solo se describirá el Examen ordinario)		
A. OBJETIVO:	Aplicar los exámenes del Proceso de Admisión		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF ,Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Controlar ingreso de los postulantes.		Dirección de Admisión	Subcomisión de Ingreso de Postulantes, Subcomisión de Vigilancia y Orden Exterior del Campus Universitario	Registro de carné de postulantes verificados, Registro de ocurrencias
2	Realizar toma de fotografía y de videograbación de la revisión de postulantes.		Dirección de Admisión	Subcomisión de Publicación de Resultados y Premiación	Registro de Videograbación, Registro de imágenes fotográficas
3	Recibir y orientar a los postulantes.		Dirección de Admisión	Subcomisión de Orientación de Postulantes, Subcomisión de Vigilancia del Campus Universitario	Registro de ocurrencias
4	Realizar entrega de caja lacrada con exámenes de admisión a los integrantes de la Subcomisión de Control del Examen.		Dirección de Admisión	Subcomisión de Recepción y Traslado del Examen	Formato de Control
5	Recepcionar caja lacrada, verificar y distribuir material para el desarrollo del examen de admisión y firmar conformidad correspondiente.		Dirección de Admisión	Subcomisión de Control del Examen	Formato de Control, Prueba de admisión por canal de ingreso, Hojas Ópticas de Respuestas, Hojas Ópticas de identificación de postulantes, Padrón de postulantes por aula
6	Verificar el orden y correcto desarrollo del examen de admisión hasta su culminación.		Dirección de Admisión	Subcomisión de Control del Examen	Registro de ocurrencias
7	Realizar entrega de pruebas de admisión, Hojas Ópticas, padrones, empaquetar en caja lacrada y registrar formato de Control.		Dirección de Admisión	Subcomisión de Control del Examen	Prueba de admisión por canal de ingreso, Hojas Ópticas de respuestas de postulantes,

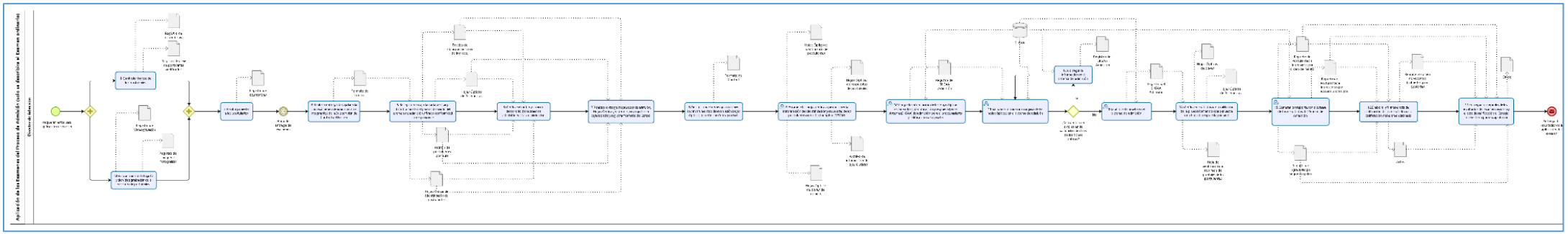
					Hojas Ópticas de identificación de postulantes, Padrón de postulantes por aula, Formato de Control
8	Recepcionar sobres que contienen los instrumentos de evaluación (hojas ópticas, padrón con fotos, pruebas)		Dirección de Admisión	Subcomisión de Calificación del Examen	Formato de Control
9	Escanear las hojas ópticas que contienen la información de identificación y respuestas de los postulantes con el lector óptico OPSCAN.		Dirección de Admisión	Subcomisión de Calificación del Examen	Hojas Ópticas de identificación de postulantes, Hojas Ópticas de respuestas de postulantes, Hojas Ópticas de claves del examen, Archivo de información de Hojas Ópticas (extensión dat)
10	Cargar la información de las Hojas Ópticas escaneadas (identificación y respuestas) en el sistema (SIIGAA) de admisión para el procesamiento y calificación de la prueba.		Dirección de Admisión	Subcomisión de Calificación del Examen	Archivo de información de Hojas Ópticas (extensión dat), Registro del SIIGAA Admisión
11	Validar la información cargada de las hojas ópticas en el sistema de admisión.		Dirección de Admisión	Subcomisión de Calificación del Examen	Registro del SIIGAA Admisión
	Si existen errores en la validación de datos de las fichas ópticas continuar, caso contrario ir al paso 14.		Dirección de Admisión	Subcomisión de Calificación del Examen	
12	Corregir la información en el sistema de admisión, ir al paso 11.		Dirección de Admisión	Subcomisión de Calificación del Examen	Registro del SIIGAA Admisión
13	Calificar la prueba en el sistema de admisión.		Dirección de Admisión	Subcomisión de Calificación del Examen	Registro del SIIGAA Admisión
14	Verificar resultados de la calificación de la prueba tomando como muestra una hoja de respuesta por canal.		Dirección de Admisión	Subcomisión de Calificación del Examen	Hojas Ópticas de claves, Hojas Ópticas de Respuestas, Hoja de verificación con resumen de puntajes de los postulantes
15	Generar los reportes en el sistema de los resultados del Proceso de Admisión.		Dirección de Admisión	Subcomisión de Calificación del Examen	Reporte de Postulantes e ingresantes por orden de mérito, Reporte de Postulantes e ingresantes por escuela profesional, Reporte de ingresantes por segunda opción

16	Elaborar y firmar el acta de calificación de los resultados de la calificación del examen ordinario.		Dirección de Admisión	Subcomisión de Calificación del Examen	Reporte de Postulantes e ingresantes por orden de mérito, Reporte de Postulantes e ingresantes por escuela profesional, Reporte de ingresantes por segunda opción, Reporte resumen de vacantes (cubiertas y no cubiertas), Actas
17	Entregar los reportes de los resultados del examen ordinario y el acta de calificación al Consejo Universitario para su aprobación.		Dirección de Admisión	Subcomisión de Calificación del Examen	Oficio, Reporte de Postulantes e ingresantes por orden de mérito, Reporte de Postulantes e ingresantes por escuela profesional, Reporte de ingresantes por segunda opción, Reporte resumen de vacantes (cubiertas y no cubiertas), Actas
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 82: PM01.01.04.04 (General) - Diagrama BPMN 2.0



v

Figura N° 83: PM01.01.04.04 (Parte 1) - Diagrama BPMN 2.0

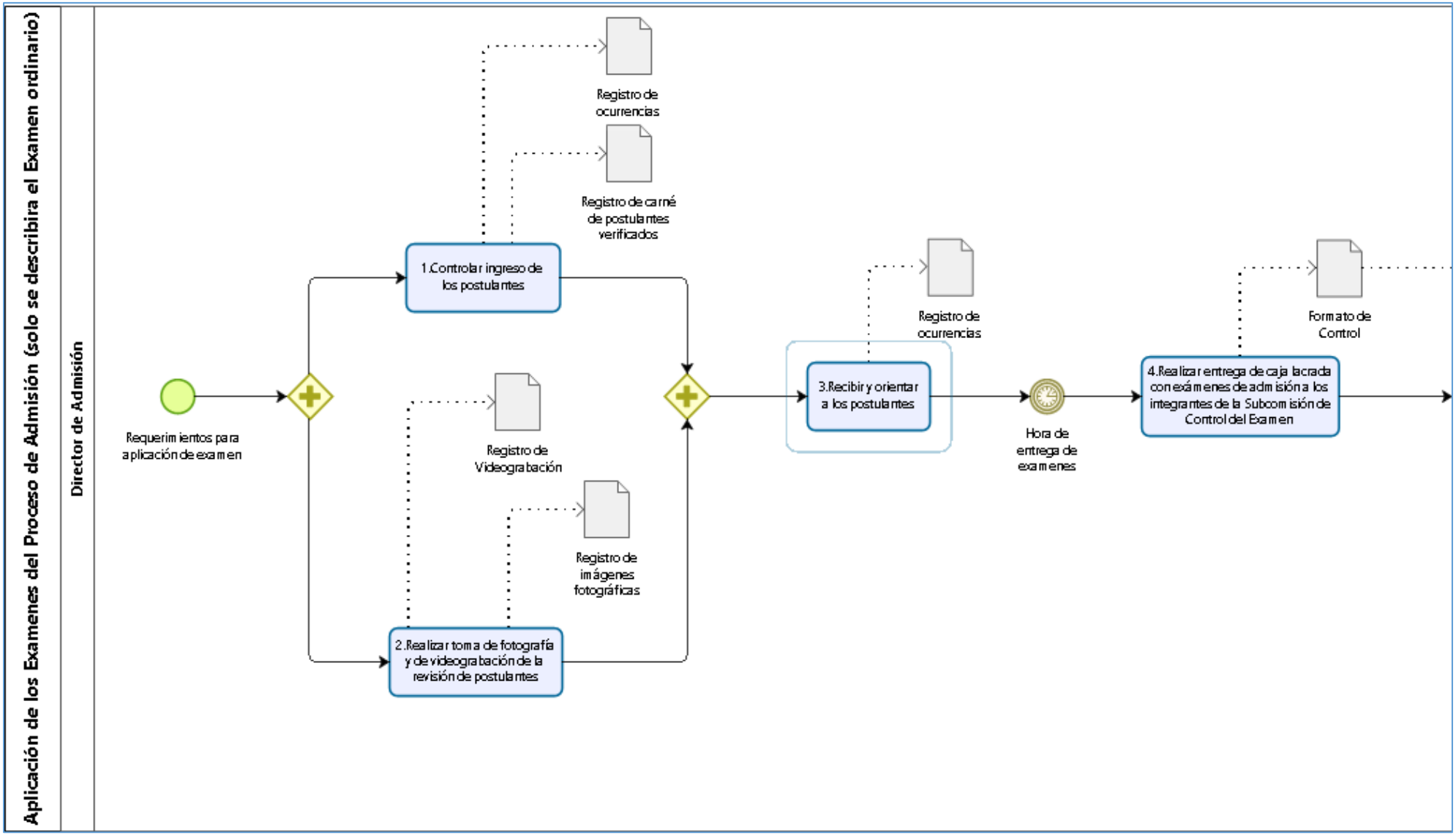


Figura N° 84: PM01.01.04.04 (Parte 2) - Diagrama BPMN 2.0

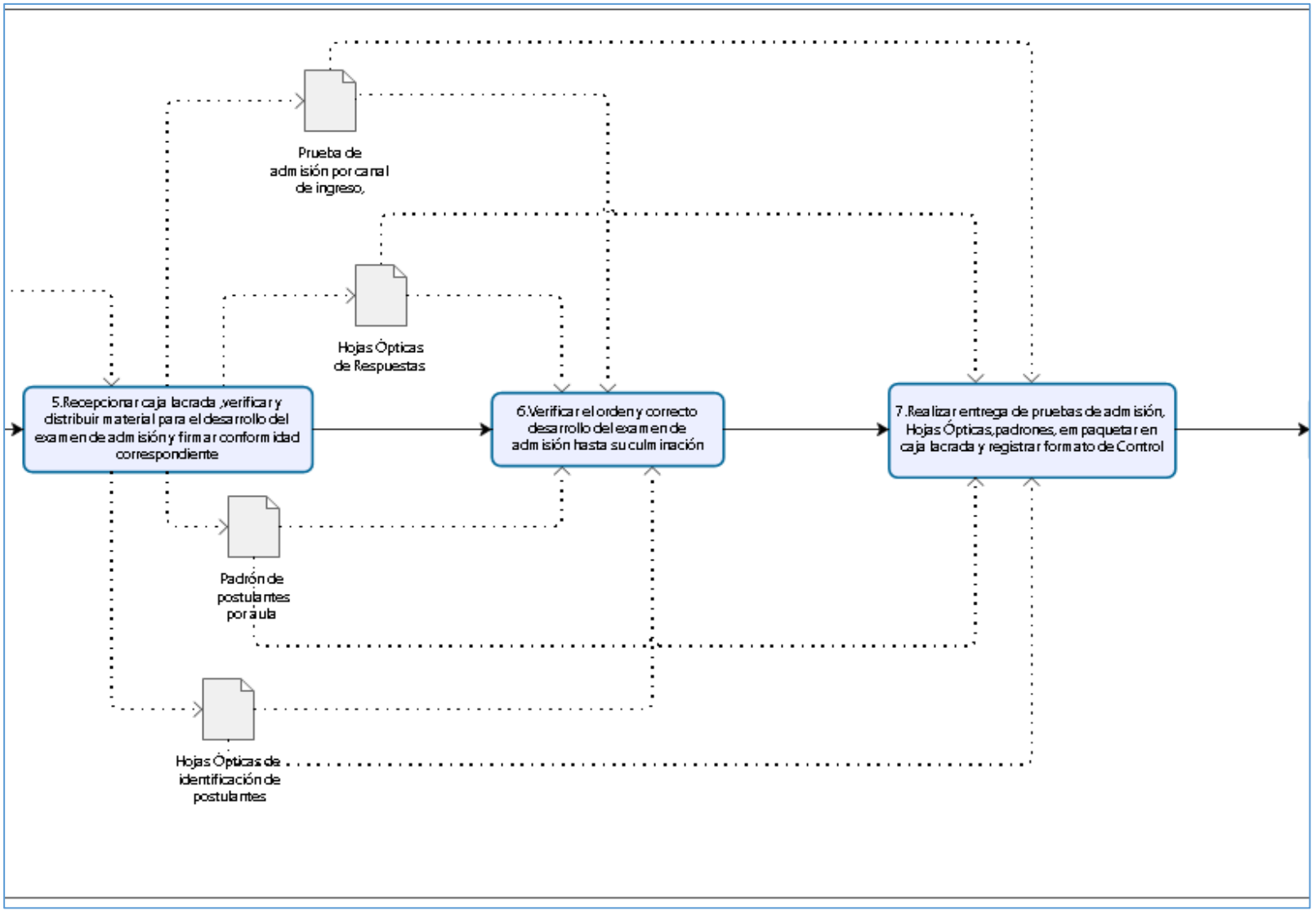


Figura N° 85: PM01.01.04.04 (Parte 3) - Diagrama BPMN 2.0

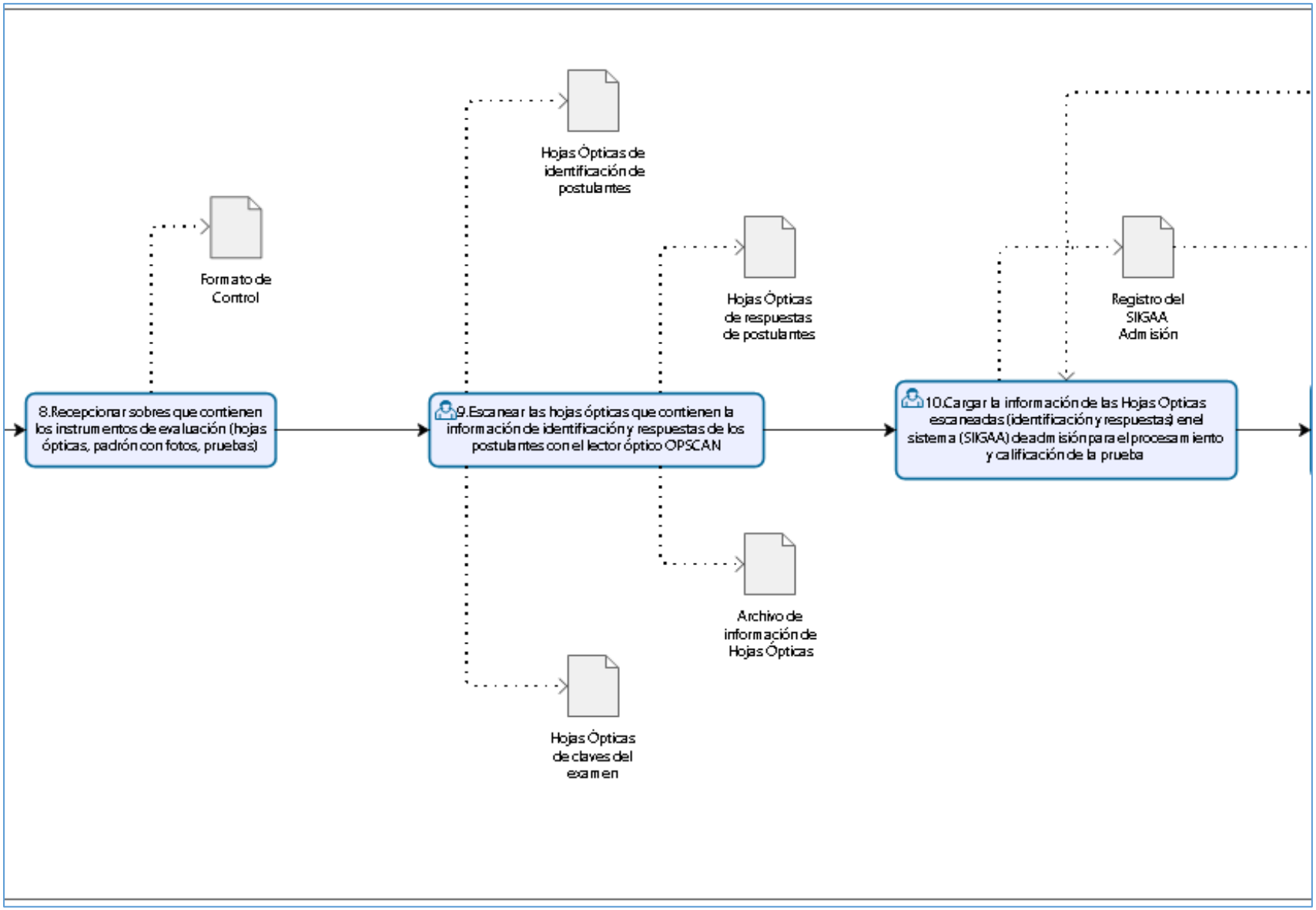


Figura N° 86: PM01.01.04.04 (Parte 4) - Diagrama BPMN 2.0

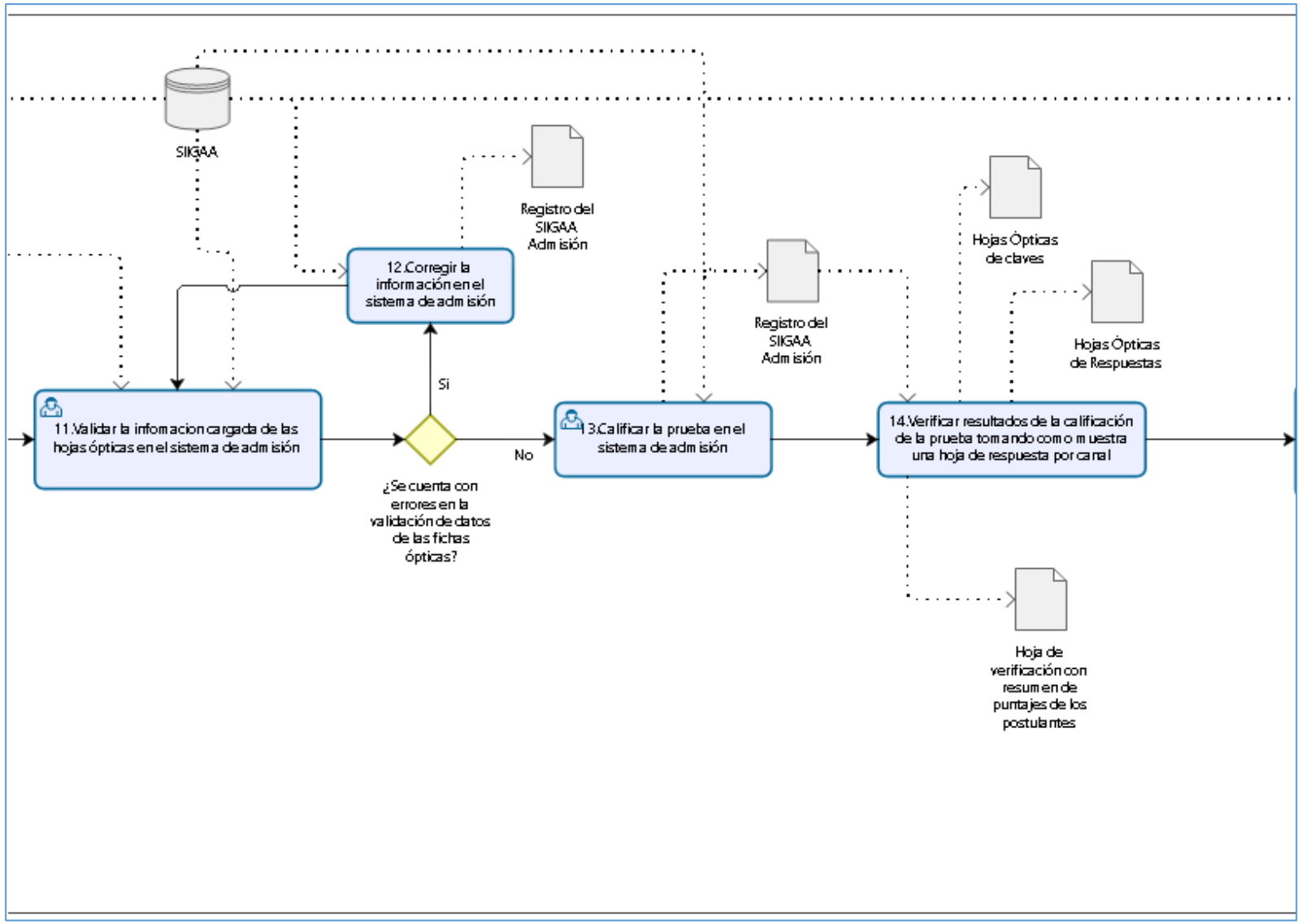


Figura N° 87: PM01.01.04.04 (Parte 5) - Diagrama BPMN 2.0

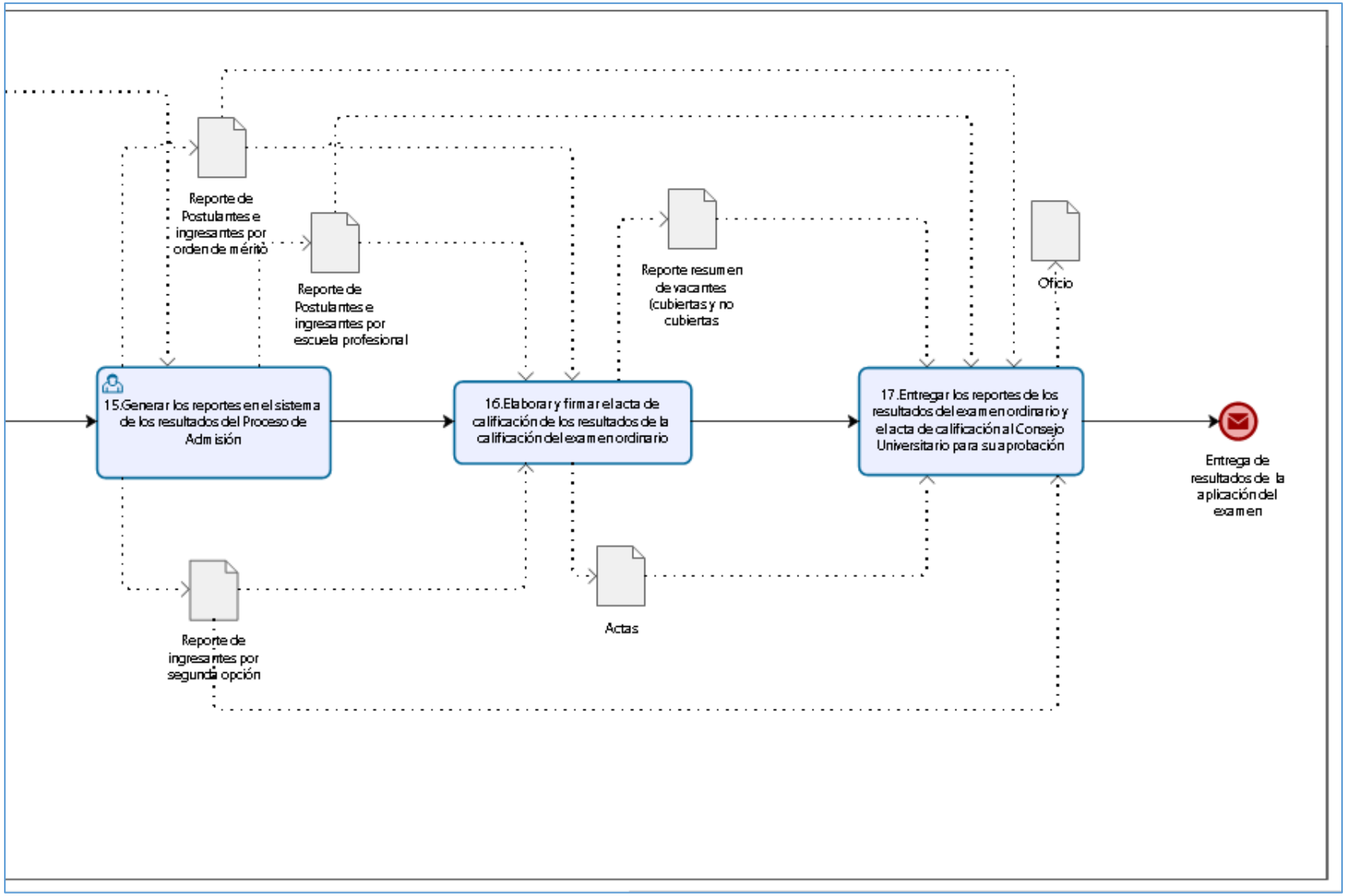


Tabla N° 27: PM01.01.04.05 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.04.05 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.04.Gestión de Exámenes del Proceso de Admisión de Pregrado
TÍTULO:	Aprobación y Publicación de resultados del Proceso de Admisión		
A. OBJETIVO:	Aprobar y publicar los resultados de los postulantes a las carreras profesionales de Pregrado		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Verificar, aprobar y visar los resultados del Proceso de Admisión.		Consejo Universitario	Consejo Universitario	Libro de actas de Sesión de Consejo Universitario, Reporte visado de Postulantes e ingresantes por orden de mérito, Reporte visado de Postulantes e ingresantes por escuela profesional, Reporte visado de ingresantes por segunda opción, Reporte visado de resumen de vacantes (cubiertas y no cubiertas)
2	Solicitar la publicación de los resultados aprobados del Proceso de Admisión.		Consejo Universitario	Consejo Universitario	Oficio
3	Realizar publicación de resultados del Proceso de Admisión en el portal web institucional, redes sociales y en los murales de la puerta de ingreso del campus universitario.		Dirección de Admisión	Subcomisión de Publicación de Resultados y Premiación	Reporte visado de Postulantes e ingresantes por orden de mérito en el mural, Reporte visado de Postulantes e ingresantes por escuela profesional en el mural, Reporte visado de ingresantes por segunda opción de mérito en el mural, Registro en Portal Web, Registro en redes sociales institucionales

4	Redactar resolución de aprobación de los resultados del Proceso de Admisión de las Carreras Profesionales de Pregrado de la UNS		Secretaría General	Secretario(a) General	Registro de Resoluciones, Reporte visado de Postulantes e ingresantes por orden de mérito, Reporte visado de Postulantes e ingresantes por escuela profesional, Reporte visado de ingresantes por segunda opción, Reporte visado de resumen de vacantes (cubiertas y no cubiertas)
5	Enviar resolución a la Dirección de Admisión y dependencias interesadas.		Secretaría General	Secretario(a) General	Resolución de Consejo Universitario
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo:			
Revisado por:			
Cargo:			
Aprobado por:			
Cargo:			

Figura N° 88: PM01.01.04.05 - Diagrama BPMN 2.0

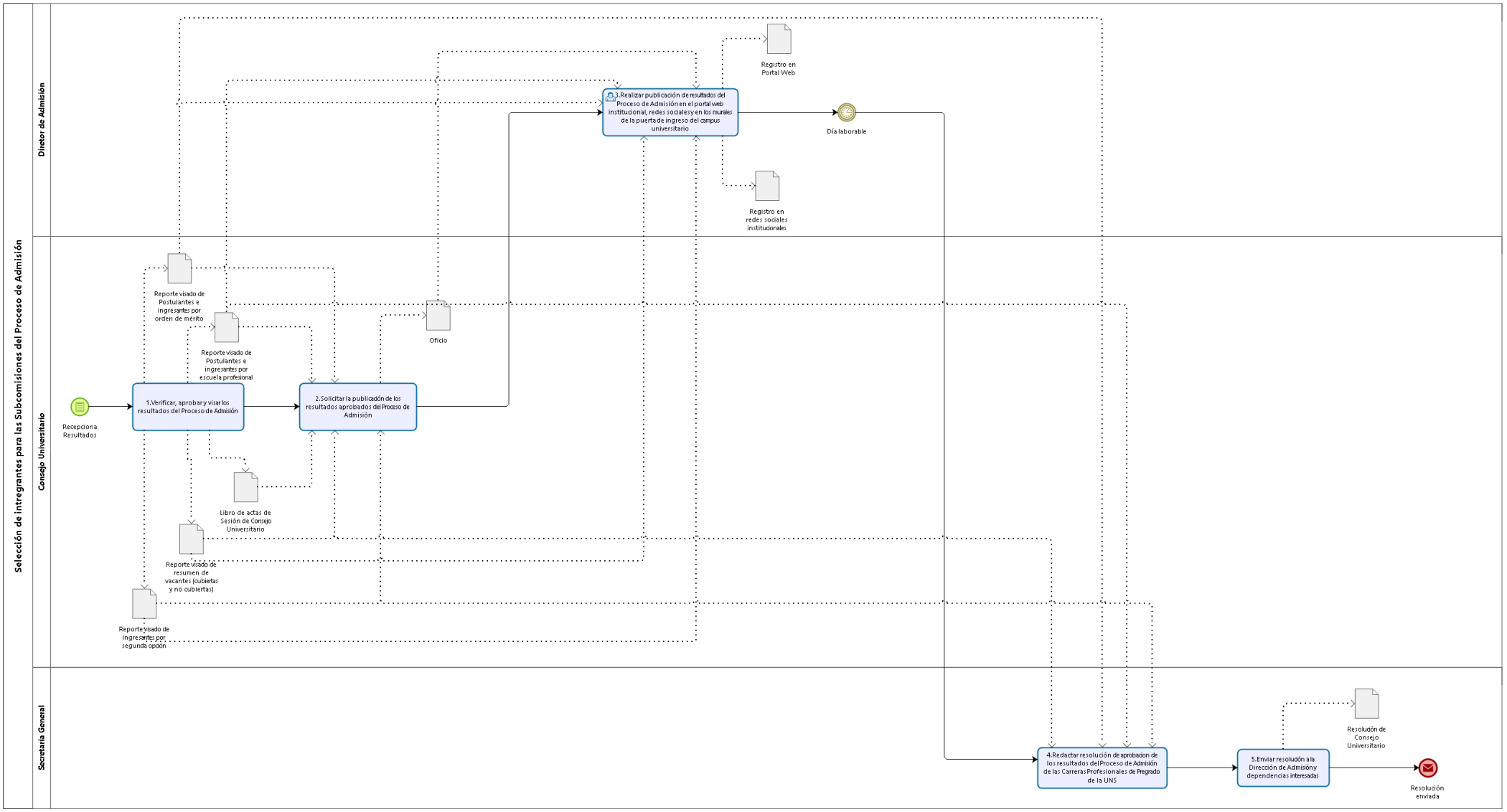


Figura N° 89: PM01.01.04.05 (Parte 1) - Diagrama BPMN 2.0

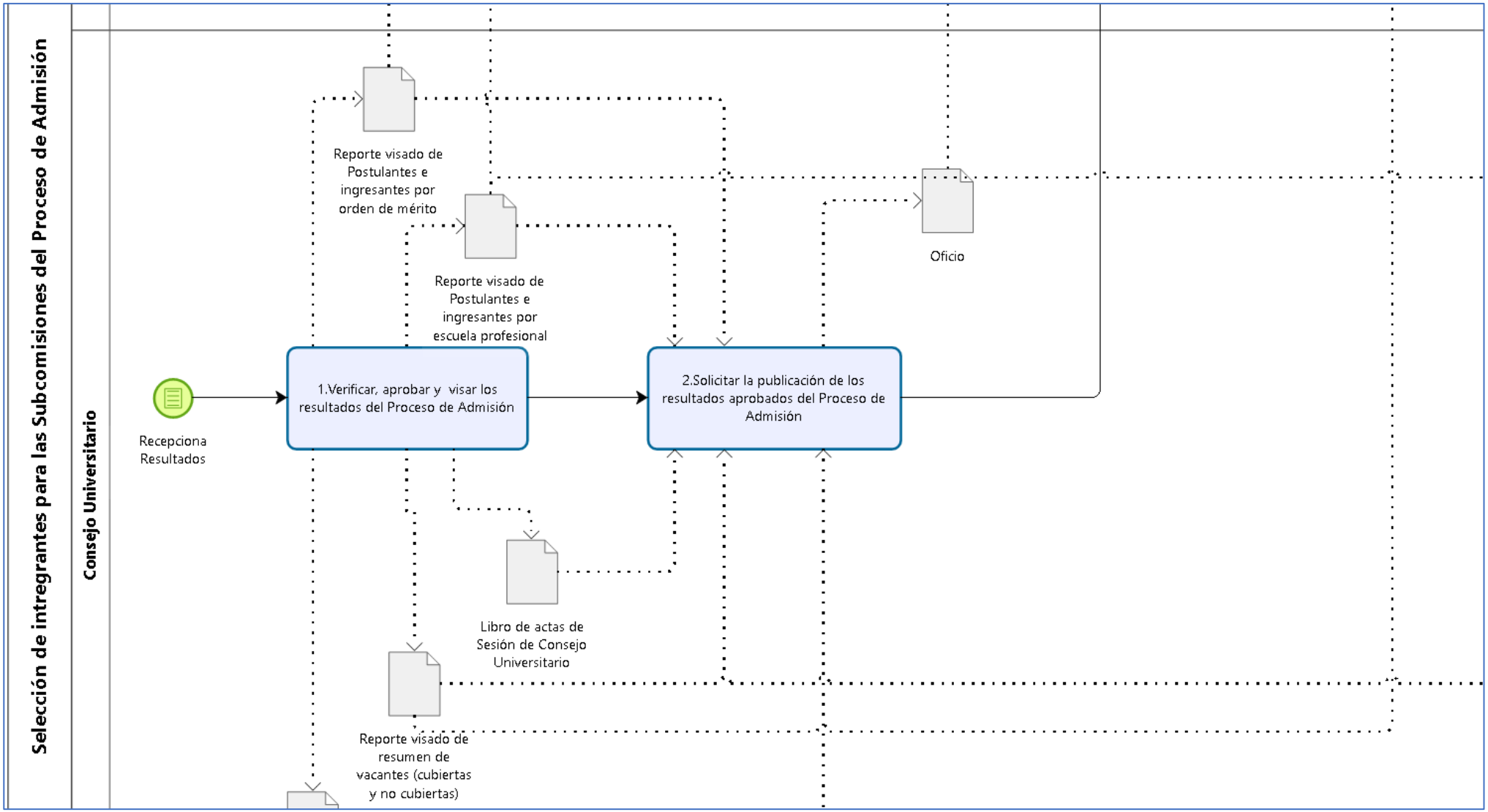


Figura N° 90: PM01.01.04.05 (Parte 2) - Diagrama BPMN 2.0

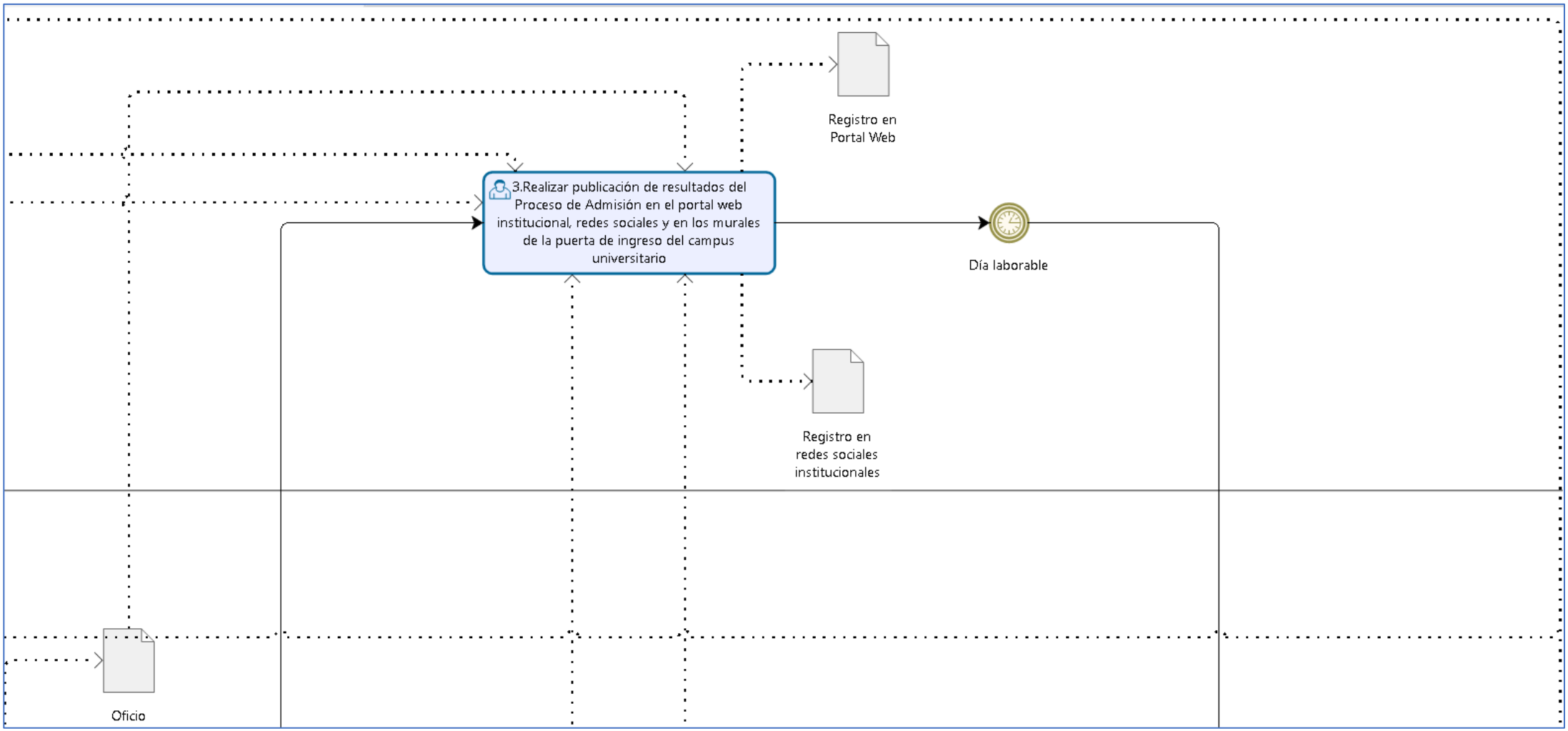


Figura N° 91: PM01.01.04.05 (Parte 3) - Diagrama BPMN 2.0

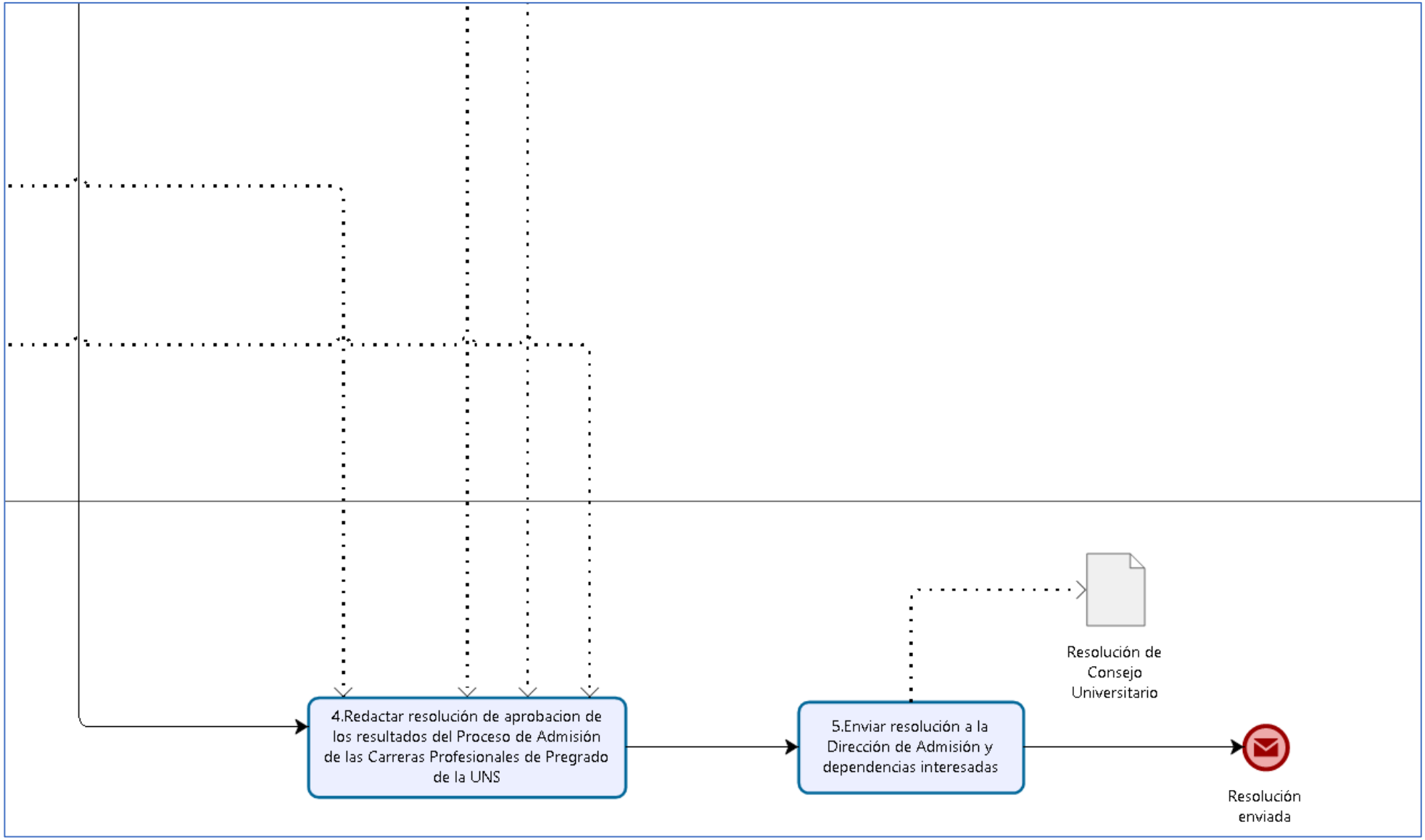


Tabla N° 28: PM01.01.05 - Ficha de Proceso

	FICHA DE PROCESO DE NIVEL 2					**Código:** PM01.01.05 **Versión:** 1.0
I. DATOS GENERALES DEL PROCESO						
1. NOMBRE DEL PROCESO	Acreditación de ingresantes a las Carreras Profesionales de Pregrado		**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Proceso de Admisión de Programas de Pregrado	
2. OBJETIVO DEL PROCESO	Hacer entrega de constancia de acreditación de ingreso a la Universidad					
4. DUEÑO DEL PROCESO	Director de Admisión		**5. LÍMITES DEL PROCESO**	**INICIO**	Presentación de requisitos para acreditación de los ingresantes	
				FIN	Culmina con la presentación del informe de constancias de ingreso	
II. DESCRIPCIÓN DEL PROCESO						
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**		**9. CONTROLES APLICADOS**	**10. PRODUCTOS**	**11. CLIENTES**
Dirección de Admisión	Registros de Ingresantes	**PM01.01.05.01.Elaboración y validación de constancias de ingresantes**		Se verifica y valida las constancias de ingresantes	Constancias de Ingresantes	Dirección de Admisión
Ingresante	Requisitos documentarios especificados en el Reglamento de Admisión tales como: DNI, Certificado de estudios original, Acta de nacimiento original, Voucher de Pago por acreditación de ingreso	**PM01.01.05.02.Presentación y validación de requisitos de ingresantes**		Se verifica los requisitos y se realiza la entrega de constancia y el ingresante acreditado firma el registro de entrega	Registro de Constancias de Ingresantes	Dirección de Admisión
Dirección de Admisión	Registro de Constancias de Ingresantes firmados	**PM01.01.05.03.Entrega de informe de constancias de ingreso**		Se verifica y contabiliza los registros y las incidencias que se presentaron renuncias entre otros	Informe de entrega de constancias de ingreso	Dirección de Admisión Vicerrectorado Académico
III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO						
12. TIPO	**13. DESCRIPCIÓN**					
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica, 1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas.					
	Infraestructura: Oficinas, PCs, Scanner Óptico, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).					
	Material: Material de Oficina					
IV. DOCUMENTACIÓN DEL PROCESO						
14. REGISTROS DEL PROCESO				**15. REFERENCIAS DOCUMENTALES**		
1. Registro de Constancias de Ingresantes				1. Ley Universitaria 30220		
				2. Estatuto		
				3. Reglamento General		
				4. Plan Operativo Institucional		
				5. Reglamento de Organización y Funciones		
				6. Manual de Organización y Funciones		
				7. Reglamento para Pago de Subvenciones al Personal		
				8. Reglamento de Admisión		

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 92: PM01.01.05 (General) - Diagrama BPMN 2.0

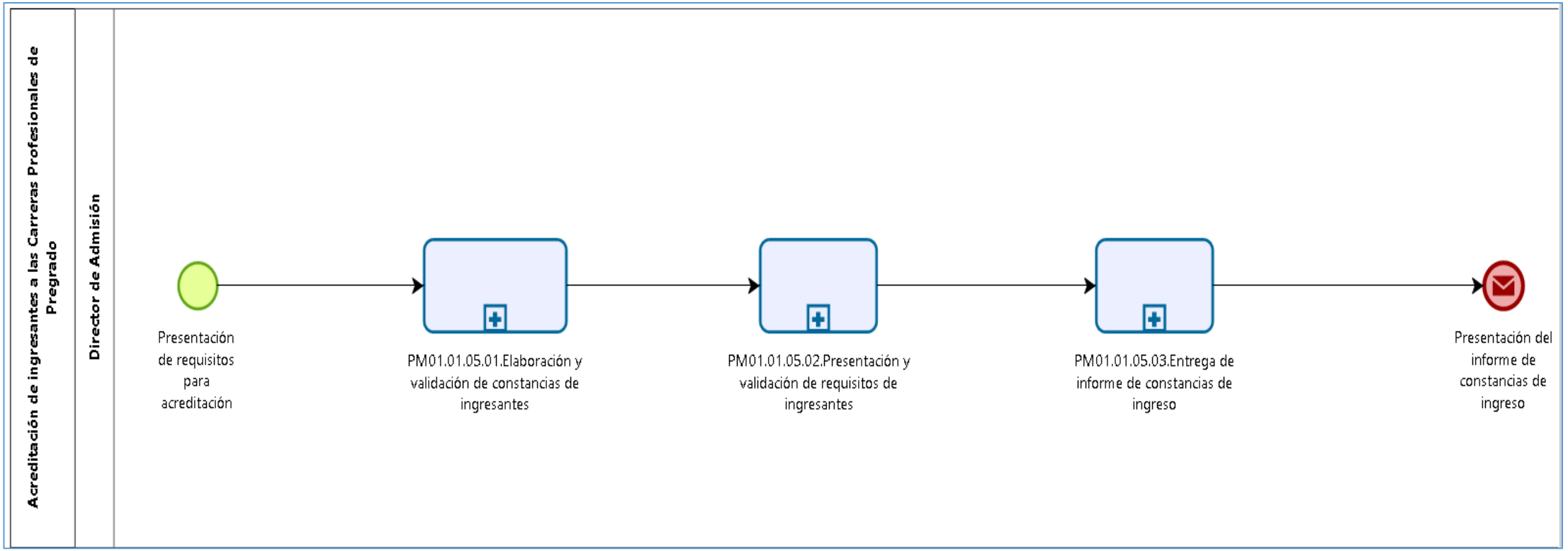


Figura N° 93: PM01.01.05 (Parte 1) - Diagrama BPMN 2.0

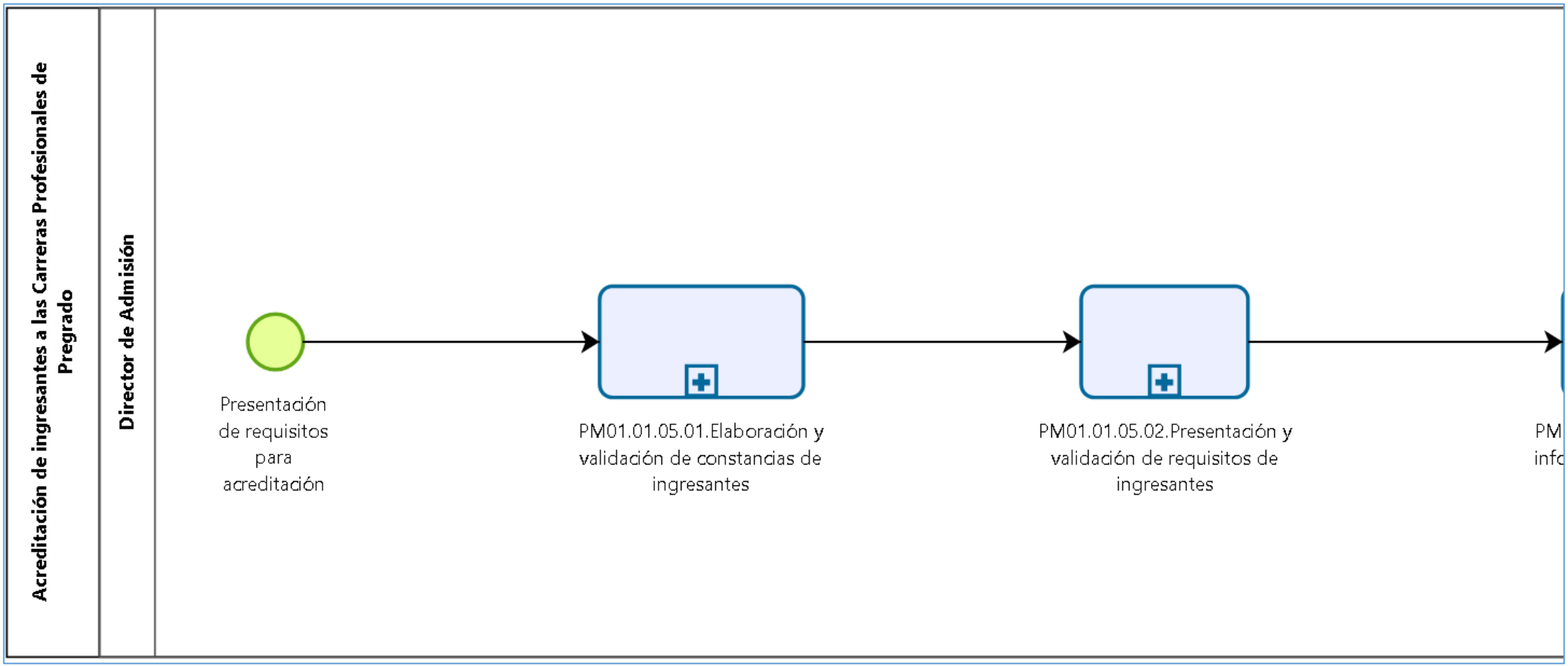


Figura N° 94: PM01.01.05 (Parte 2) - Diagrama BPMN 2.0

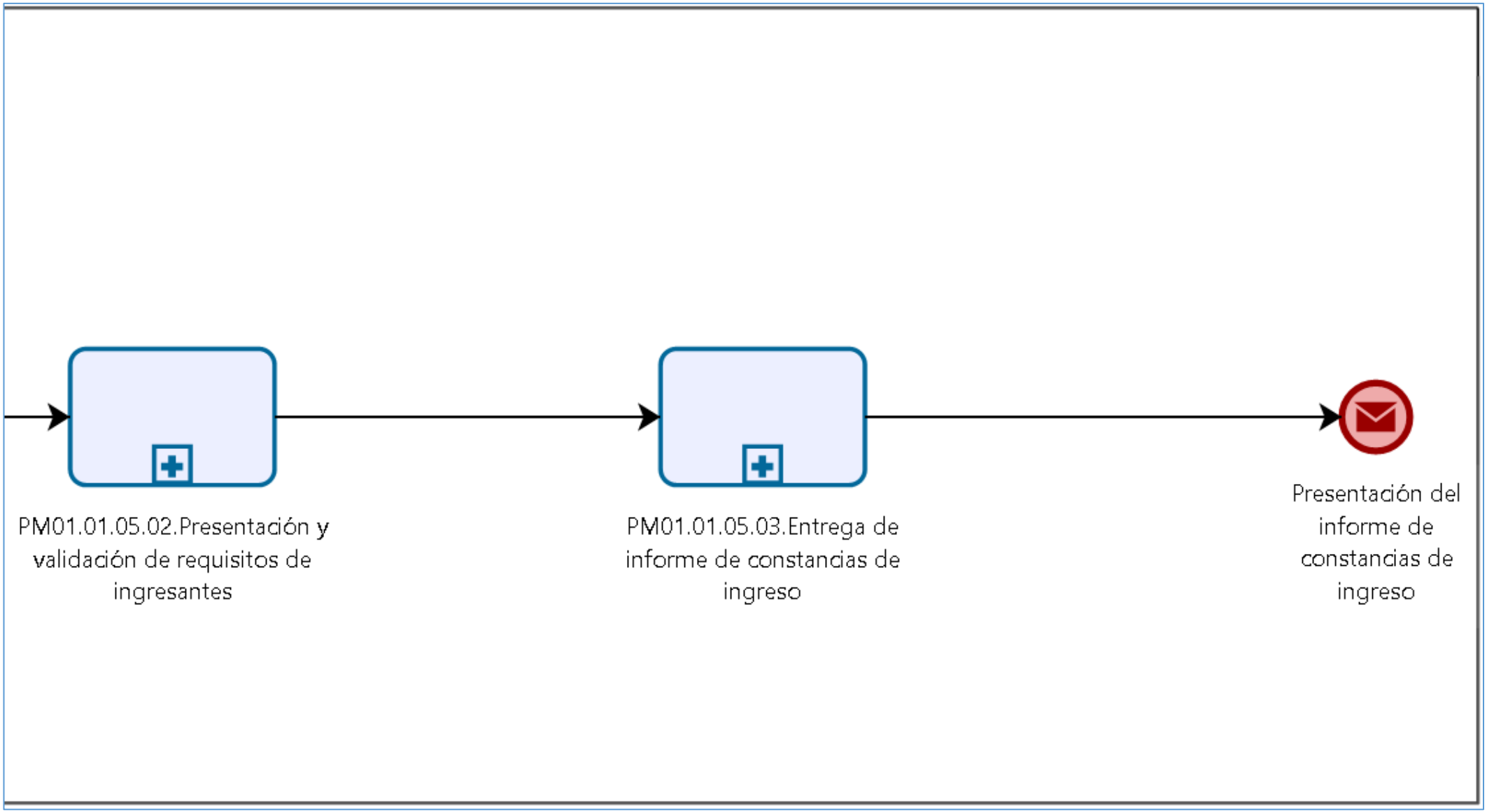


Tabla N° 29: PM01.01.05.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.05.01 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.05.Acreditación de ingresantes a las Carreras Profesionales de Pregrado
TÍTULO:	Elaboración y visado de constancias de ingresantes		
A. OBJETIVO:	Elaborar y visar las constancias de ingresantes a las Escuelas Profesionales		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Realizar la emisión de los reportes de constancias de ingresantes por Escuela Profesional en el Sistema (SIIGAA) de Admisión y remitir al Director de Admisión.		Dirección de Admisión	Especialista de Sistemas	Registro del SIIGAA Admisión, Constancias de Ingresantes, Oficio
2	Recepcionar, verificar, visar y retornar constancias de ingresantes por Escuela Profesional a Especialista.		Dirección de Admisión	Director de Admisión	Constancias de Ingresantes visadas, Oficio
3	Recepcionar constancias de ingresantes por Escuela Profesional visadas.		Dirección de Admisión	Especialista de Sistemas	Constancias de Ingresantes visadas, Oficio
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 95: PM01.01.05.01 - Diagrama BPMN 2.0

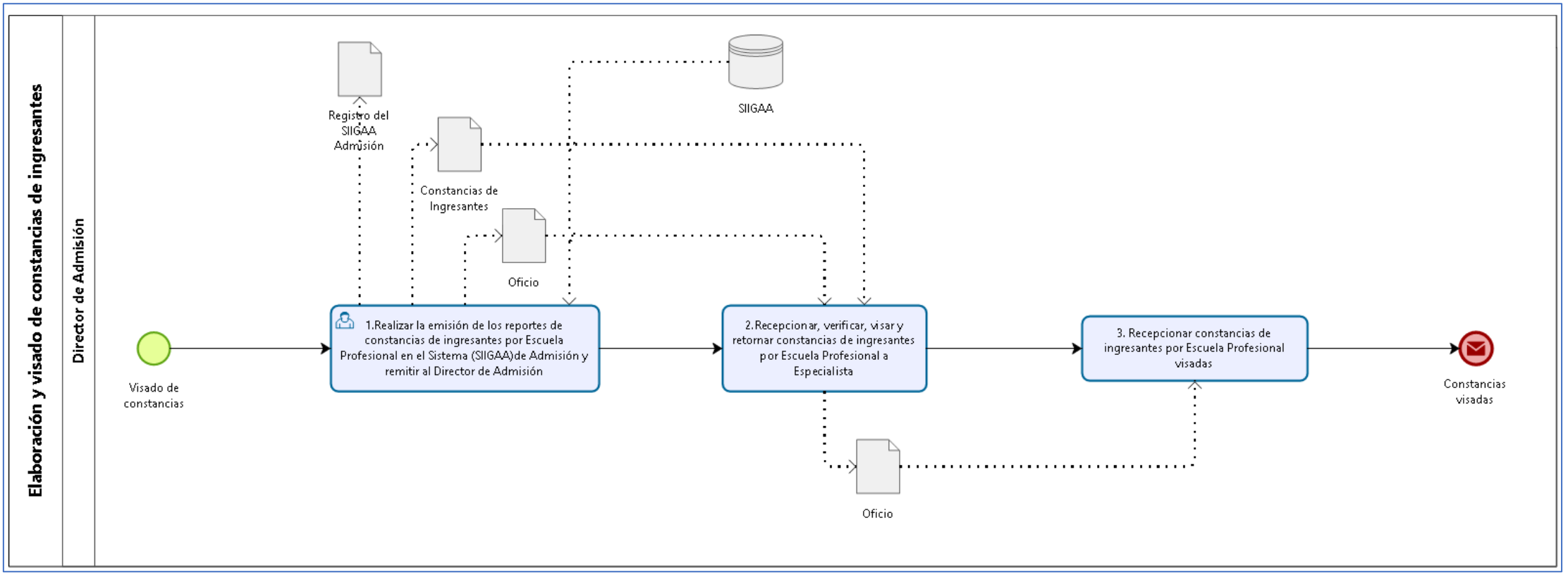


Figura N° 96: PM01.01.05.01 (Parte 1) - Diagrama BPMN 2.0

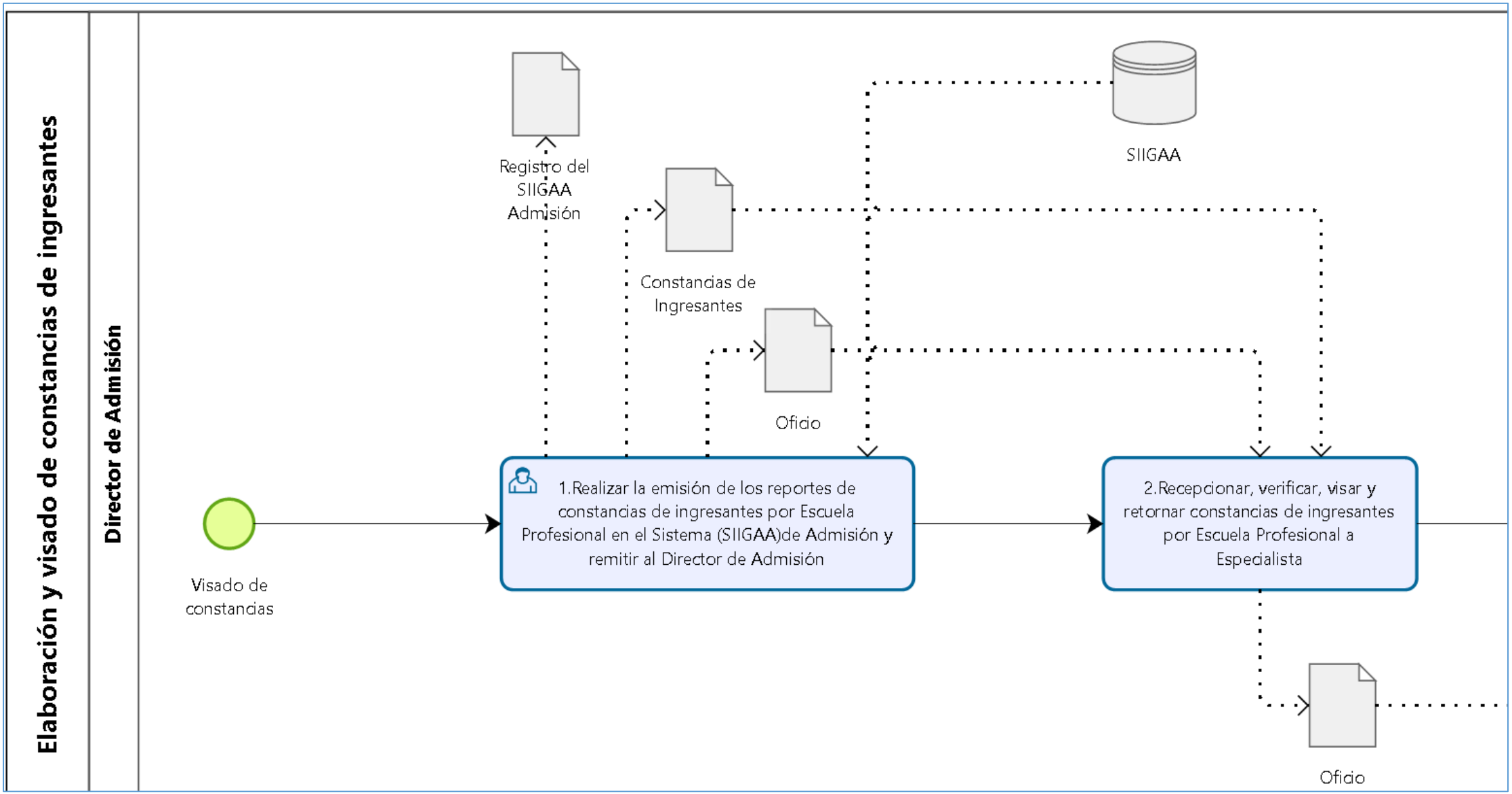


Figura N° 97: PM01.01.05.01 (Parte 2) - Diagrama BPMN 2.0

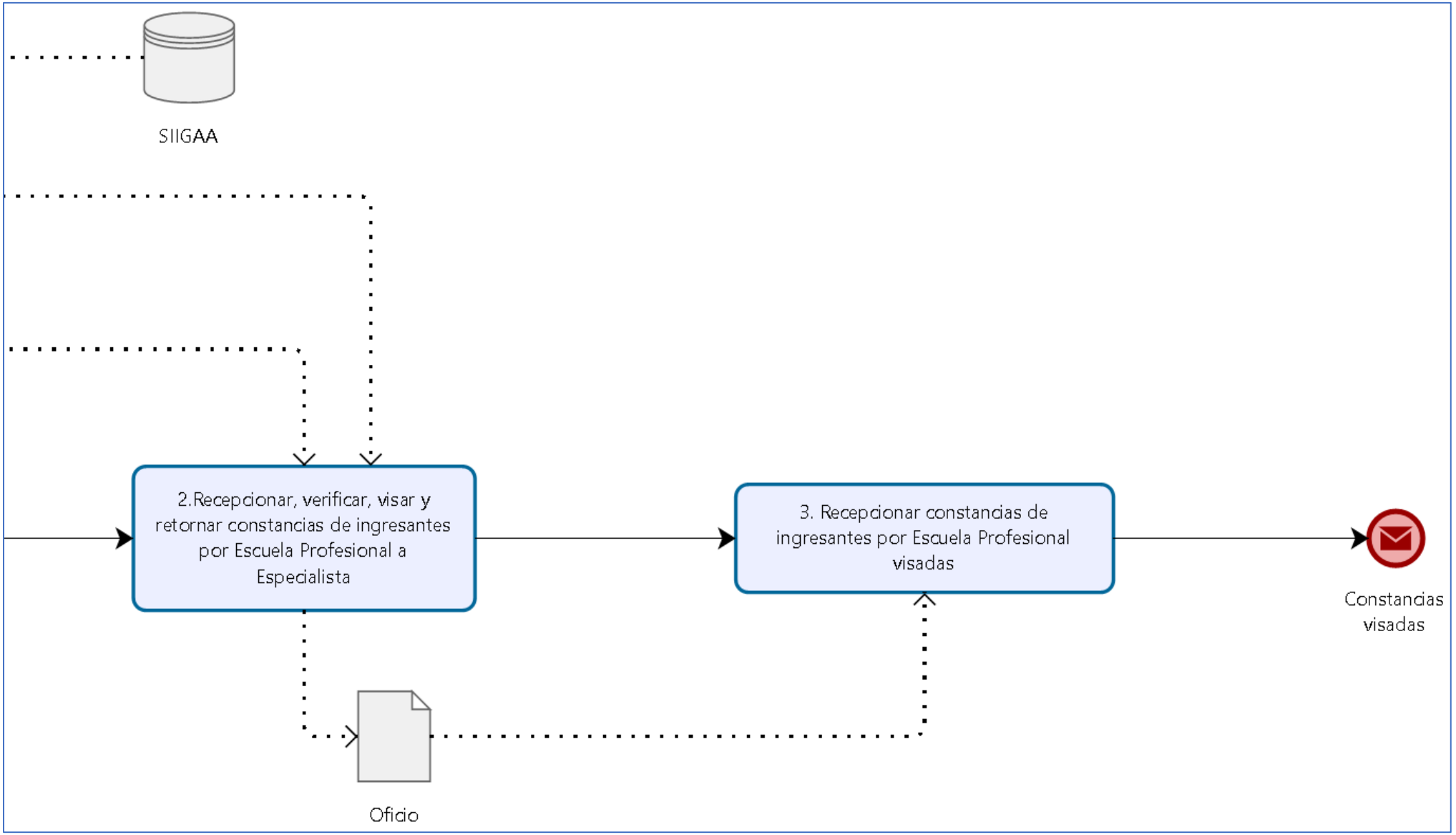


Tabla N° 30: PM01.01.05.02 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.05.02 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.05.Acreditación de ingresantes a las Carreras Profesionales de Pregrado
TÍTULO:	Presentación y validación de requisitos de ingresantes		
A. OBJETIVO:	Validar requisitos de los ingresantes a las Escuelas Profesionales		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF ,Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

	E. DESCRIPCIÓN DEL PROCEDIMIENTO:	**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Realizar pago por derecho de acreditación de ingreso a escuela profesional (indicar el número de DNI) a la cuenta de la UNS del Banco de la Nación.		Ingresante	Ingresante	Voucher
2	Presentar requisitos documentarios (según Reglamento de Admisión) y solicitar constancia en el cronograma establecido.		Ingresante	Ingresante	Documentos requisito
3	Verificar y validar requisitos documentarios.		Dirección de Admisión	Especialista de Sistemas	Documentos requisito
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 98: PM01.01.05.02 (General) - Diagrama BPMN 2.0

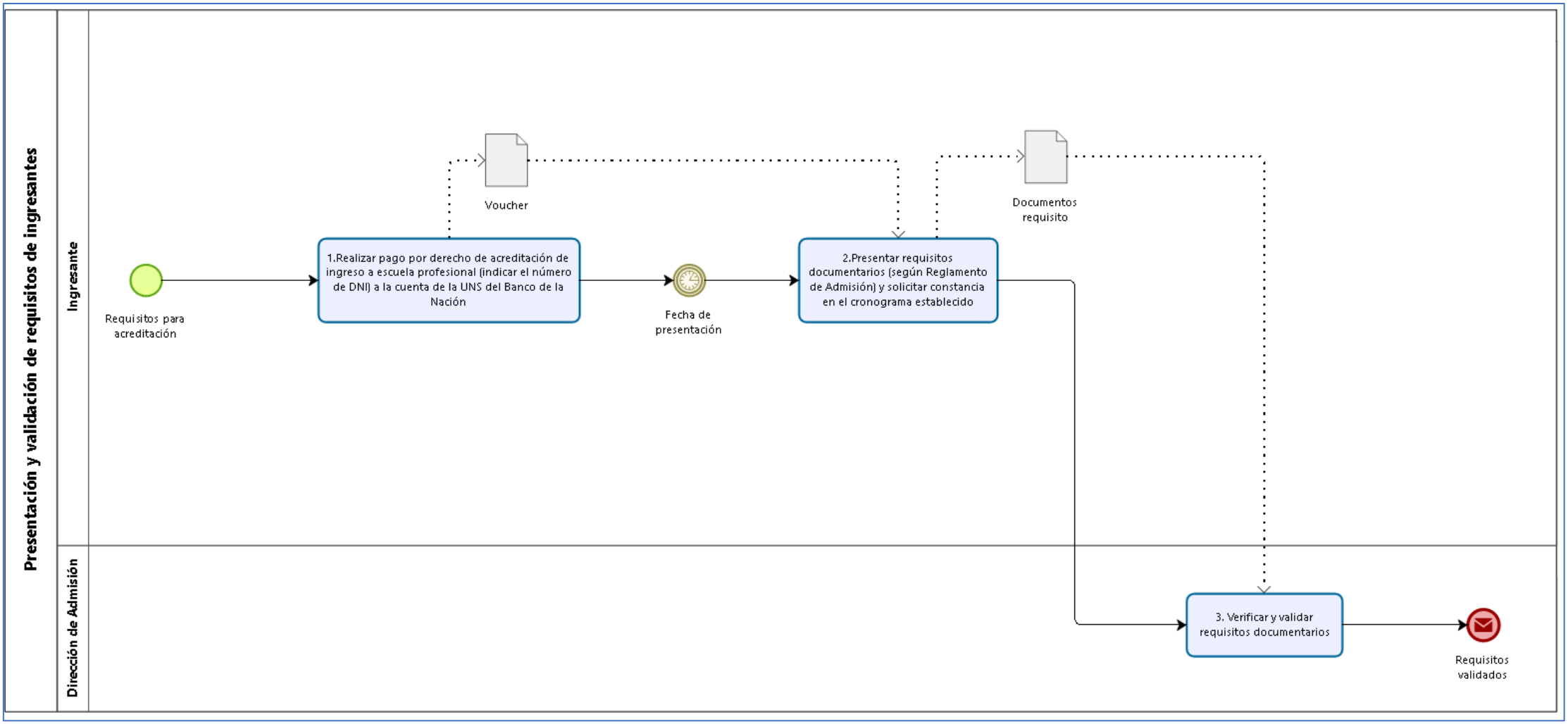


Figura N° 99: PM01.01.05.02 (Parte 1) - Diagrama BPMN 2.0

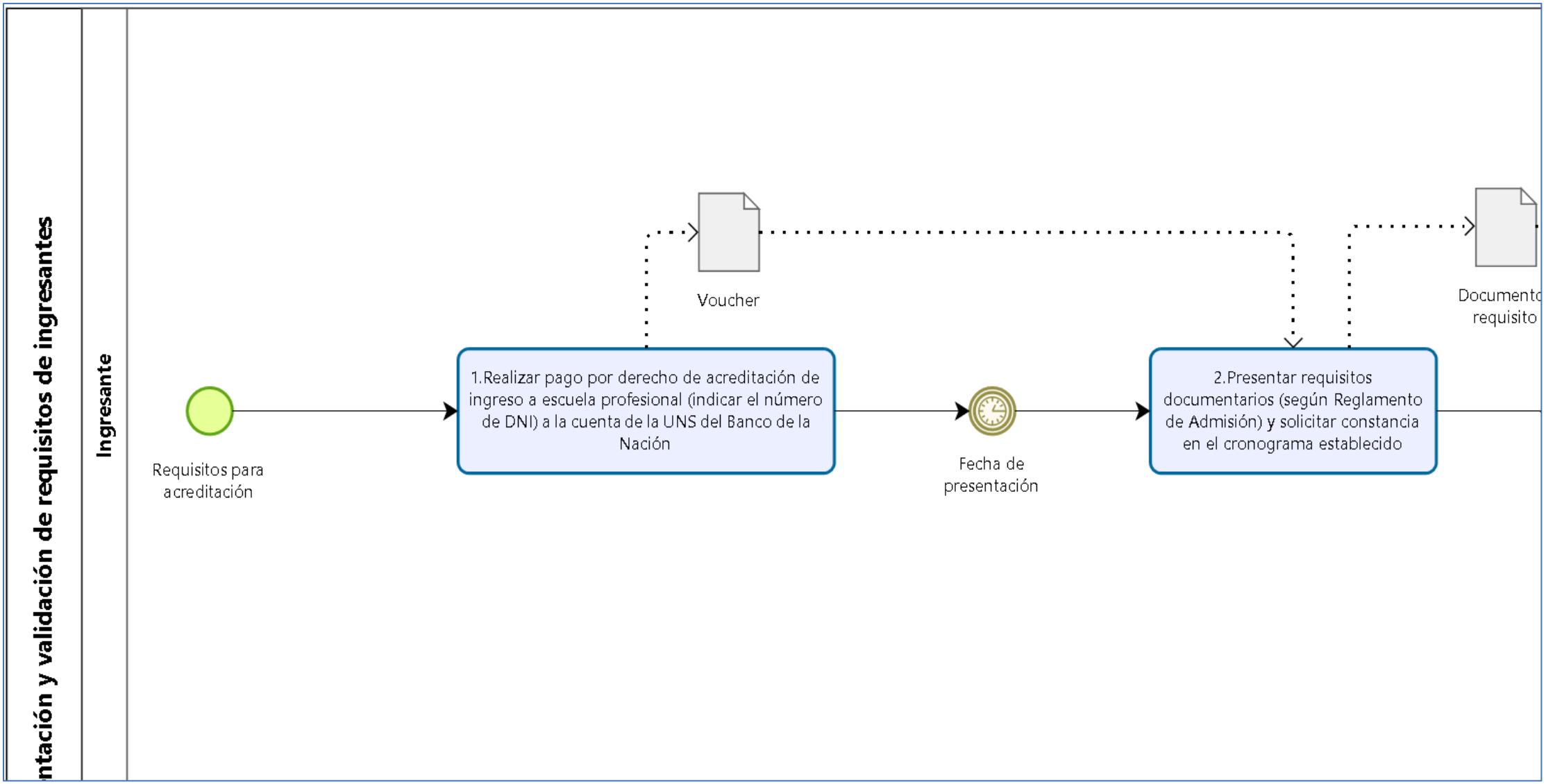


Figura N° 100: PM01.01.05.02 (Parte 2) - Diagrama BPMN 2.0

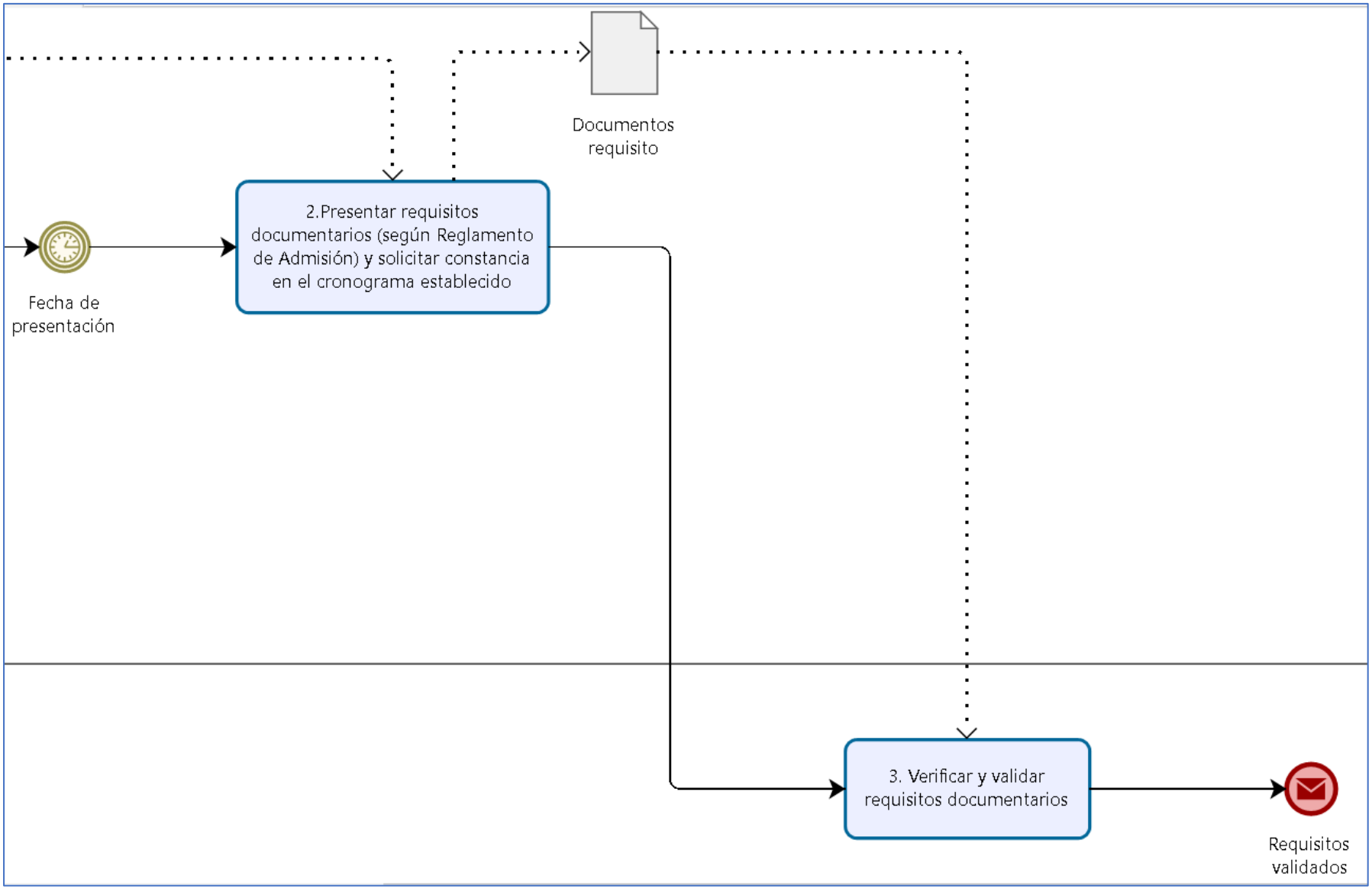


Tabla N° 31: PM01.01.05.03 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.05.03 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.05.Acreditación de ingresantes a las Carreras Profesionales de Pregrado
TÍTULO:	Entrega de constancias de ingreso		
A. OBJETIVO:	Entregar constancias a los ingresantes acreditados a las Escuelas Profesionales		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Realizar la entrega de constancias a los ingresantes por Escuela Profesional.		Dirección de Admisión	Especialista de Sistemas	Constancias de Ingresantes
2	Solicitar firma de conformidad de constancia a ingresantes acreditados.		Dirección de Admisión	Especialista de Sistemas	Registro de entrega de constancias
3	Elaborar informe entrega de constancias de ingreso y remitir al Director de Admisión.		Dirección de Admisión	Especialista de Sistemas	Oficio, Informe de entrega de constancias de ingresantes
4	Recepcionar y verificar informe entrega de constancias de ingreso.		Dirección de Admisión	Especialista de Sistemas	Oficio, Informe de entrega de constancias de ingresantes
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 101: PM01.01.05.03 - Diagrama BPMN 2.0

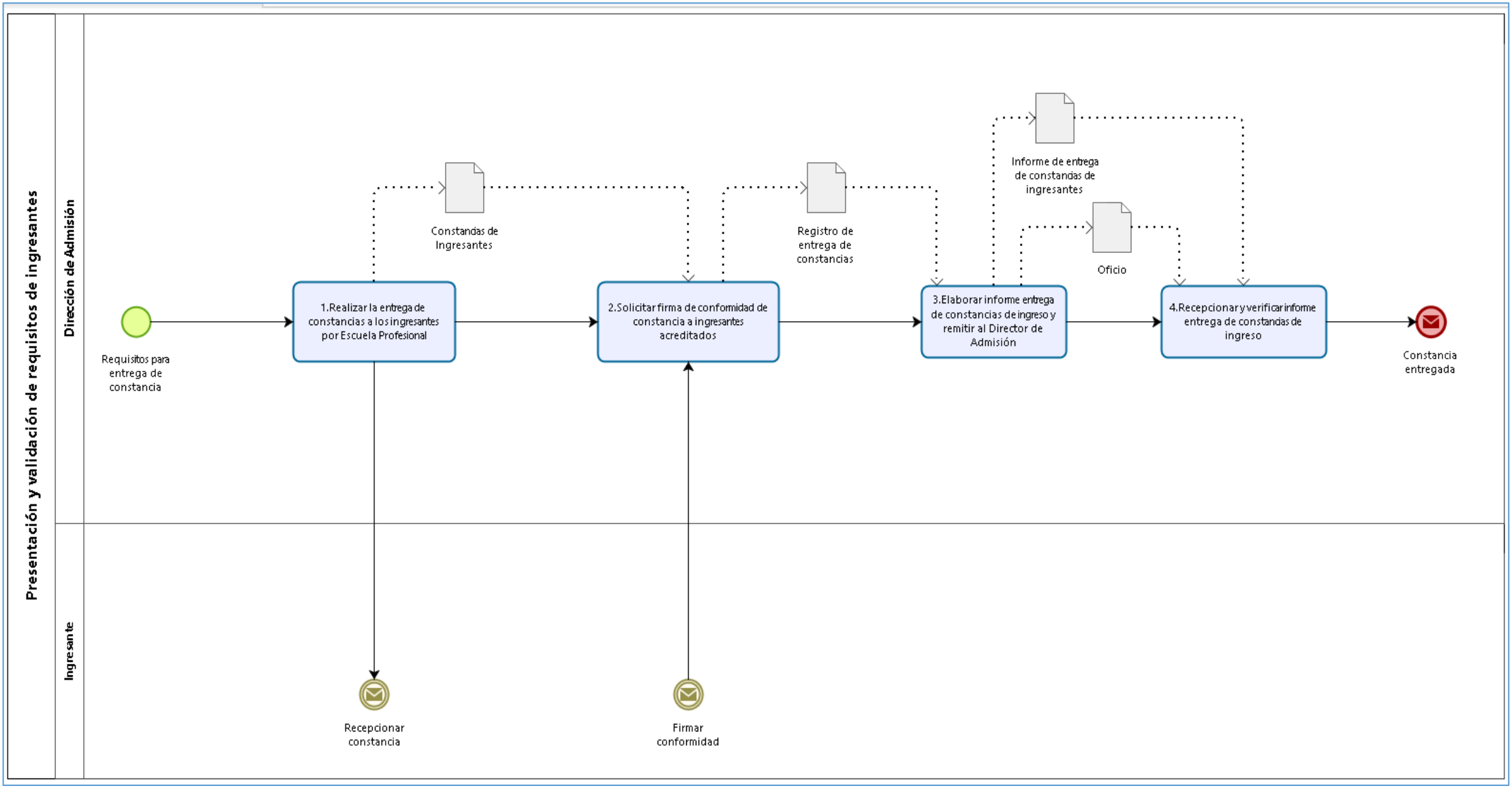


Figura N° 102: PM01.01.05.03 (Parte 1) - Diagrama BPMN 2.0

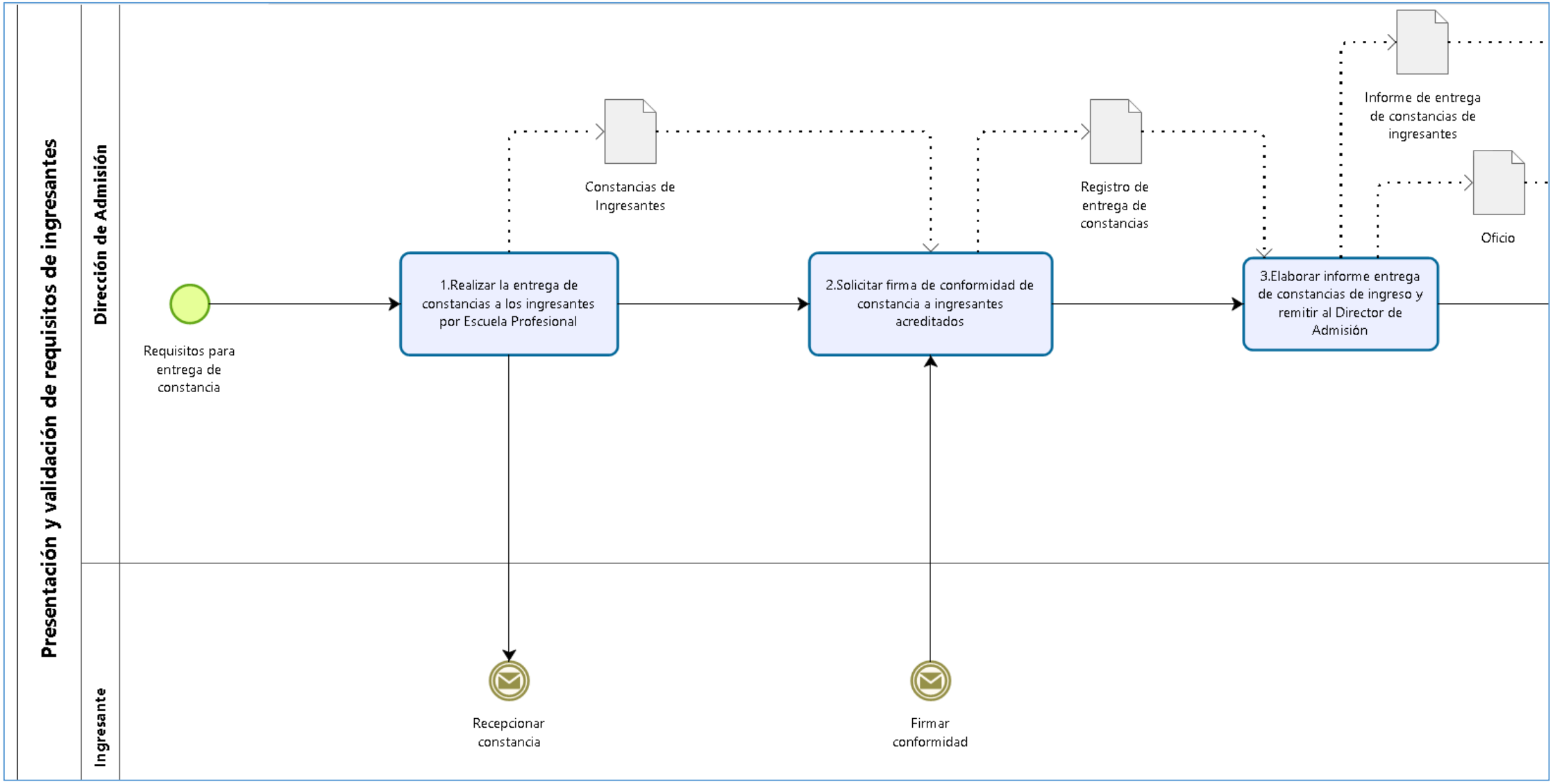


Figura N° 103: PM01.01.05.03 (Parte 2) - Diagrama BPMN 2.0

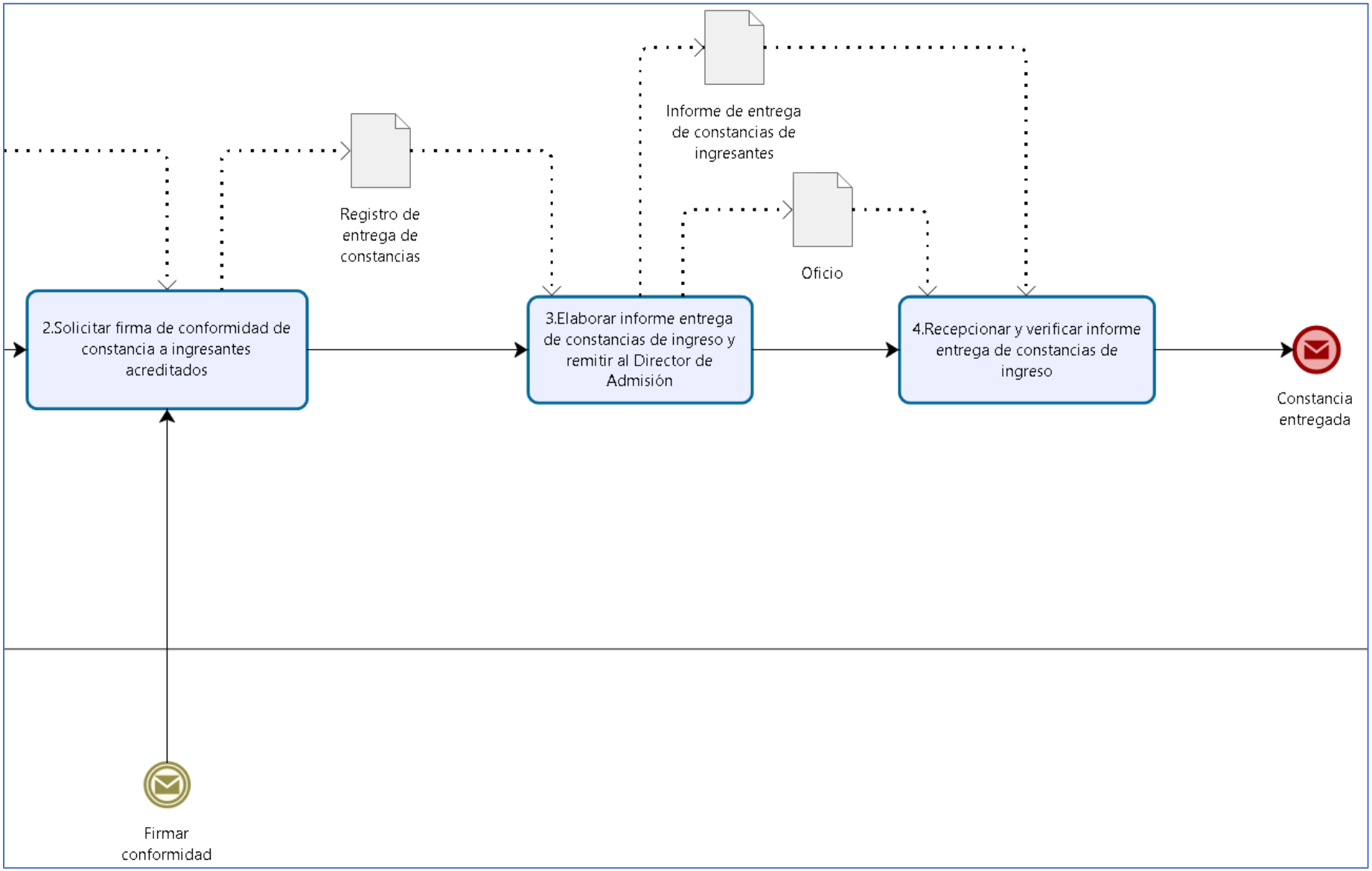


Tabla N° 32: PM01.01.06 - Ficha de Proceso

	FICHA DE PROCESO DE NIVEL 2						**Código:** PM01.01.06 **Versión:** 1.0
I. DATOS GENERALES DEL PROCESO							
1. NOMBRE DEL PROCESO	Verificación del Proceso de Admisión de Pregrado		**2. NOMBRE DEL PROCESO DE NIVEL SUPERIOR**		Proceso de Admisión de Programas de Pregrado		
2. OBJETIVO DEL PROCESO	Presentación del Informe de Ejecución del Proceso de Admisión						
4. DUEÑO DEL PROCESO	Director de Admisión		**5. LÍMITES DEL PROCESO**	**INICIO**	Elaboración del Informe de Ejecución del Proceso de Admisión		
				FIN	Entrega de expedientes de ingresantes a las Escuelas Profesionales		
II. DESCRIPCIÓN DEL PROCESO							
6. PROVEEDORES	**7. INSUMOS**	**8. PROCESOS DE NIVEL INFERIOR**		**9. CONTROLES APLICADOS**	**10. PRODUCTOS**	**11. CLIENTES**	
Dirección de Admisión	Reporte de Ingresantes y No Ingresantes del Proceso Reporte de Ingresos Económicos del Proceso Incidencias	**PM01.01.06.01.Presentación de Informe de Ejecución del Proceso de Admisión de Pregrado**		Se verifica la información documentada del proceso de admisión y se realiza una análisis de datos con cuadros estadísticos y recomendaciones para la toma de decisiones	Informe de Ejecución del Proceso de Admisión	Dirección de Admisión Vicerrectorado Académico	
Postulante no ingresante	Solicitud de devolución de documentos	**PM01.01.06.02.Devolución de documentos**		Se verifica la solicitud y el expediente del postulante para realizar la entrega al postulante en caso de no presentar solicitud estos serán incinerados	Registro de devolución de documentos Documentos del Postulante	Dirección de Admisión Postulante no ingresante	
Dirección de Admisión	Expedientes de Ingresantes acreditados	**PM01.01.06.03.Remisión de expedientes de Ingresantes Acreditados**		Se verifica y acopia los expedientes de ingresantes para ser entregados a las direcciones de escuela	Expedientes de Ingresantes acreditados por Escuela Profesional	Dirección de Escuela	
III. RECURSOS PARA LA EJECUCIÓN DEL PROCESO							
12. TIPO	**13. DESCRIPCIÓN**						
Infraestructura, personal o materiales	**Recursos Humanos:** 1 Director de Admisión, 1 Coordinador de Apoyo de Unidad Académica, 1 Coordinador de Apoyo de Unidad Administrativa, 1 Especialista de Sistemas.						
	Infraestructura: Oficinas, PCs, Impresoras, Software Ofimático, Software Escáner, SIGAMEF, SIIGAA (Sistema de Información Integral de Gestión Académica y Administrativa).						
	Material: Material de Oficina						

IV. DOCUMENTACIÓN DEL PROCESO	
14. REGISTROS DEL PROCESO	**15. REFERENCIAS DOCUMENTALES**
1. Registro de devolución de documentos	1. Ley Universitaria 30220
	2. Estatuto
	3. Reglamento General
	4. Plan Operativo Institucional
	5. Reglamento de Organización y Funciones
	6. Manual de Organización y Funciones
	7. Reglamento para Pago de Subvenciones al Personal
	8. Reglamento de Admisión

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo:			

Figura N° 104: PM01.01.06 (General) - Diagrama BPMN 2.0

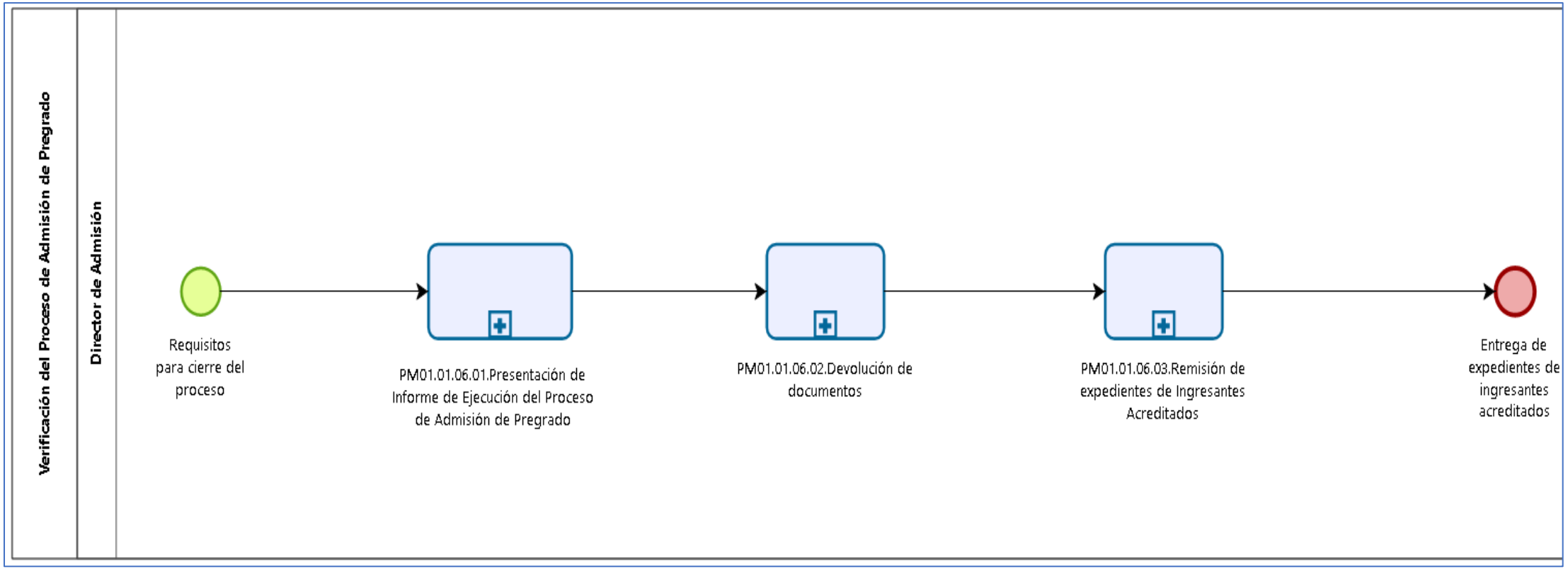


Figura N° 105: PM01.01.06 (Parte 1) - Diagrama BPMN 2.0

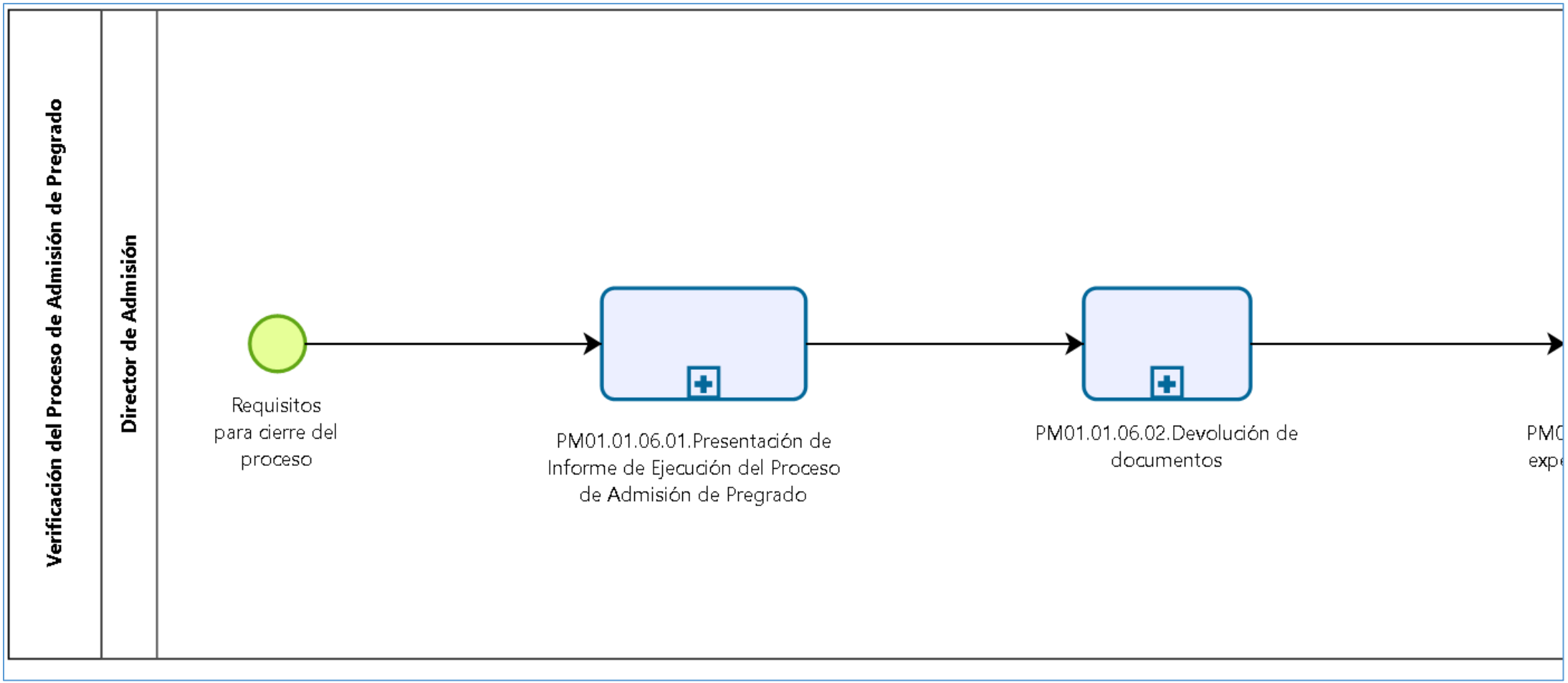


Figura N° 106: PM01.01.06 (Parte 2) - Diagrama BPMN 2.0

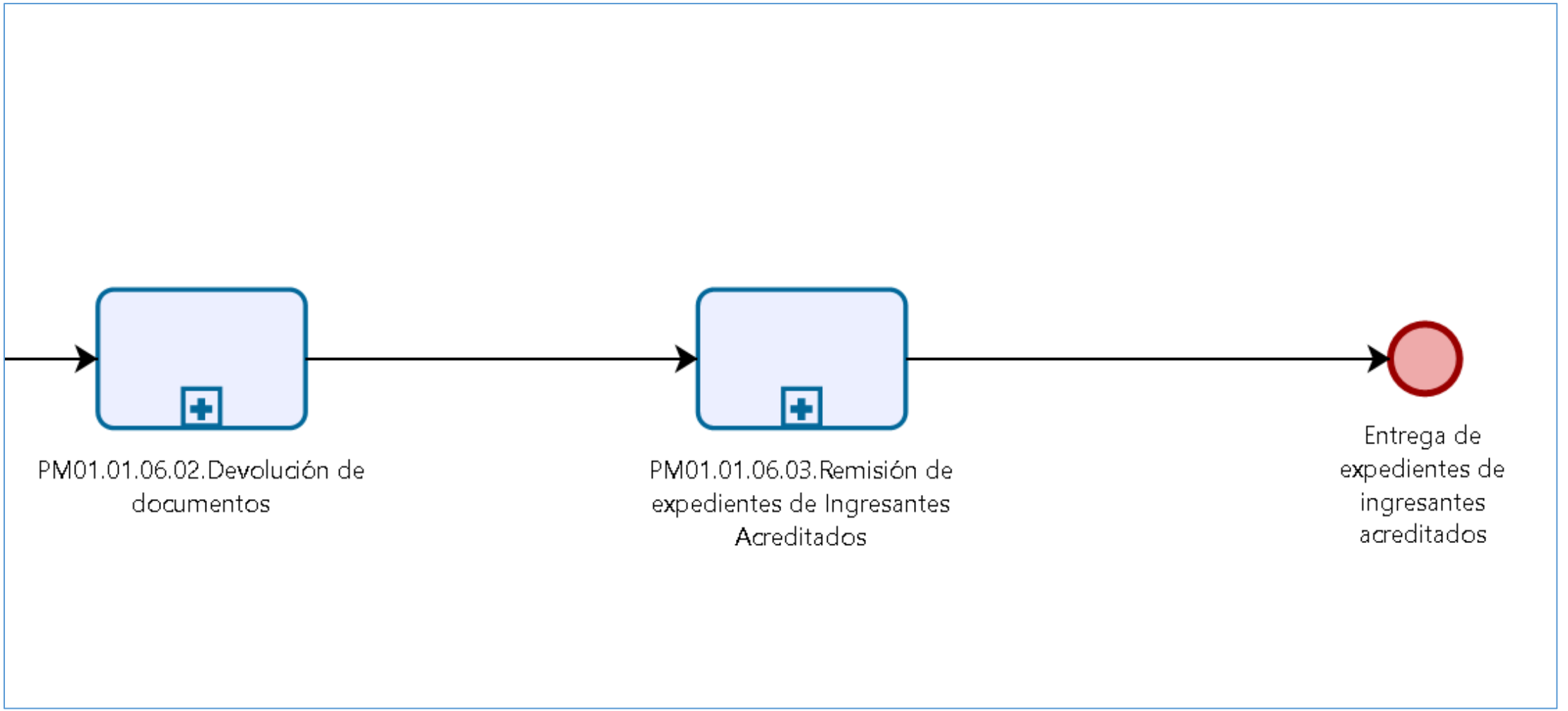


Tabla N° 33: PM01.01.06.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.06.01 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.06.Verificación del Proceso de Admisión de Pregrado
TÍTULO:	Presentación de Informe de Ejecución del Proceso de Admisión de Pregrado		
A. OBJETIVO:	Elaborar y presentar al Vicerrectorado el Informe de Ejecución del Proceso de Admisión de Pregrado		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Solicitar Informe de Ejecución del Proceso de Admisión.		Dirección de Admisión	Director de Admisión	Oficio
2	Elaborar Informe de Ejecución del Proceso de Admisión y remitir al Director de Admisión.		Dirección de Admisión	Especialista de Sistemas	Oficio, Informe de Ejecución del Proceso de Admisión
3	Recepcionar y verificar Informe de Ejecución del Proceso de Admisión y remitir al Vicerrectorado Académico.		Dirección de Admisión	Director de Admisión	Oficio, Informe de Ejecución del Proceso de Admisión
4	Recepcionar y verificar Informe de Ejecución del Proceso de Admisión y remitir recomendaciones.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio, Informe de Ejecución del Proceso de Admisión
5	Recepcionar recomendaciones y determinar plazos para implementación.		Dirección de Admisión	Director de Admisión	Actas
6	Elaborar y remitir plan de acción de mejora a Vicerrectorado Académico.		Dirección de Admisión	Director de Admisión	Oficio, Plan de Acción de Mejora
7	Recepcionar plan de acción de mejora.		Vicerrectorado Académico	Vicerrector(a) Académico(a)	Oficio, Plan de Acción de Mejora
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 107: PM01.01.06.01 (General) - Diagrama BPMN 2.0

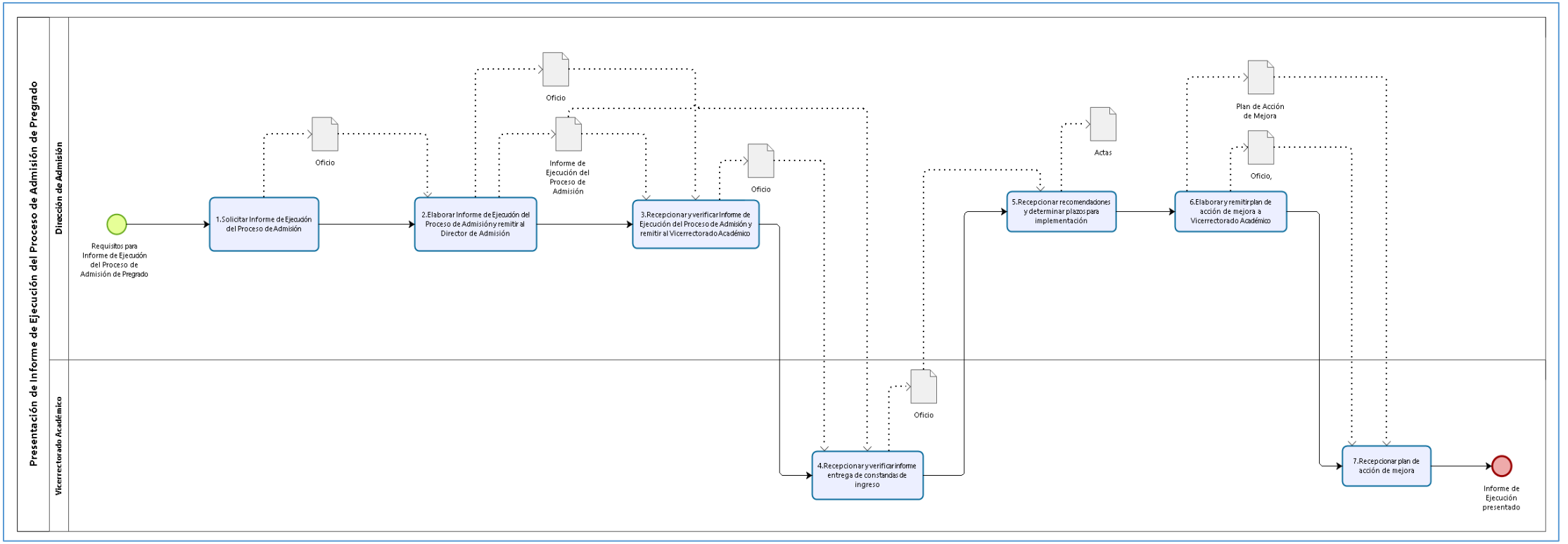


Figura N° 108: PM01.01.06.01 (Parte 1) - Diagrama BPMN 2.0

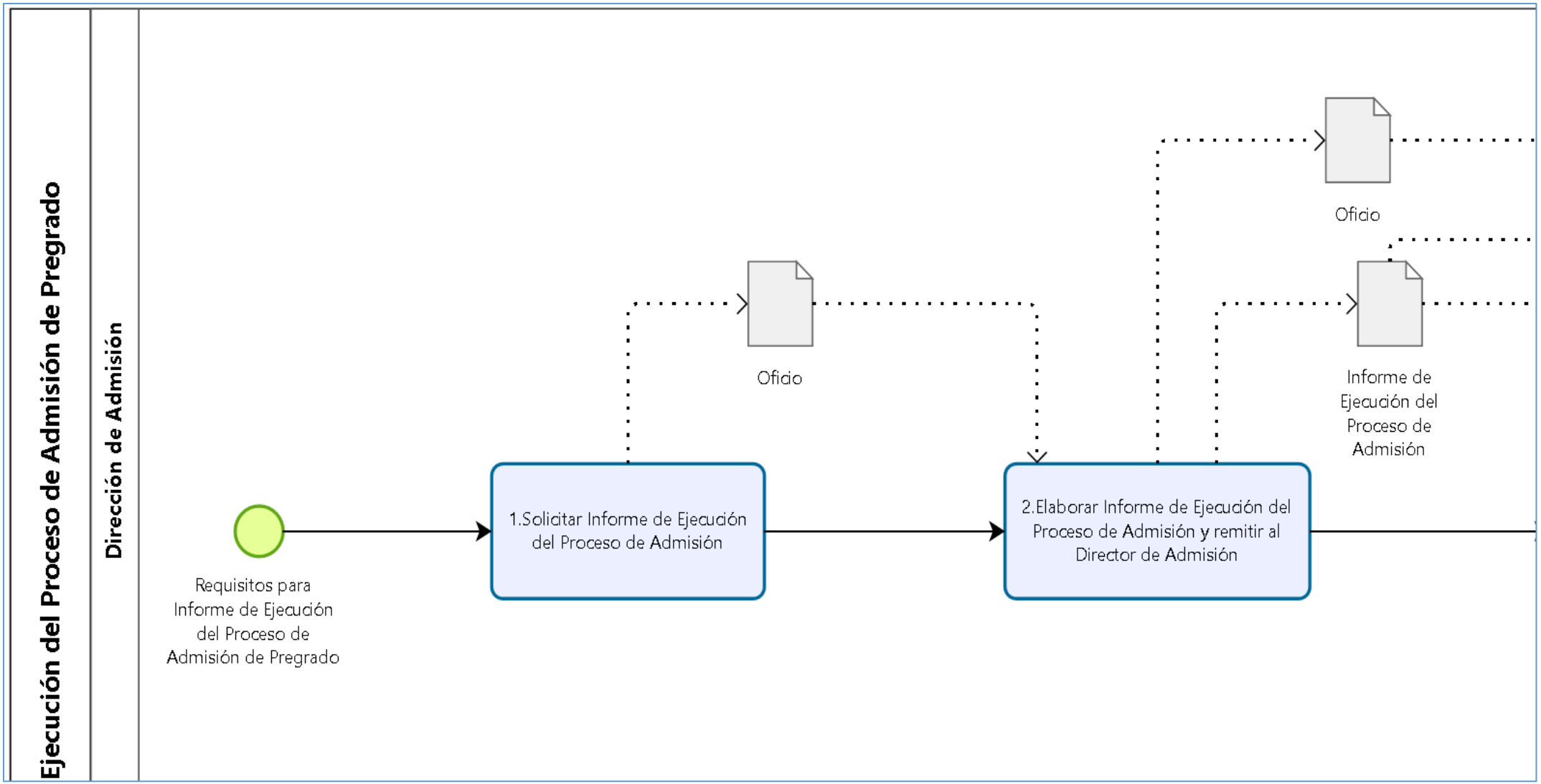


Figura N° 109: PM01.01.06.01 (Parte 2) - Diagrama BPMN 2.0

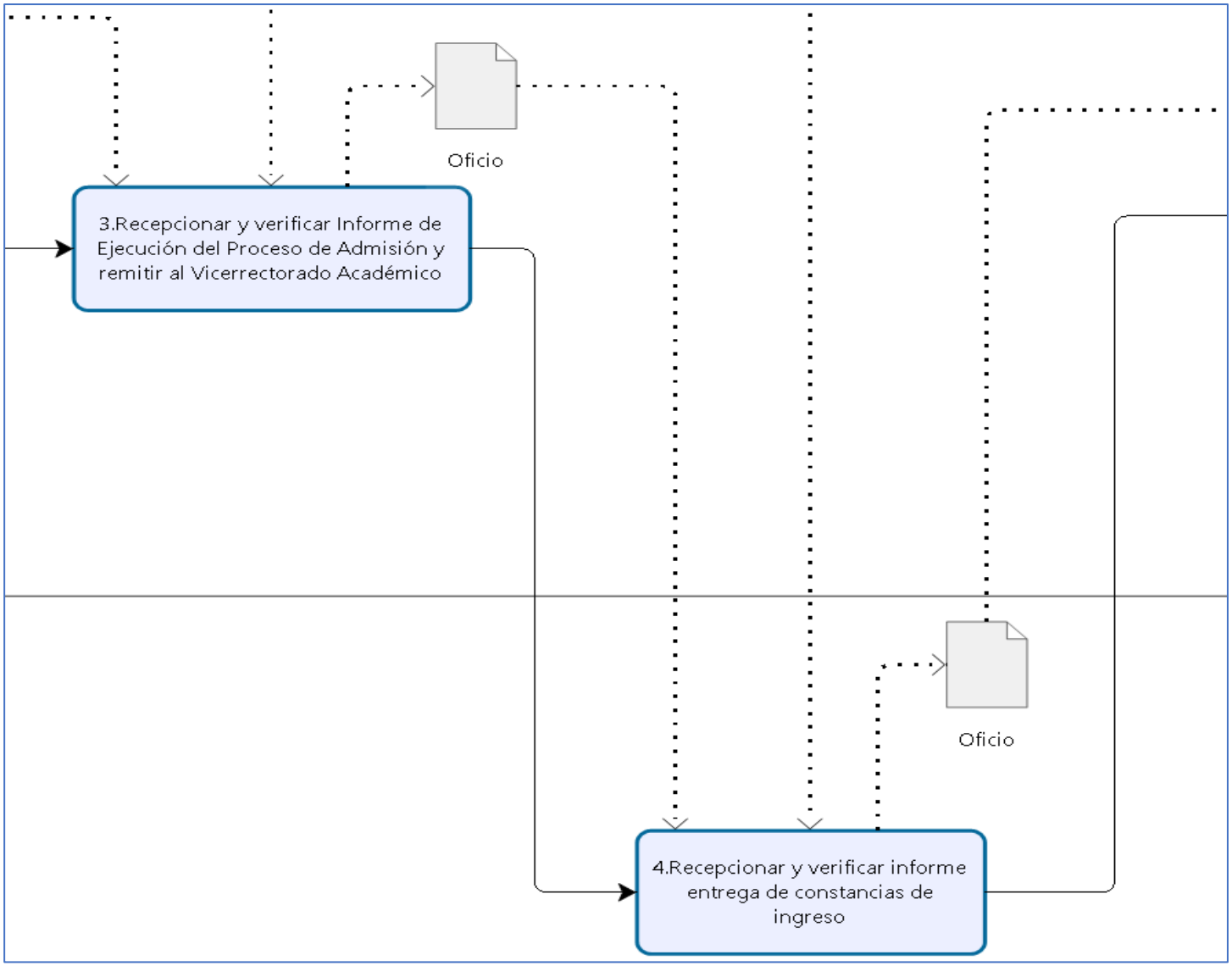


Figura N° 110: PM01.01.06.01 (Parte 3) - Diagrama BPMN 2.0

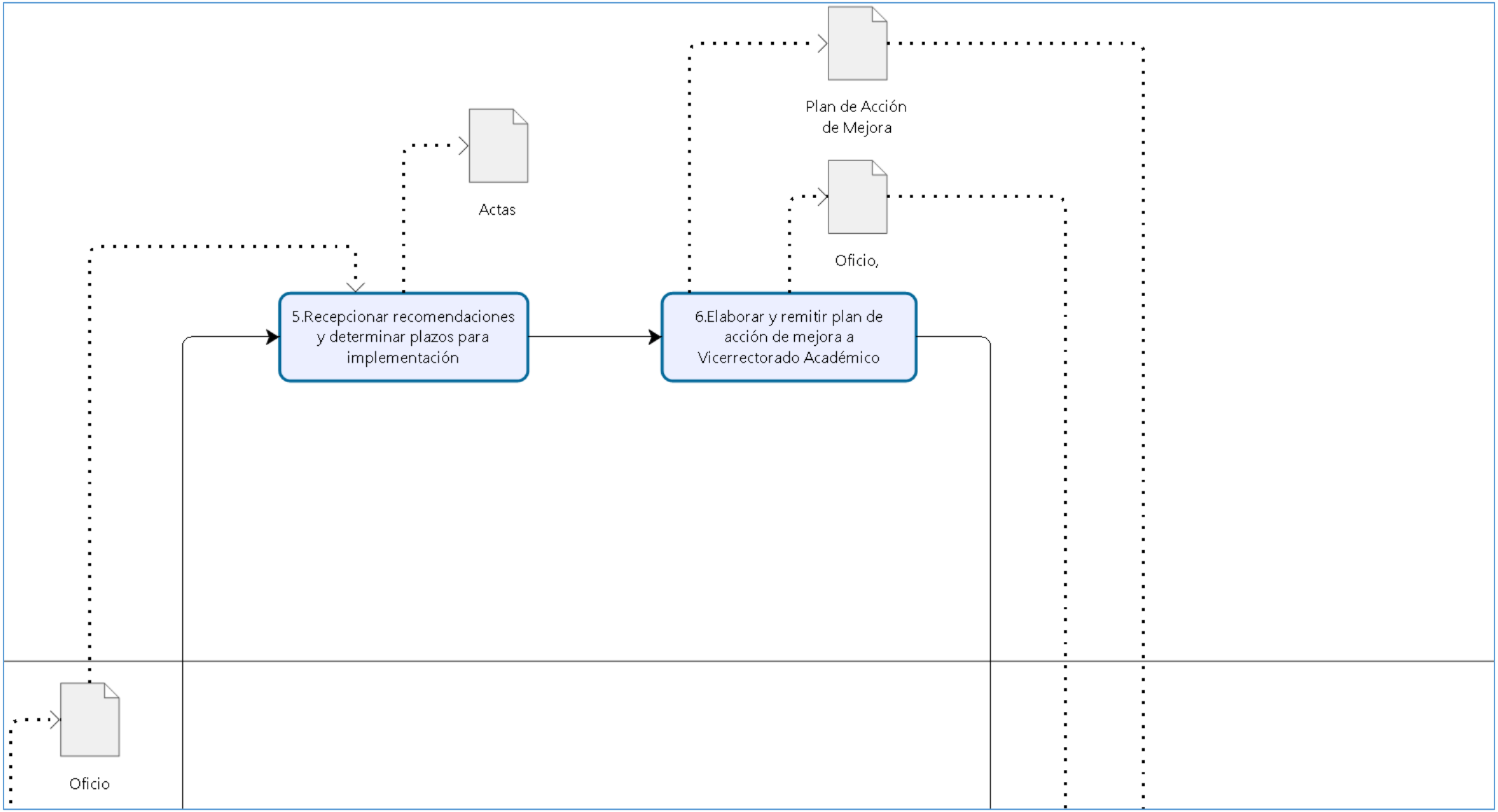


Figura N° 111: PM01.01.06.01 (Parte 4) - Diagrama BPMN 2.0

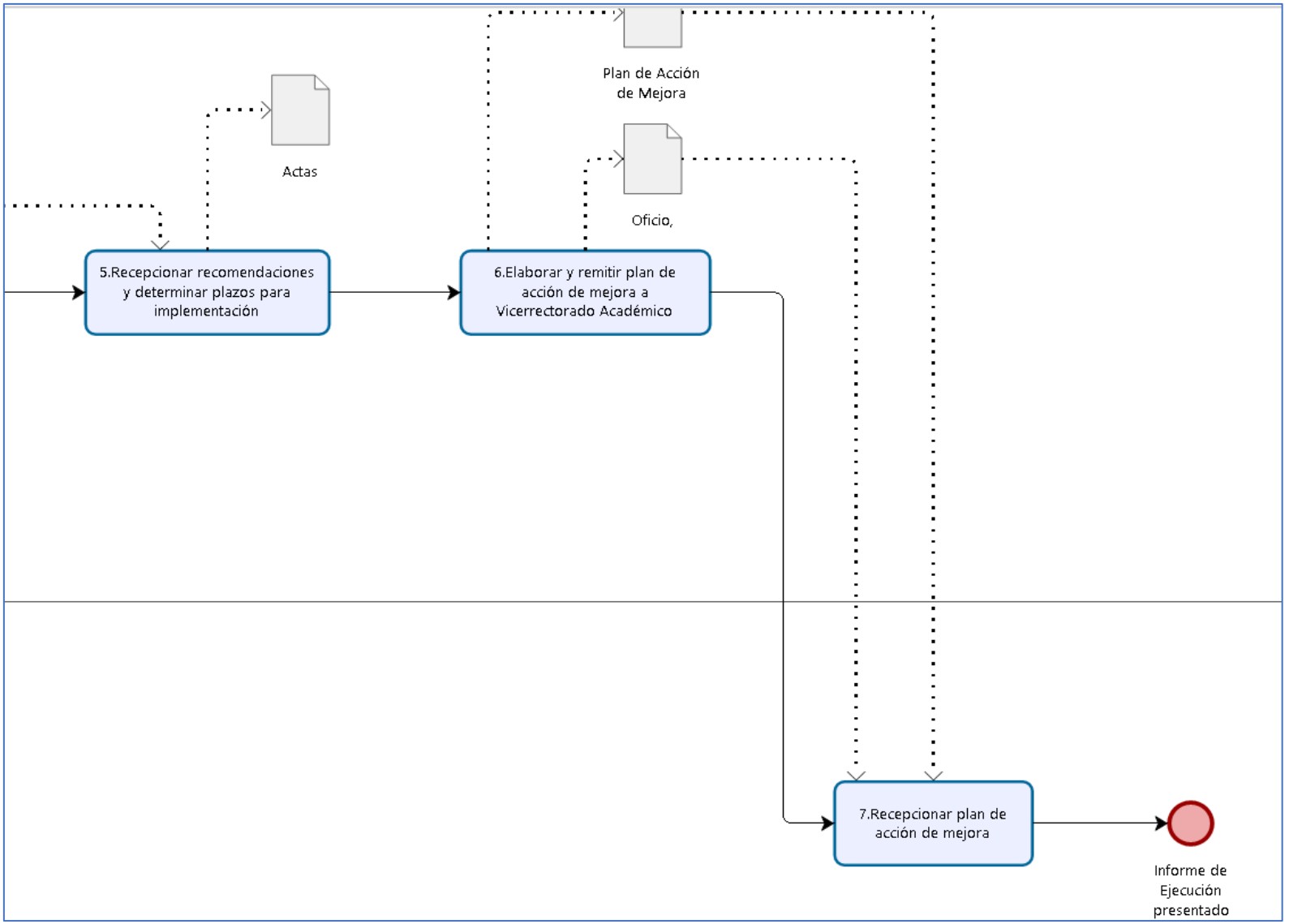


Tabla N° 34: PM01.01.06.02 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO			**Código**: PM01.01.06.02	
				Versión: 1.0	
TIPO:	PROCEDIMIENTO		**PROCESO DE NIVEL SUPERIOR:**	PM01.01.06.Verificación del Proceso de Admisión de Pregrado	
TÍTULO:	Devolución de documentos de Postulantes No Ingresantes				
A. OBJETIVO:	Realizar la devolución de documentos de Postulantes que no lograron ingreso a alguna carrera profesional				
B. UNIDAD RESPONSABLE:	Dirección de Admisión				
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.				
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.				
E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F. REGISTROS**
1	Presentar solicitud de devolución documentos dentro de los treinta días calendario a la Dirección de Admisión.		Postulante	Postulante	Solicitud
2	Realizar devolución de documentos a los postulantes.		Dirección de Admisión	Secretaria de la Dirección de Admisión	Expediente de Postulante
3	Solicitar firma de conformidad de devolución de documentos.		Dirección de Admisión	Secretaria de la Dirección de Admisión	Registro de entrega de documentos
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 112: PM01.01.06.02 (General) - Diagrama BPMN 2.0

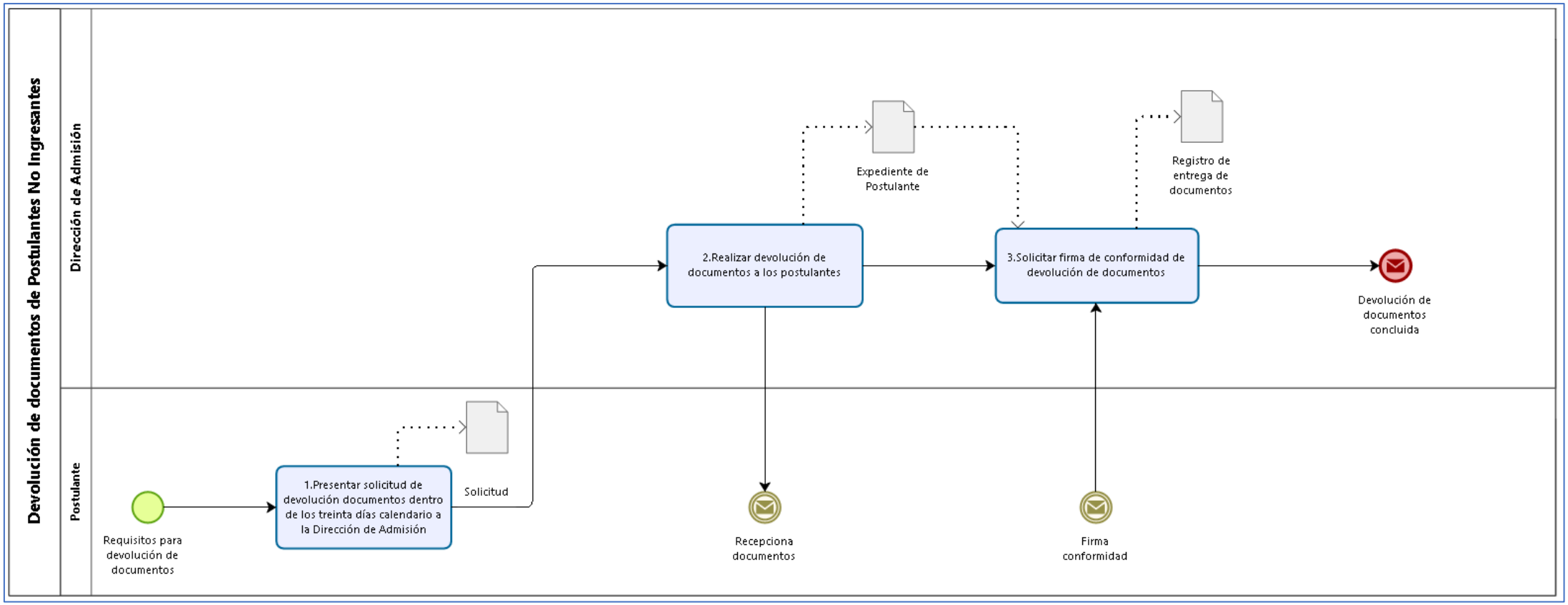


Figura N° 113: PM01.01.06.02 (Parte 1) - Diagrama BPMN 2.0

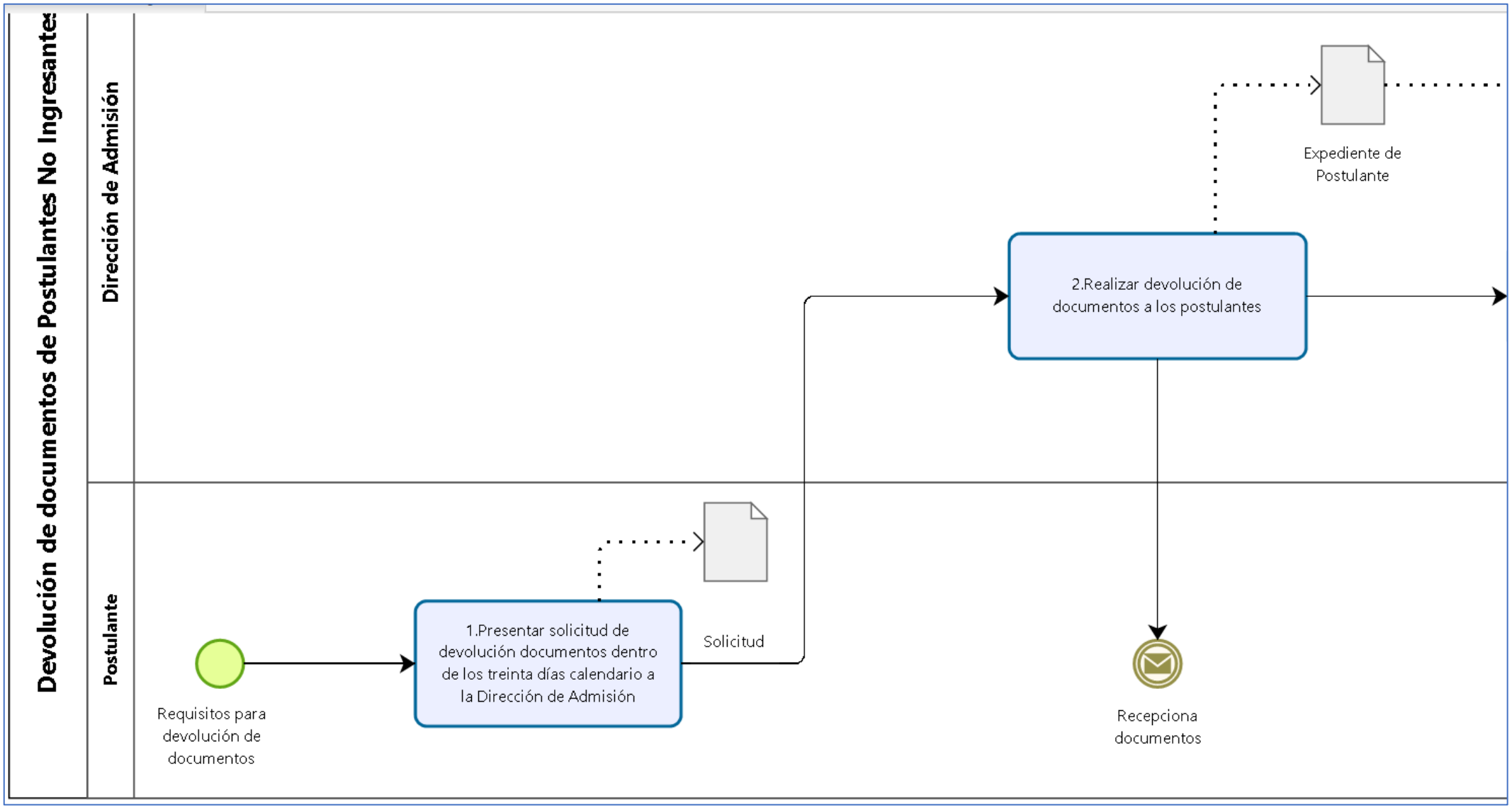


Figura N° 114: PM01.01.06.02 (Parte 2) - Diagrama BPMN 2.0

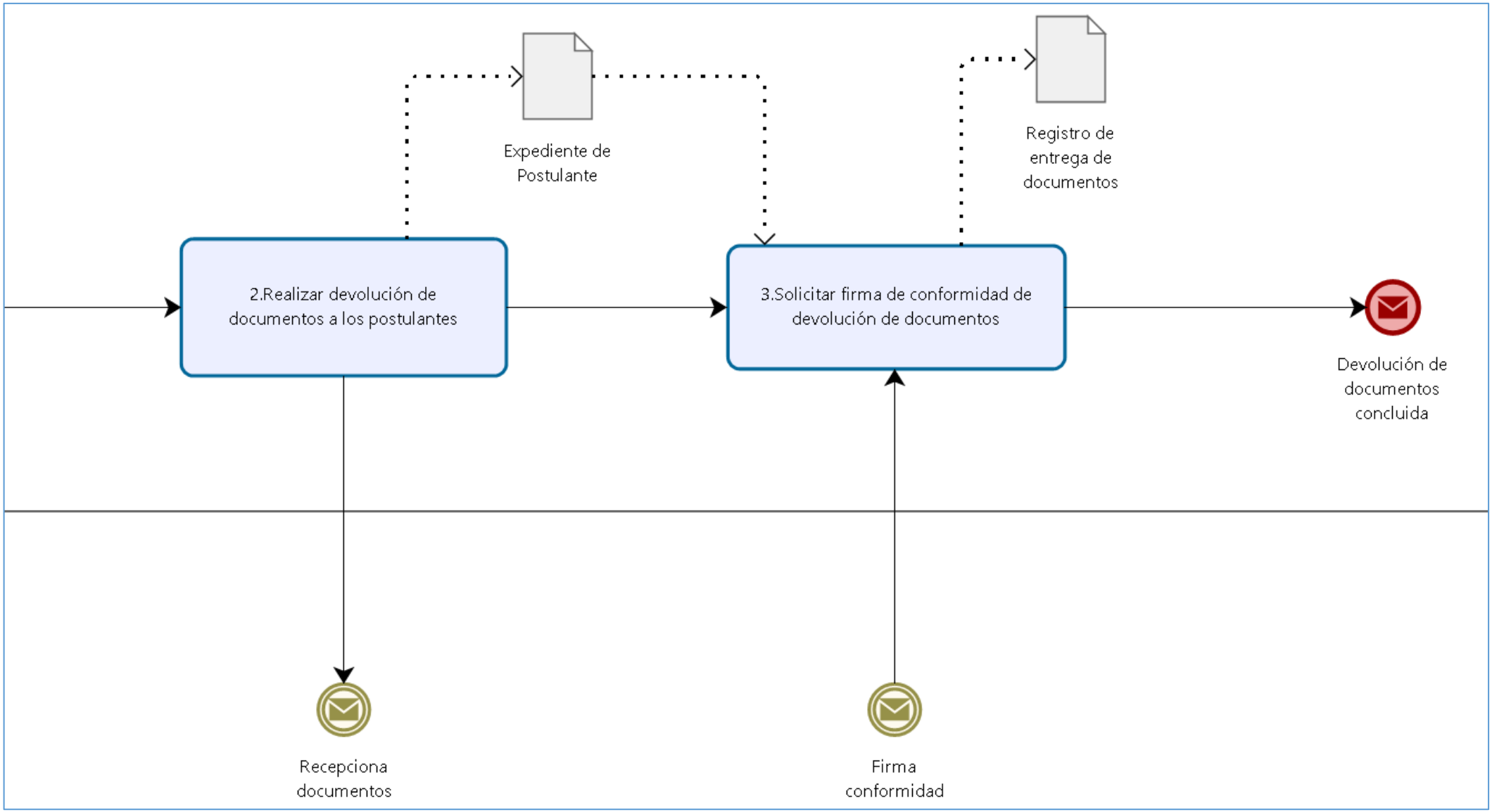


Tabla N° 35: PM01.01.06.03 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**: PM01.01.06.03 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	**PROCESO DE NIVEL SUPERIOR:**	PM01.01.06.Verificación del Proceso de Admisión de Pregrado
TÍTULO:	Remisión de expedientes de Ingresantes Acreditados		
A. OBJETIVO:	Derivar expedientes de ingresantes acreditados a las Escuelas Profesionales		
B. UNIDAD RESPONSABLE:	Dirección de Admisión		
C. BASE LEGAL:	Ley Universitaria N°30220, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional ,MOF, Resolución de designación de Director Admisión y de Coordinadores Académico y Administrativo, Cuadro de Vacantes de Carrera profesional por modalidad, Perfil del Ingresante, Perfil del Egresado, Prospecto de Admisión.		

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		**DURACIÓN horas (8h por día)**	**ÓRGANO/UNIDAD ORGÁNICA**	**RESPONSABLE**	**F.REGISTROS**
1	Verificar y organizar expedientes de ingresantes acreditados por escuela profesional		Dirección de Admisión	Director de Admisión	Registro de ingresantes acreditados
2	Remitir expedientes acreditados por escuela profesional a las Direcciones de Escuela.		Dirección de Admisión	Director de Admisión	Oficio, Expediente de ingresantes acreditados por Escuela
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:		Suma de duraciones			

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	**RESPONSABLE**	**FECHA**	**FIRMA Y SELLO**
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 115: PM01.01.06.03 (General) - Diagrama BPMN 2.0

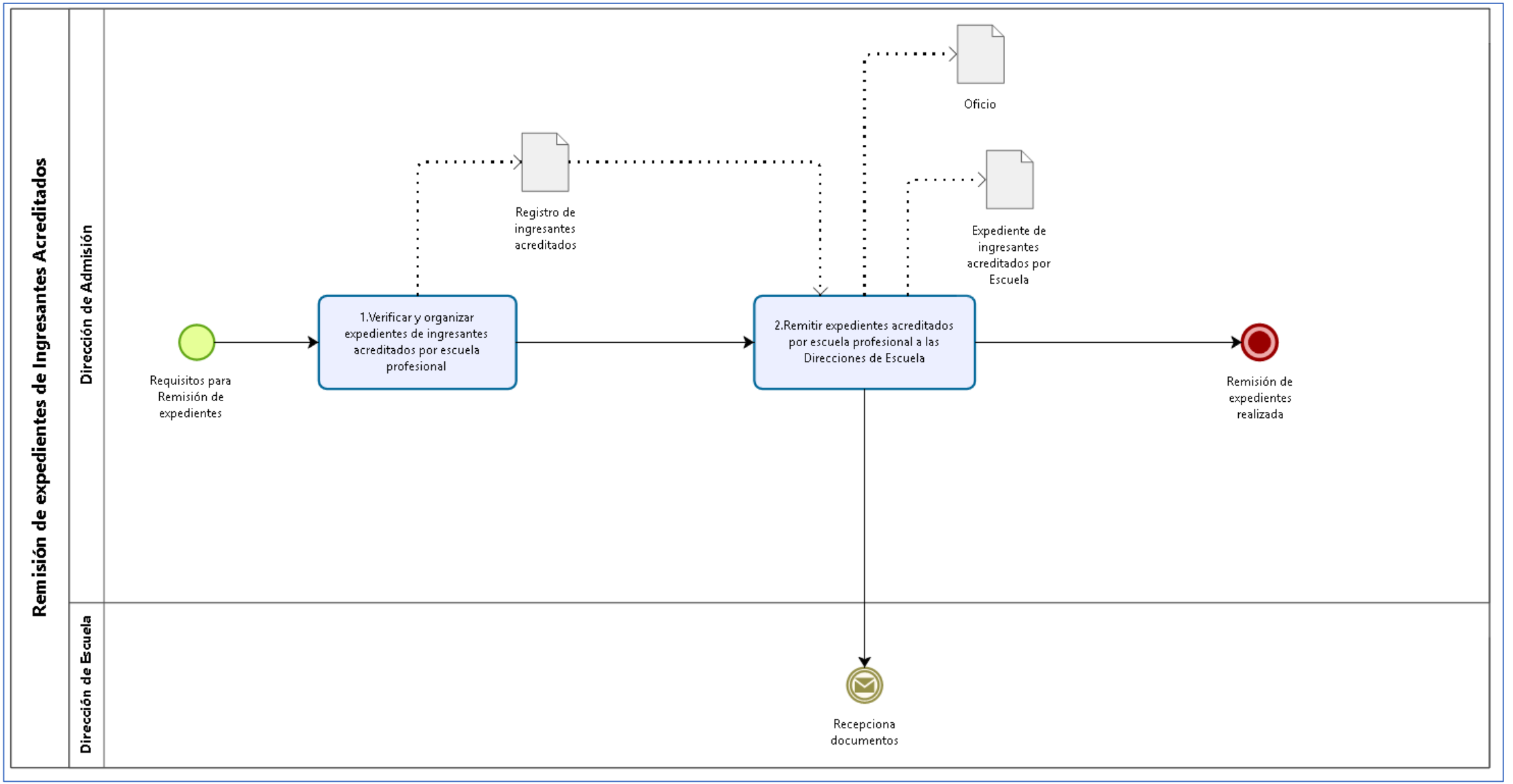


Figura N° 116: PM01.01.06.03 (Parte 1) - Diagrama BPMN 2.0

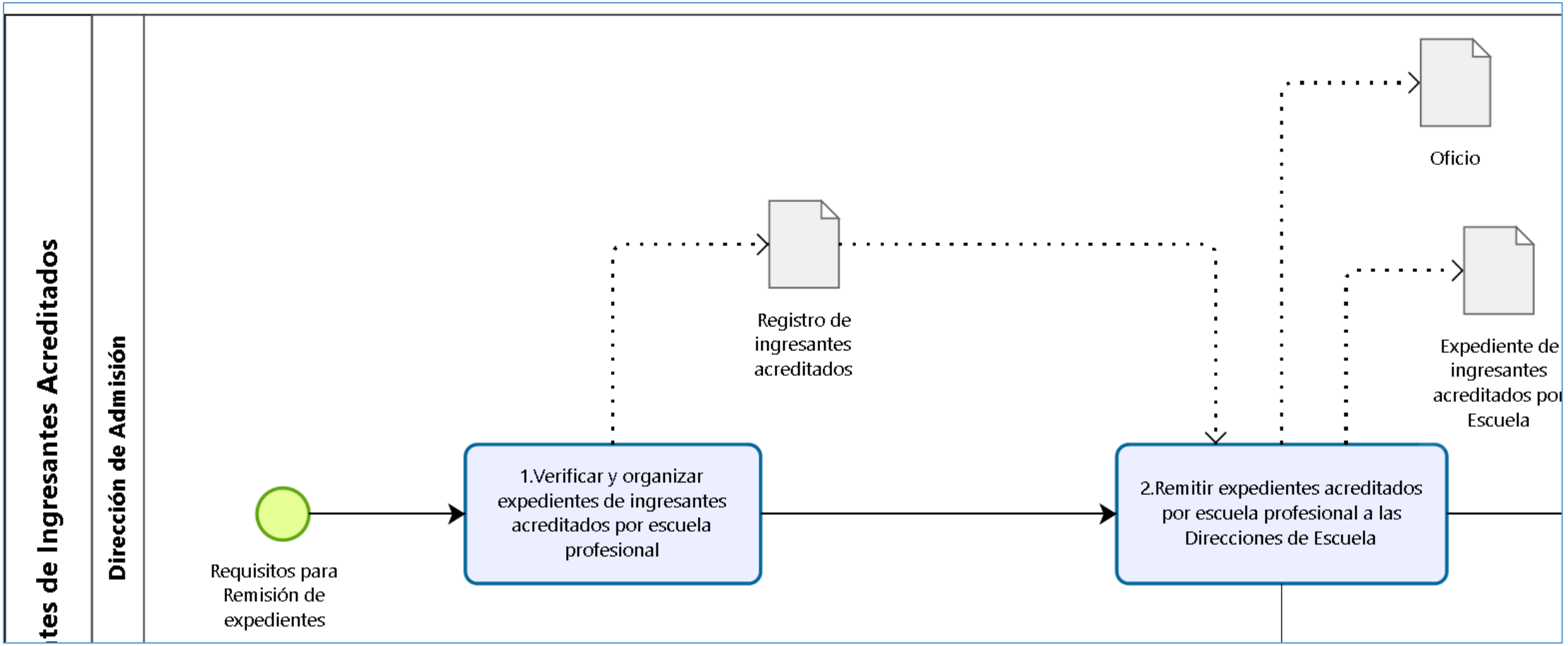
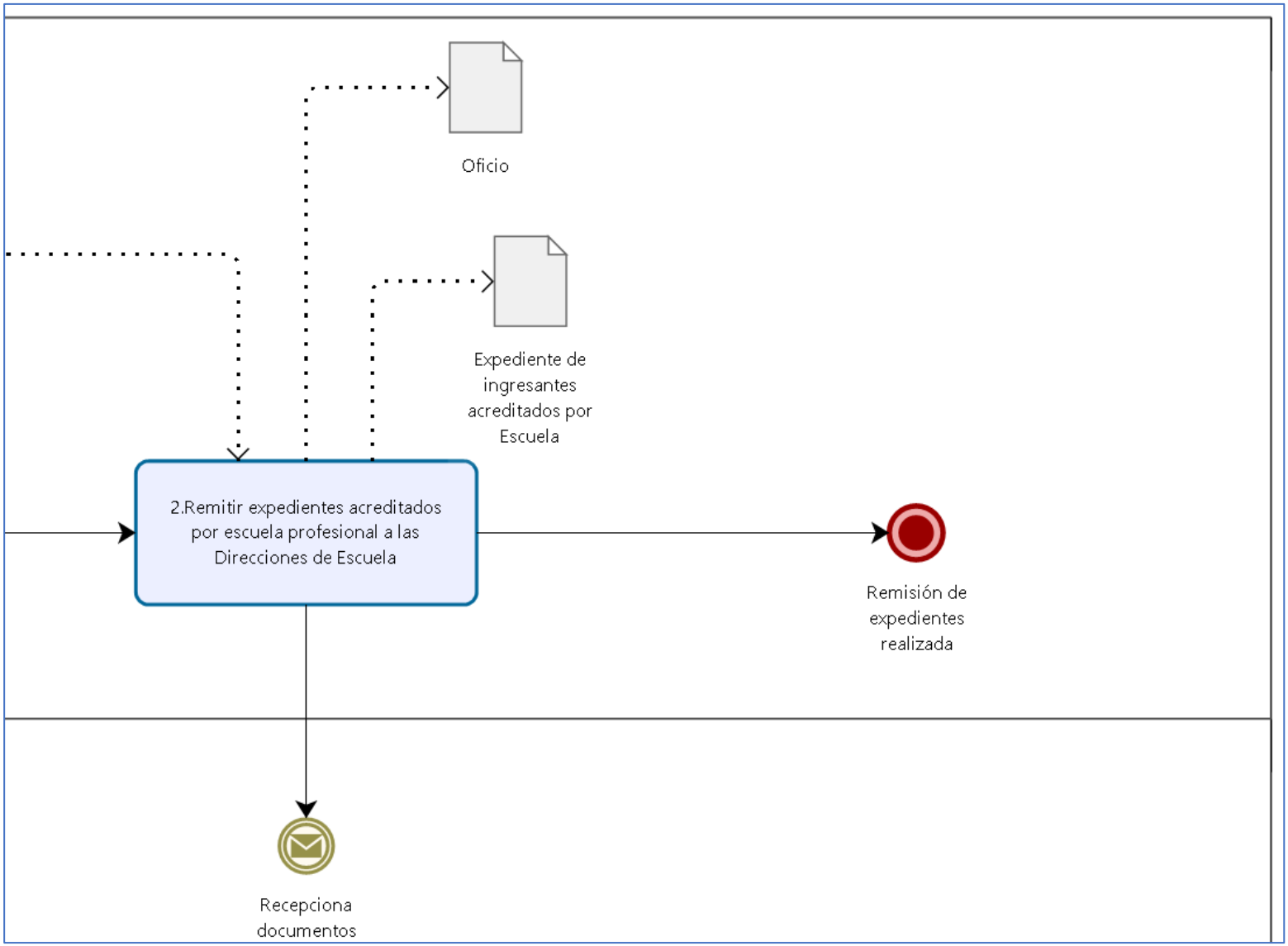


Figura N° 117: PM01.01.06.03 (Parte 2) - Diagrama BPMN 2.0



5.2 Fase II- Análisis, Diseño y Documentación para clasificación de Bancos de Datos Personales

5.2.1 Objetivos de la Fase II

- Revisar la documentación de Ley de Protección de Datos Personales, su reglamento y su directiva.
- Definir matriz de apoyo para clasificar los Bancos de Datos Personales.
- Realizar la clasificación del Banco de Datos Personales de la Dirección de Admisión.
- En base a los resultados de la clasificación del Banco de Datos Personales de la Dirección de Admisión, se determinará si es requerido la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001:2013.

5.2.2 Marco de Trabajo de la Fase II

Elaborar y documentar el procedimiento de clasificación de Banco de Datos Personales y registrar el formato de inventario de Banco de Datos Personales.

5.2.3 Desarrollo de la Fase II

A continuación se realiza la documentación

Tabla N° 36: PE04.01.02.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**:PE04.01.02.01 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	PROCESO DE NIVEL SUPERIOR:	PE04.01.02.Gestión de Protección de Datos Personales
TÍTULO:	Identificación y Registro de Banco de Datos Personales		
A. OBJETIVO:	Registrar Banco de Datos Personales de la Universidad		
B. UNIDAD RESPONSABLE:	Dirección de Información y Documentación		
C. BASE LEGAL:	Ley de Protección de Datos Personales Ley N° 29733Decreto Supremo. Nº 003-2013-JUS Reglamento de la Ley de Protección de Datos Personales, Resolución Directoral Nº019-2013-JUS/DGPDP Autoridad Nacional de Protección de Datos Personales/Ministerio de Justicia y Derechos Humanos, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de aprobación de Política y Procedimientos de la Ley de Protección de Datos Personales.		

	E. DESCRIPCIÓN DEL PROCEDIMIENTO:	DURACIÓN horas (8h por día)	ÓRGANO/UNIDAD ORGÁNICA	RESPONSABLE	F. REGISTROS
1	Analiza información y documentación respecto a la Ley de Protección de Datos Personales y elaborar formato de identificación de Banco de Datos Personales.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Inventario de Banco de Datos
2	Determinar los Banco de Datos Personales y los responsables de su tratamiento acorde con el contexto de la Universidad y la documentación respecto a la Ley de Protección de Datos.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Inventario de Banco de Datos
3	Solicitar reunión con los encargados de los Banco de Datos de la Universidad identificados.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Oficio
4	Recepcionar y enviar invitaciones a los encargados de los Banco de Datos de la Universidad		Dirección de Información y Documentación	Director DID	Oficio
5	Realizar taller de inducción respecto a la Ley de Protección de Datos Personales, su Reglamento y Directiva a personal de dependencia seleccionada.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de participantes, Registro de Inventario de Banco de Datos
6	Realizar consultas con los encargados de los Banco de Datos acorde con los criterios de la Directiva de Seguridad y registrar en formato de inventario de Banco de Datos.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Inventario de Banco de Datos
7	Revisar, validar y firmar conformidad en el formato de Inventario de Banco de Datos.		Encargado del tratamiento del Banco de Datos Personal	Encargado del tratamiento del Banco de Datos Personal	Registro de Inventario de Banco de Datos

8	Entregar formulario de inscripción de Banco de Datos y asesorar a encargados de los Bancos de Datos.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Formulario de inscripción de Banco de Datos
9	Registrar información en formulario de inscripción para entidades públicas y entregar a Oficial de Seguridad.		Encargado del tratamiento del Banco de Datos Personal	Encargado del tratamiento del Banco de Datos Personal	Formulario de inscripción de Banco de Datos
10	Recepcionar y remitir formulario de inscripción a Director.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Oficio, Formulario de inscripción de Banco de Datos
11	Recepcionar y remitir formulario de inscripción a la Dirección de Asesoría Legal.		Dirección de Información y Documentación	Director DID	Oficio, Formulario de inscripción de Banco de Datos
12	Recepcionar, verificar, corregir y realizar proceso de inscripción de los Bancos de Datos Personales en el Ministerio de Justicia.		Dirección de Asesoría Legal	Director DAL	Oficio, Formulario de inscripción de Banco de Datos
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento				
I. ANEXOS:					

ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 118: PE04.01.02.01 - Diagrama BPMN 2.0

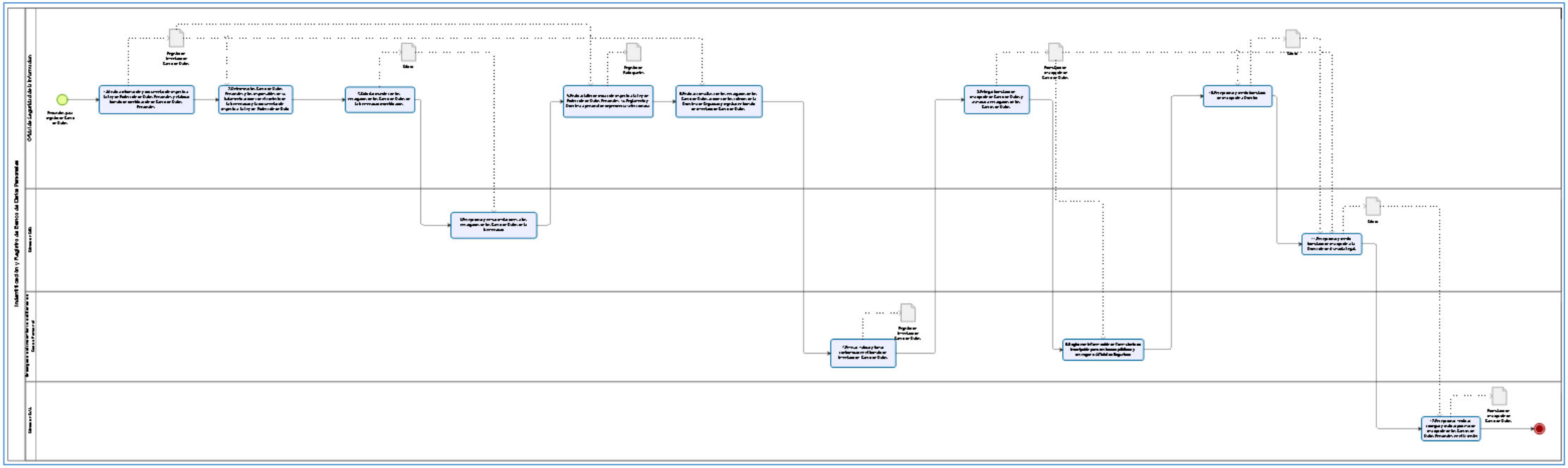


Figura N° 119: PE04.01.02.01 (Parte 1) - Diagrama BPMN 2.0

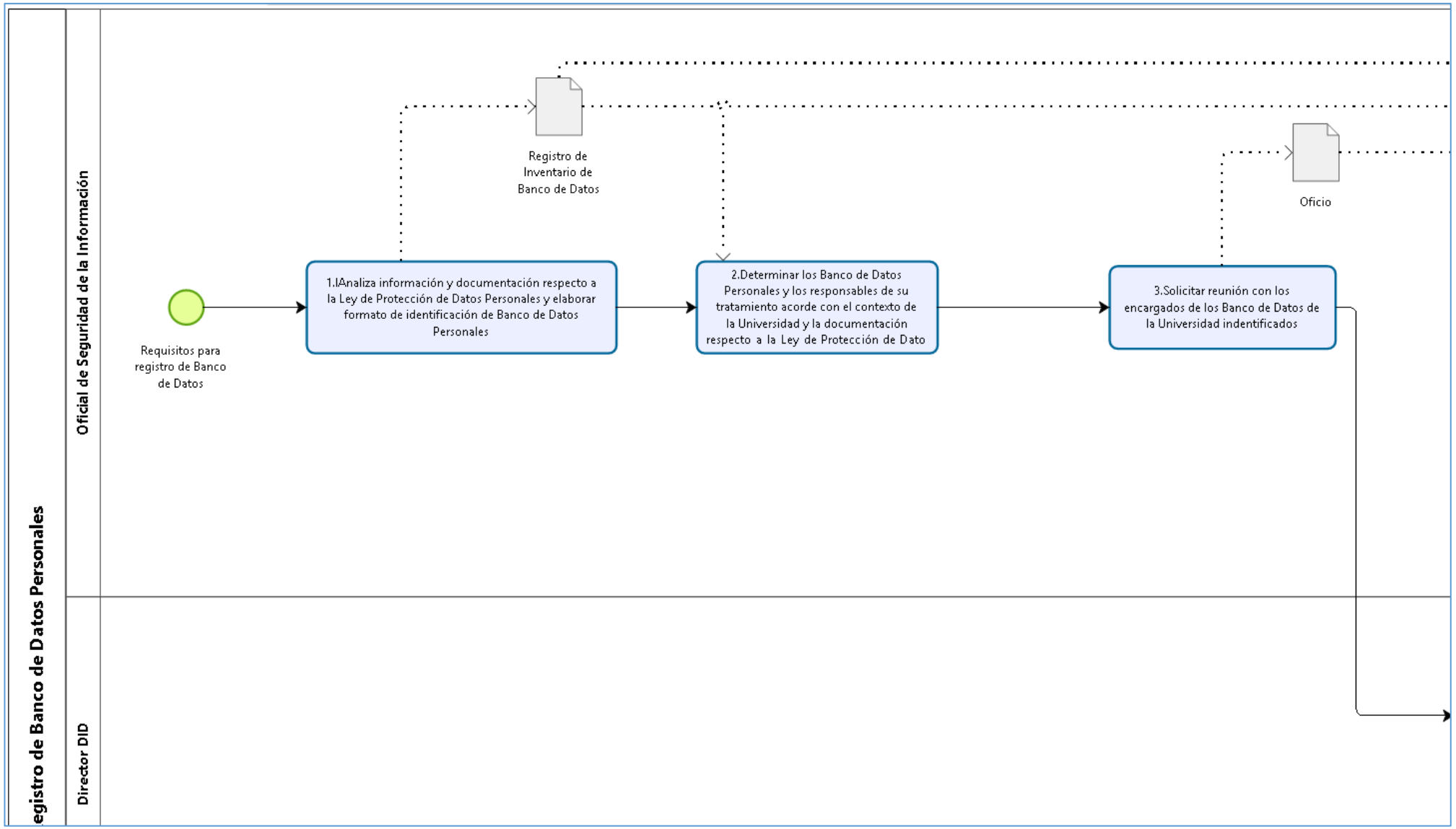


Figura N° 120: PE04.01.02.01 (Parte 2) - Diagrama BPMN 2.0

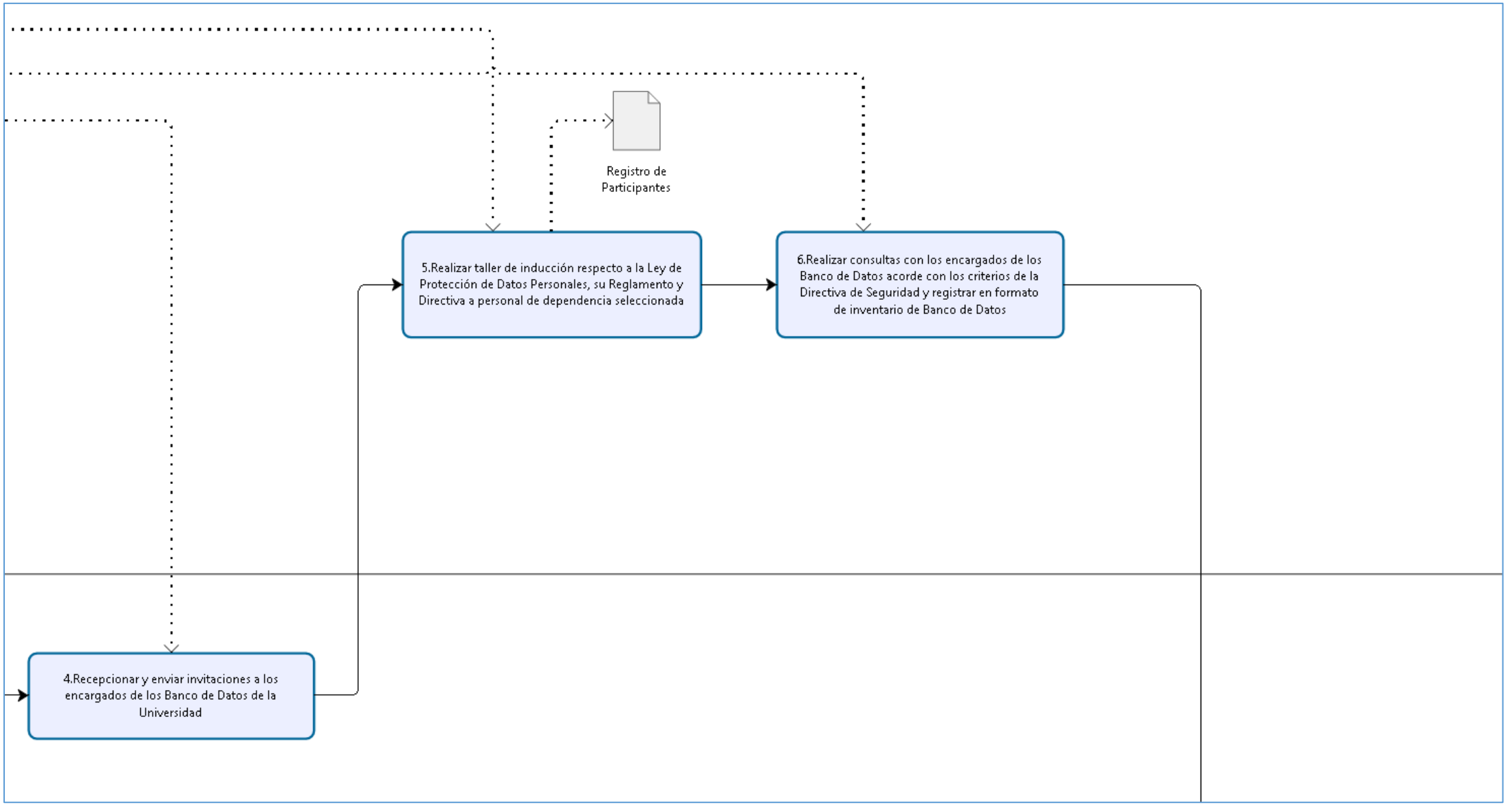


Figura N° 121: PE04.01.02.01 (Parte 3) - Diagrama BPMN 2.0

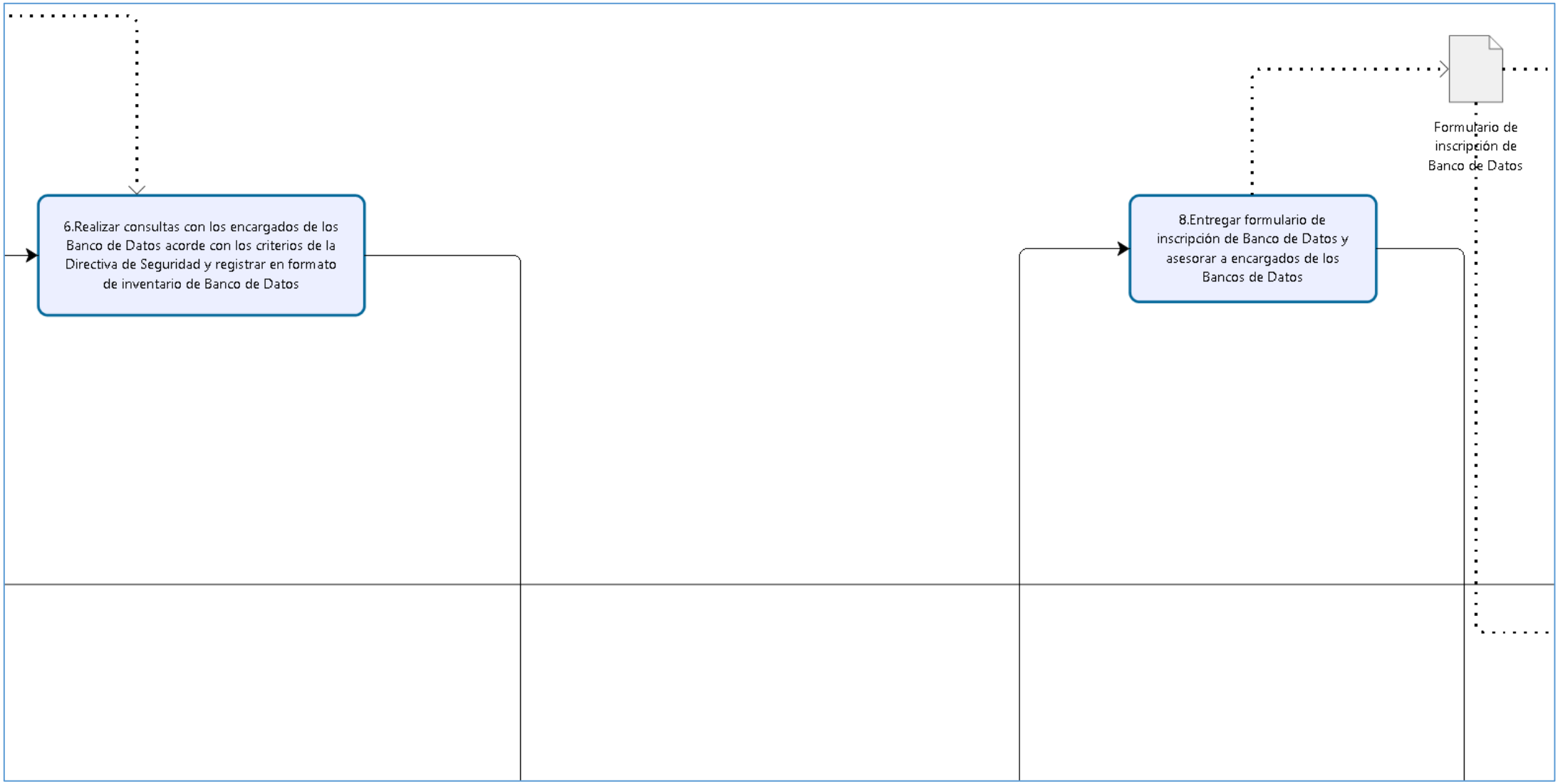


Figura N° 122: PE04.01.02.01 (Parte 4) - Diagrama BPMN 2.0

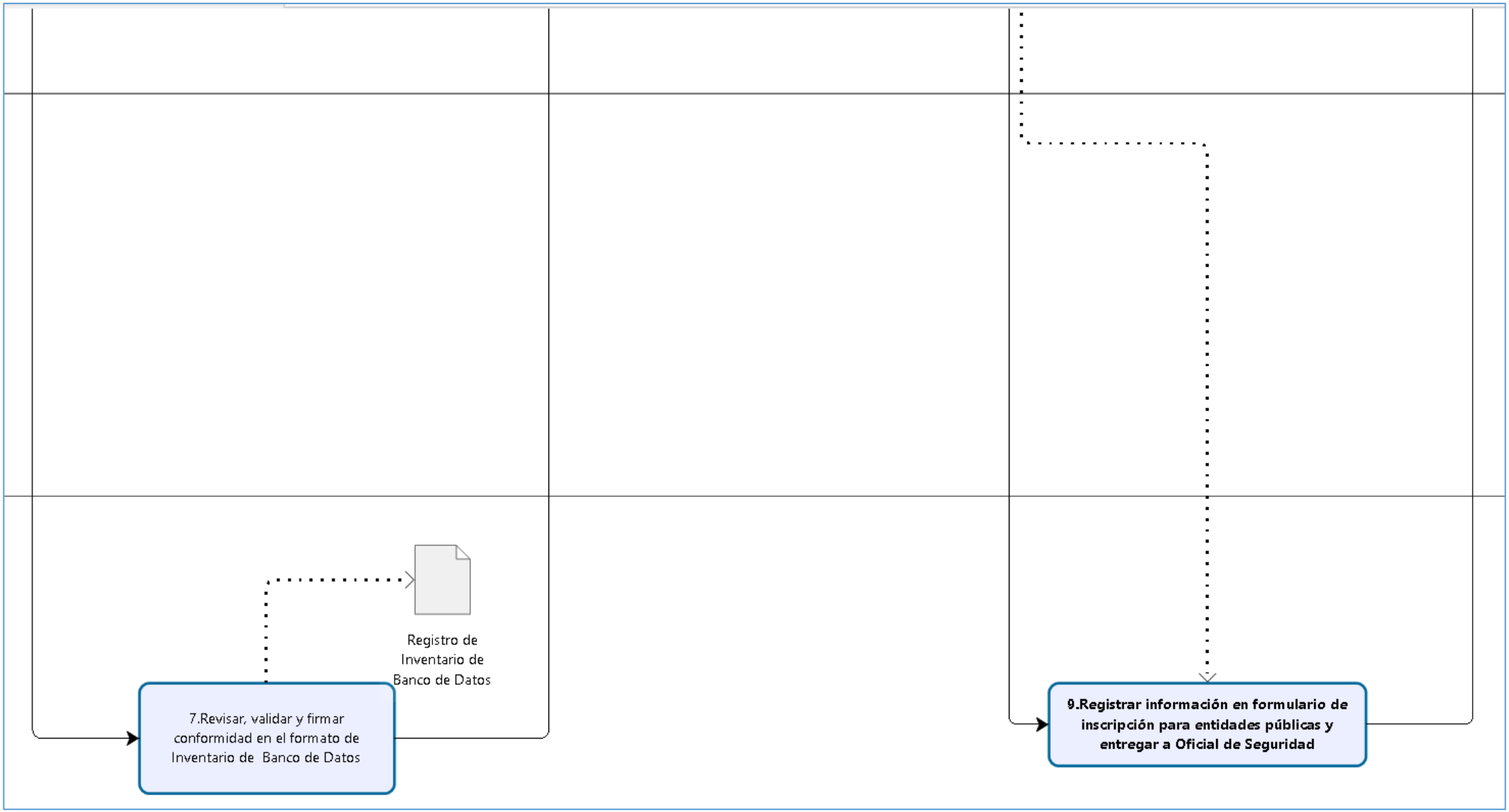


Figura N° 123: PE04.01.02.01 (Parte 5) - Diagrama BPMN 2.0

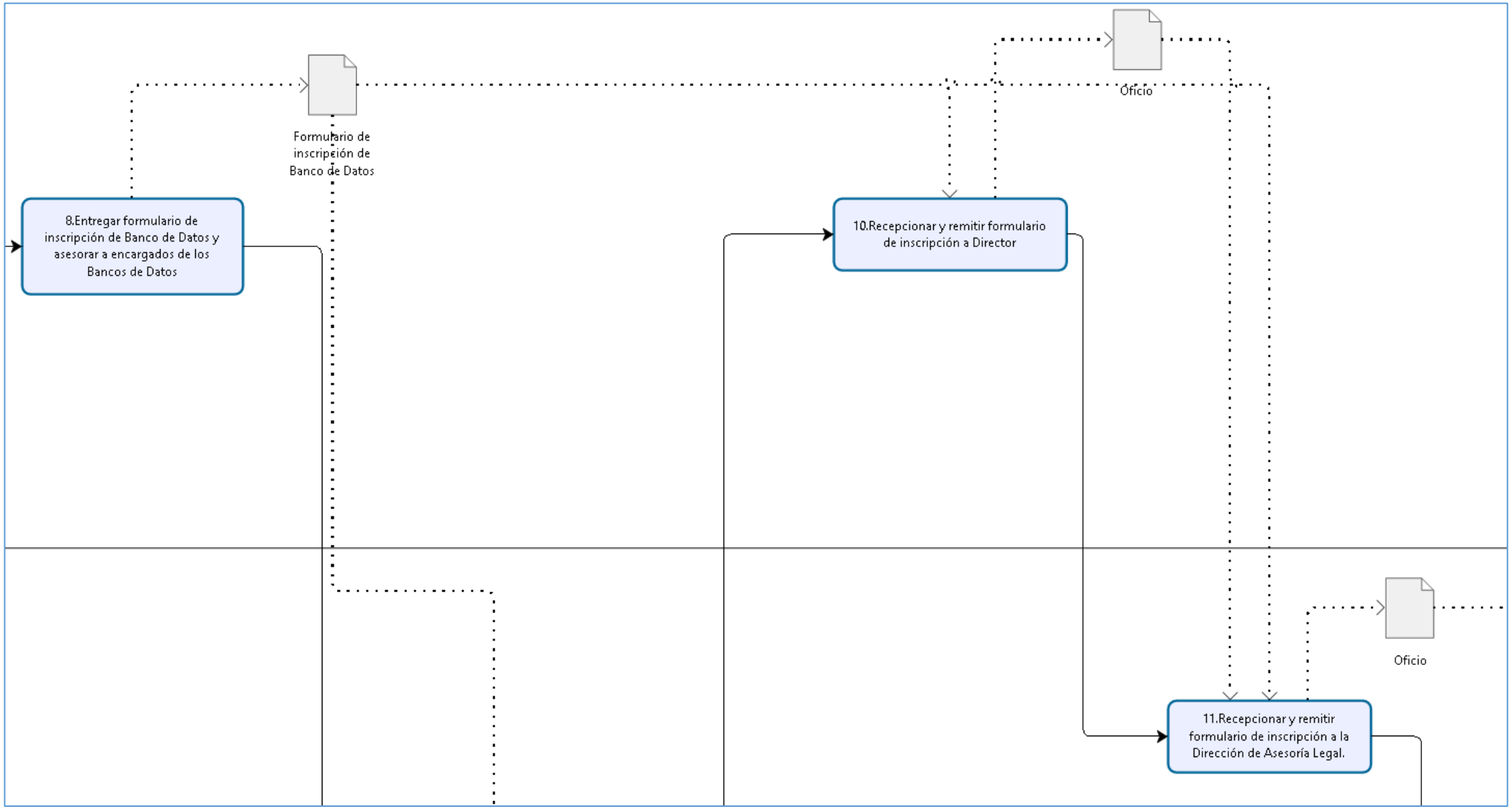


Figura N° 124: PE04.01.02.01 (Parte 6) - Diagrama BPMN 2.0

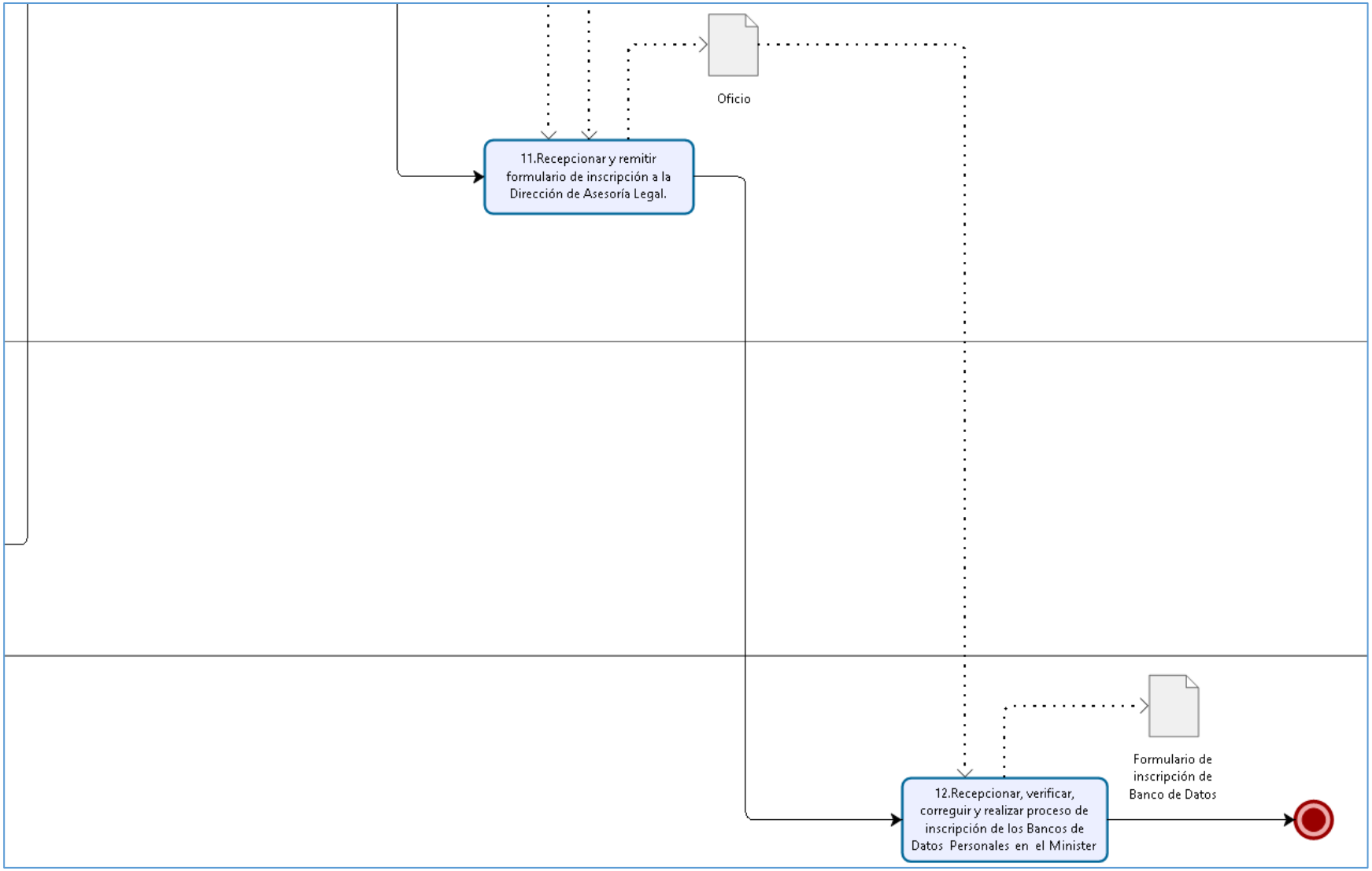


Tabla N° 37: Criterios para Clasificar Banco de Datos Personales

Criterios para Clasificar Banco de Datos Personales según la Directiva de Seguridad de LPDP										
Nivel	**Categoría**	**Tipo de Titular del Banco de Datos Personales es Persona Natural**	**Tipo de Titular del Banco de Datos Personales es Persona Jurídica**	**Tipo de Titular del Banco de Datos Personales es Entidad Pública**	**Cantidad de Registros de Datos Personales**	**Cantidad de tipos de Datos Personales**	**Datos Sensibles**	**Período para cumplir con la Finalidad**	**Múltiples Oficinas**	**Finalidad del tratamiento respaldado por Norma Legal**
1	**Básico**	Aplica	No Aplica	No Aplica	Hasta 50	Hasta 5	No	Hasta 1 año	No	No Aplica
2	**Simple**	Aplica	Aplica	No Aplica	Hasta 100	Más de 5	No	Hasta 1 año	No	No Aplica
3	**Intermedio**	Aplica	Aplica	No Aplica	Hasta 1 000	Más de 5	Si	Mayor a 1 año	Si	No Aplica
4	**Complejo**	No Aplica	Aplica	Aplica (*)	Indeterminado	Más de 5	Si	Mayor a 1 año	Si	No Aplica
5	**Crítico**	No Aplica	Aplica	Aplica (*)	Indeterminado	Más de 5	Si	Mayor a 1 año	Si	Aplica (**)
				Leyenda: **(*) Define Banco de Datos, tipo Complejo u Crítico**			**Leyenda:** **(**) Define Banco de Datos, tipo Crítico se debe implementar un SGSI 27001 vigente**			

Tabla N° 38: Inventario de Banco de Datos Personales

INVENTARIO DE BANCO DE DATOS PERSONALES DE LA UNIVERSIDAD NACIONAL DEL SANTA												
Código	**Nombre**	**Descripción y Finalidad**	**Tipo de Titular del Banco de Datos Personales**	**Responsable**	**Tipo de Tratamiento**	**Cantidad de Registros de Datos Personales**	**Cantidad de tipo de Datos Personales**	**Datos Sensibles**	**Período para cumplir con la Finalidad**	**Múltiples Oficinas**	**Finalidad Legal**	**Clasificación (Según directiva)**
BDP-001	**Postulantes Pregrado y Posgrado**	**Administrar los datos personales de los postulantes a los programas de pregrado y posgrado, para fines de atención de su postulación, cobros de derechos por postulación, permitir que las autoridades de la institución educativa de la cual proviene consulten los resultados de su participación en el proceso de admisión, informar sobre**	**Entidad Pública**	**Universidad Nacional del Santa**	**Mixto**	**Indeterminado**	**Más de 5**	**Si**	**Mayor a 1 año**	**Si**	**Aplica**	**Crítico**

		la oferta educativa de la UNS, en general para el cumplimiento de cualquier finalidad conexa con su postulación a la UNS.										
BDP-002	Alumnos y Egresados		Entidad Pública	Universidad Nacional del Santa	Mixto	Indeterminado	Más de 5	Si	Mayor a 1 año	Si	Aplica	**Crítico**
BDP-003	Postulantes a Docentes y Colaboradores Administrativos		Entidad Pública	Universidad Nacional del Santa	No Automatizado	Hasta 100	Más de 5	No	Hasta 1 año	No	No Aplica	**Complejo**
BDP-004	Docentes		Entidad Pública	Universidad Nacional del Santa	Mixto	Indeterminado	Más de 5	Si	Mayor a 1 año	Si	Aplica	**Crítico**

BDP-005	Colaboradores Administrativos		Entidad Pública	Universidad Nacional del Santa	Mixto	Indeterminado	Más de 5	Si	Mayor a 1 año	Si	Aplica	**Crítico**
BDP-006	Representantes de Convenios		Entidad Pública	Universidad Nacional del Santa	No Automatizado	Hasta 1 000	Más de 5	No	Mayor a 1 año	Si	No Aplica	**Complejo**
BDP-007	Proveedores		Entidad Pública	Universidad Nacional del Santa	Mixto	Hasta 1 000	Más de 5	No	Mayor a 1 año	Si	No Aplica	**Complejo**
BDP-008	Clientes		Entidad Pública	Universidad Nacional del Santa	No Automatizado	Hasta 100	Más de 5	Si	Mayor a 1 año	Si	No Aplica	**Complejo**
BDP-009	Visitantes (uso de los servicios de la UNS)		Entidad Pública	Universidad Nacional del Santa	No Automatizado	Hasta 50	Hasta 5	No	Hasta 1 año	Si	No Aplica	**Complejo**
BDP-010	Videovigilancia		Entidad Pública	Universidad Nacional del Santa	No Automatizado	Hasta 100	Hasta 5	No	Hasta 1 año	Si	No Aplica	**Complejo**
BDP-011	Alumnos de Institución Educativa		Entidad Pública	Universidad Nacional del Santa	No Automatizado	Hasta 1 000	Más de 5	Si	Mayor a 1 año	Si	No Aplica	**Complejo**

BDP-012	Padres y/o Apoderados de Familia de Institución Educativa		Entidad Pública	Universidad Nacional del Santa	Mixto	Hasta 1 000	Más de 5	No	Mayor a 1 año	Si	No Aplica	**Complejo**

El Banco de Datos Personales de Admisión es del tipo **crítico** por tanto se requiere la implementación de un SGSI basado en la Norma ISO/IEC 27001:2013.

5.3 Fase III - Análisis de Brechas

5.3.1 Objetivos de la Fase III

- Elaborar una adaptación del Modelo CMMI para medir el nivel de madurez relacionado a la seguridad de la información en la Universidad.

- Evaluar el nivel de madurez de los requisitos de la Norma ISO/IEC 27001:2013 y determinar las brechas.

- Integrar los controles de la Norma ISO/IEC 27002:2013 con los controles dispuestos por la Directiva de Seguridad de la Ley de Protección de Datos Personales.

- Evaluar el nivel de madurez de los controles de la Norma ISO/IEC 27002:2013 y la Directiva de Seguridad de la Ley de Protección de Datos Personales, a fin de determinar las brechas.

5.3.2 Marco de Trabajo la Fase III

Evaluar el Nivel de Madurez de la Universidad respecto a la seguridad de la información y documentar las brechas encontradas.

5.3.3 Desarrollo de la Fase III

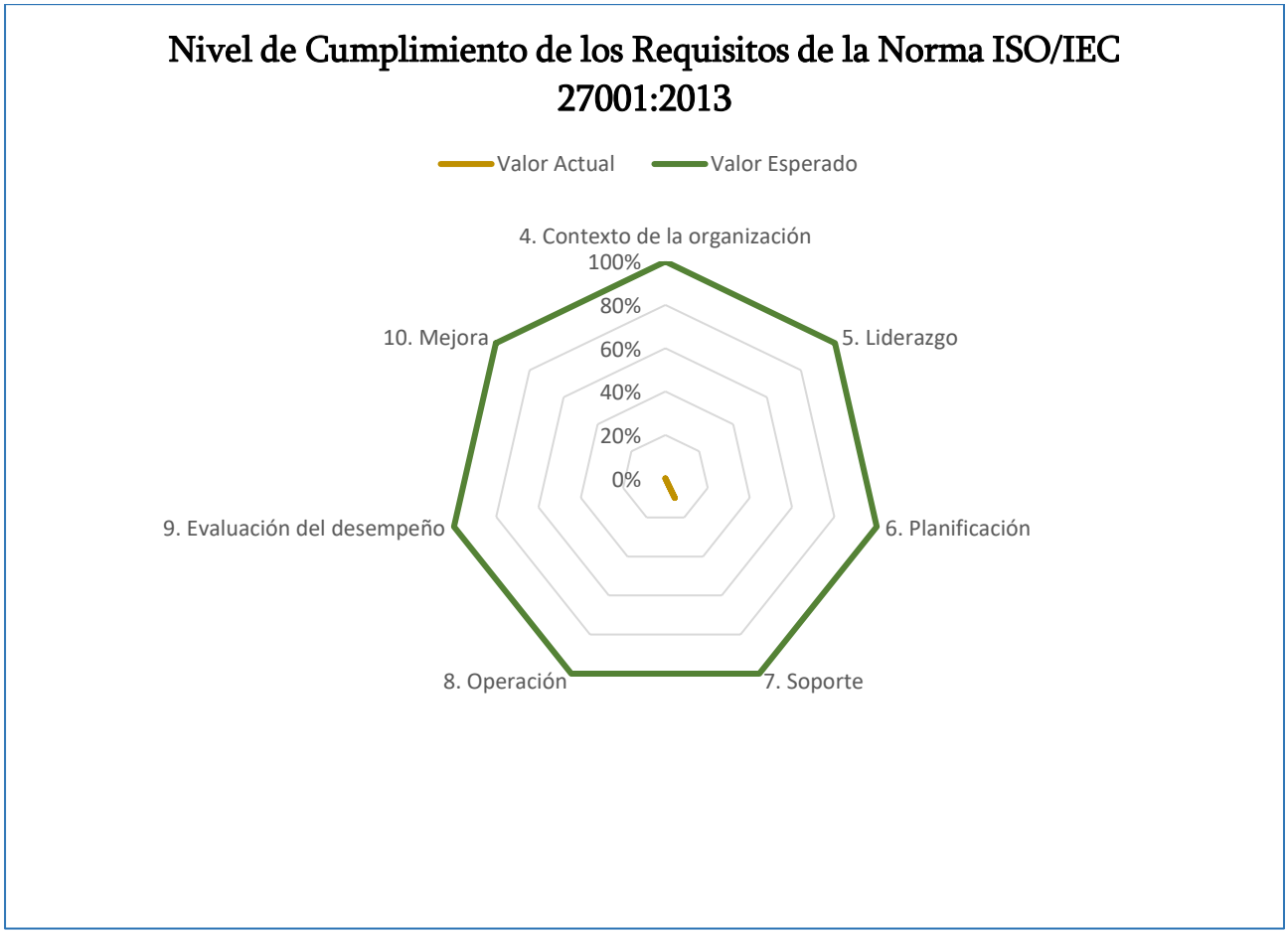
Tabla N° 39: Nivel de Madurez adaptado para la Seguridad de la Información

Modelo de Madurez de la Capacidad (CMMI)		
Estado	**Descripción**	**Valoración Cualitativa**
Desconocido	Todavía no ha sido revisado.	0%
Inexistente	Completa falta de política reconocible, procedimiento, control, etc.	0%
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para cumplir con los requerimientos.	10%
Limitado	Progresando de manera correcta pero todavía no completado	50%
Definido	Desarrollo más o menos completo aunque el detalle es deficiente y/o todavía no se ha implementado y respaldado activamente por la Alta Dirección.	70%
Gestionado	Desarrollo está completo, el proceso/control ha sido implementado y recientemente comenzó a operar.	90%
Optimizado	El requerimiento es completamente satisfactorio, está operando plenamente como era de esperar, está iniciando el monitoreo y mejora activamente, y existe evidencia substancial para probar todo a los auditores	100%

Tabla N° 40: Nivel de Cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013

Clausula	Nivel de Madurez Actual	Valor Actual	Valor Esperado
4. Contexto de la organización	Inexistente	0%	100%
5. Liderazgo	Inexistente	0%	100%
6. Planificación	Inexistente	0%	100%
7. Soporte	Inicial	10%	100%
8. Operación	Inexistente	0%	100%
9. Evaluación del desempeño	Inexistente	0%	100%
10. Mejora	Inexistente	0%	100%

Figura N° 125: Grafico de Radar de cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013



El Nivel de Madurez de los requisitos de la Norma ISO/IEC 27001:2013, está en un estado **inexistente** en su mayoría por tanto se requerirá de un trabajo arduo para su implementación, los resultados se especifican en el Anexo A de la presente investigación.

Tabla N° 41: Nivel de Cumplimiento de los 114 Controles de la Norma ISO/IEC 27002:2013

Código del Control	Control ISO/IEC 27002:2013	Nivel de Madurez Actual	Valor Actual	Valor Esperado
A.5.1.1	Políticas para la seguridad de la información	Inexistente	0%	100%
A.5.1.2	Revisión de las políticas para la seguridad de la información	Inexistente	0%	100%
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Inexistente	0%	100%
A.6.1.2	Segregación de funciones	Limitado	50%	100%
A.6.1.3	Contacto con autoridades	Inicial	10%	100%
A.6.1.4	Contacto con grupos especiales de interés	Inexistente	0%	100%
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Inexistente	0%	100%
A.6.2.1	Política de dispositivos móviles	Inexistente	0%	100%
A.6.2.2	Teletrabajo	Inexistente	0%	100%
A.7.1.1	Selección	Inexistente	0%	100%
A.7.1.2	Términos y condiciones del empleo	Inexistente	0%	100%
A.7.2.1	Responsabilidades de la gerencia	Inexistente	0%	100%
A.7.2.2	Conciencia, educación y capacitación, sobre la seguridad de la información.	Limitado	50%	100%
A.7.2.3	Proceso disciplinario	Inexistente	0%	100%
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	Definido	70%	100%
A.8.1.1	Inventario de activos	Limitado	50%	100%
A.8.1.2	Propiedad de los activos	Limitado	50%	100%
A.8.1.3	Uso aceptable de los activos	Limitado	50%	100%
A.8.1.4	Retorno de activos	Definido	70%	100%
A.8.2.1	Clasificación de la información	Limitado	50%	100%
A.8.2.2	Etiquetado de la información	Inicial	10%	100%
A.8.2.3	Manejo de activos	Inicial	10%	100%
A.8.3.1	Gestión de medios removibles	Inexistente	0%	100%
A.8.3.2	Disposición de medios	Inexistente	0%	100%
A.8.3.3	Transferencia de medios físicos	Inexistente	0%	100%
A.9.1.1	Política de control de acceso	Limitado	50%	100%
A.9.1.2	Acceso a redes y servicios de red	Definido	70%	100%
A.9.2.1	Registro y baja de usuarios	Limitado	50%	100%
A.9.2.2	Aprovisionamiento de acceso a usuario	Limitado	50%	100%
A.9.2.3	Gestión de derechos de acceso privilegiados	Limitado	50%	100%
A.9.2.4	Gestión de información de autentificación secreta de usuarios	Limitado	50%	100%
A.9.2.5	Revisión de derechos de acceso a usuarios	Limitado	50%	100%
A.9.2.6	Remoción o ajuste de derechos de acceso	Limitado	50%	100%
A.9.3.1	Uso de información de autentificación secreta	Limitado	50%	100%
A.9.4.1	Restricción de acceso a la información	Limitado	50%	100%
A.9.4.2	Procedimientos de ingreso seguro	Limitado	50%	100%
A.9.4.3	Sistema de gestión de contraseñas	Limitado	50%	100%
A.9.4.4	Uso de programas utilitarios privilegiados	Limitado	50%	100%
A.9.4.5	Control de acceso al código fuente de los programas	Limitado	50%	100%

A.10.1.1	Política sobre el uso de controles criptográficos	Inicial	10%	100%
A.10.1.2	Gestión de claves	Inicial	10%	100%
A.11.1.1	Perímetro de seguridad física	Inicial	10%	100%
A.11.1.2	Controles de ingreso físico	Inicial	10%	100%
A.11.1.3	Asegurar oficinas, áreas e instalaciones	Inicial	10%	100%
A.11.1.4	Protección contra amenazas externas y ambientales	Inicial	10%	100%
A.11.1.5	Trabajo en áreas seguras	Inicial	10%	100%
A.11.1.6	Áreas de despacho y carga	Limitado	50%	100%
A.11.2.1	Emplazamiento y protección de los equipos	Limitado	50%	100%
A.11.2.2	Servicios de suministro	Limitado	50%	100%
A.11.2.3	Seguridad del cableado	Inicial	10%	100%
A.11.2.4	Mantenimiento de equipos	Inicial	10%	100%
A.11.2.5	Remoción de activos	Gestionado	90%	100%
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Limitado	50%	100%
A.11.2.7	Disposición o reutilización segura de equipos	Inexistente	0%	100%
A.11.2.8	Equipos de usuario desatendidos.	Inexistente	0%	100%
A.11.2.9	Política de escritorio limpio y pantalla limpia.	Inexistente	0%	100%
A.12.1.1	Procedimientos operativos documentados.	Inicial	10%	100%
A.12.1.2	Gestión de cambio	Inexistente	0%	100%
A.12.1.3	Gestión de la capacidad	Inexistente	0%	100%
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Limitado	50%	100%
A.12.2.1	Controles contra códigos maliciosos	Limitado	50%	100%
A.12.3.1	Respaldo de la información	Limitado	50%	100%
A.12.4.1	Registro de eventos	Limitado	50%	100%
A.12.4.2	Protección de información de registros	Limitado	50%	100%
A.12.4.3	Registro del administrador y operador	Inexistente	0%	100%
A.12.4.4	Sincronización del reloj	Inexistente	0%	100%
A.12.5.1	Instalación de software en sistemas operacionales	Inexistente	0%	100%
A.12.6.1	Gestión de vulnerabilidades técnicas	Inexistente	0%	100%
A.12.6.2	Restricciones sobre la instalación de software	Inexistente	0%	100%
A.12.7.1	Controles de auditoría de sistemas de información	Inexistente	0%	100%
A.13.1.1	Controles de la red	Inicial	10%	100%
A.13.1.2	Seguridad de servicios de red	Definido	70%	100%
A.13.1.3	Segregación en redes	Limitado	50%	100%
A.13.2.1	Políticas y procesamientos de transferencia de la información	Inexistente	0%	100%
A.13.2.2	Acuerdo sobre transferencia de información	Inexistente	0%	100%
A.13.2.3	Mensajes electrónicos	Inexistente	0%	100%
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Inexistente	0%	100%
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Limitado	50%	100%
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Inicial	10%	100%
A.14.1.3	Protección de transacciones en servicios de aplicación	Inexistente	0%	100%
A.14.2.1	Política de desarrollo seguro	Inexistente	0%	100%
A.14.2.2	Procedimientos de control de cambio del sistema	Inexistente	0%	100%
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Inexistente	0%	100%

A.14.2.4	Restricciones sobre cambios a los paquetes de software	Limitado	50%	100%
A.14.2.5	Principios de ingeniería de sistemas seguros.	Inicial	10%	100%
A.14.2.6	Ambiente de desarrollo seguro	Inicial	10%	100%
A.14.2.7	Desarrollo contratado externamente	Inicial	10%	100%
A.14.2.8	Pruebas de seguridad del sistema	Inexistente	0%	100%
A.14.2.9	Pruebas de aceptación del sistema.	Inicial	10%	100%
A.14.3.1	Protección de datos de prueba	Inexistente	0%	100%
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Inexistente	0%	100%
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Inicial	10%	100%
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Inexistente	0%	100%
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Inexistente	0%	100%
A.15.2.2	Gestión de cambios a los servicios de proveedores	Inexistente	0%	100%
A.16.1.1	Responsabilidades y procedimientos	Inexistente	0%	100%
A.16.1.2	Reporte de eventos de seguridad de la información	Inicial	10%	100%
A.16.1.3	Reporte de debilidades de seguridad de la información	Inexistente	0%	100%
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Inexistente	0%	100%
A.16.1.5	Respuesta a incidentes de seguridad de la información	Inexistente	0%	100%
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente	0%	100%
A.16.1.7	Recolección de evidencia	Inicial	10%	100%
A.17.1.1	Planificación de continuidad de seguridad de la información	Inicial	10%	100%
A.17.1.2	Implementación de continuidad de seguridad de la información	Inicial	10%	100%
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información.	Inexistente	0%	100%
A.17.2.1	Instalaciones de procesamiento de la información	Limitado	50%	100%
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Inicial	10%	100%
A.18.1.2	Derechos de propiedad intelectual	Inexistente	0%	100%
A.18.1.3	Protección de registros	Inexistente	0%	100%
A.18.1.4	Privacidad y protección de datos personales	Inexistente	0%	100%
A.18.1.5	Regulación de controles criptográficos	Inexistente	0%	100%
A.18.2.1	Revisión independiente de la seguridad de la información	Inexistente	0%	100%
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Inexistente	0%	100%
A.18.2.3	Revisión del cumplimiento técnico	Inexistente	0%	100%

Figura N° 126: Grafico de Radar de cumplimiento de los controles de la Norma ISO/IEC 27002:2013

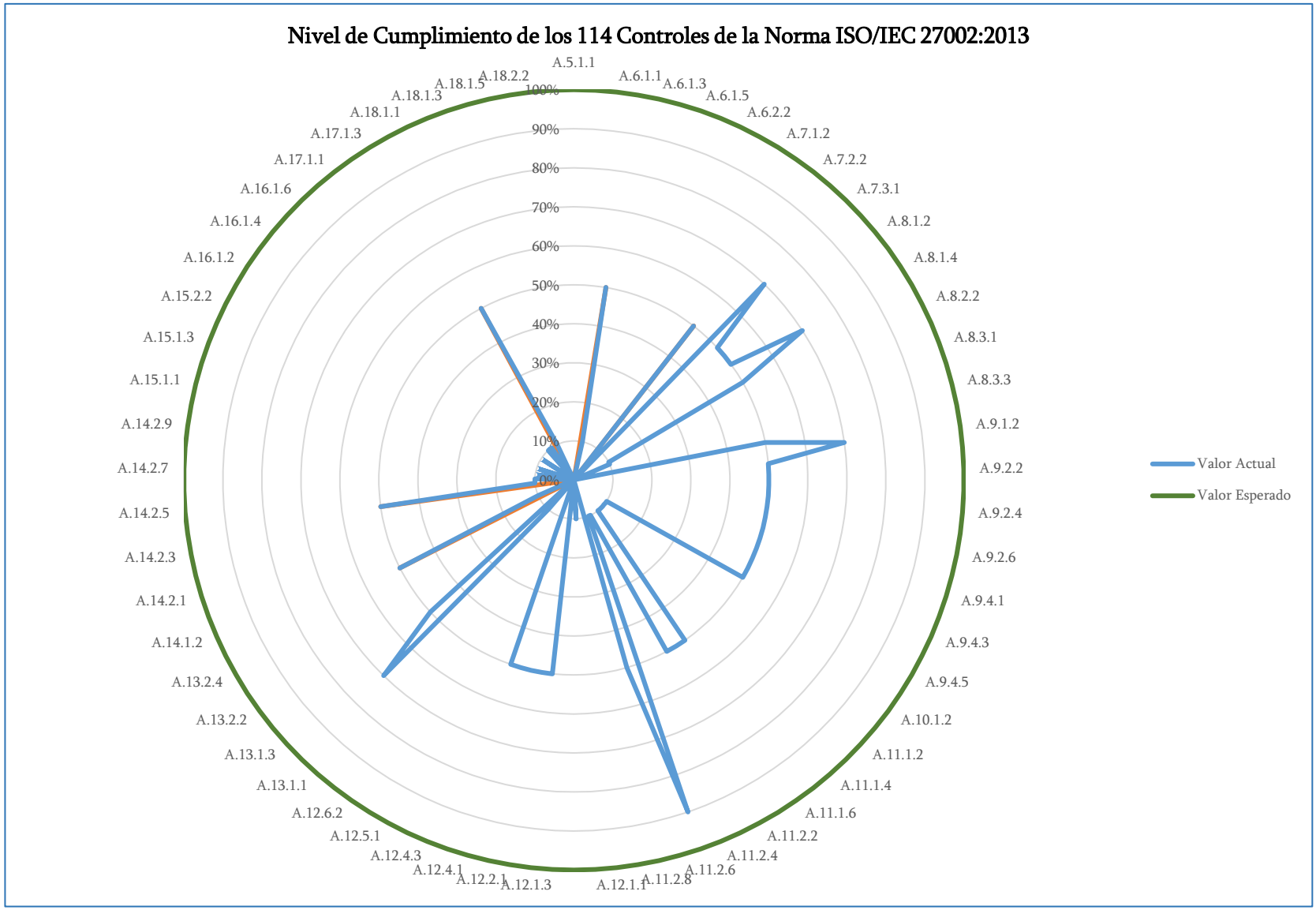
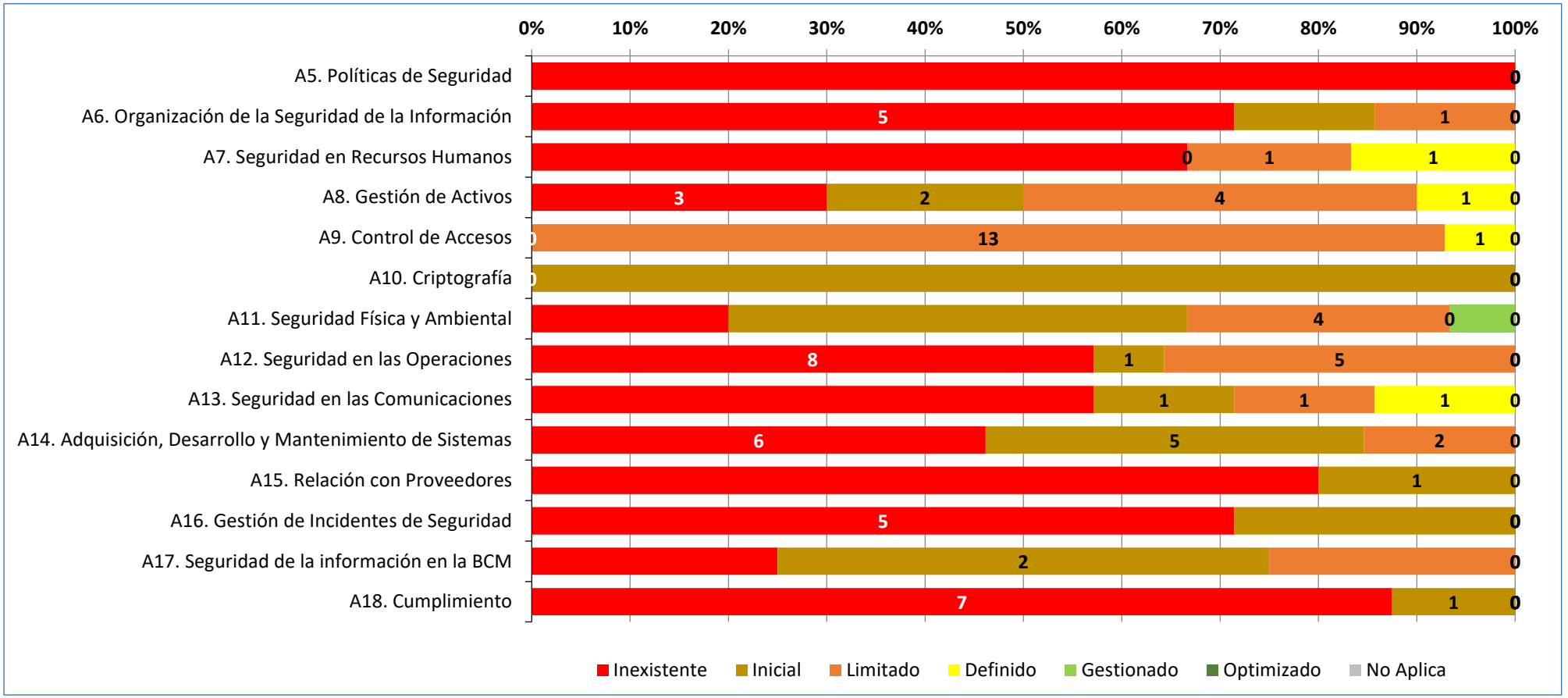


Figura N° 127: Grafico de Barras de cumplimiento de los controles a nivel de dominio del Anexo A de la Norma ISO/IEC 27001:2013



Se concluye que el Nivel de Madurez a **nivel de dominio del Anexo A de la Norma ISO/IEC 27001:2013 especificado en los 114 controles de la Norma ISO/IEC 27002:2013**, denota un alto porcentaje de inexistencia de controles administrativos y legales. Cabe precisar que algunos controles técnicos han iniciado un proceso de implementación. Los resultados se especifican en el Anexo B de la presente investigación.

5.4 Fase IV – Metodología de Análisis y Evaluación de Riesgos de Seguridad de la Información

5.4.1 Objetivos de la Fase IV

- Elaborar procedimientos documentados para la metodología análisis y evaluación de riesgos de seguridad de la información.

- Alinear los requisitos de la Norma ISO/IEC 31000:2009 de Gestión del Riesgo y la Norma ISO/IEC 27005:2011 de Gestión de Riesgos de Seguridad de la Información.

- Elaborar una metodología para analizar, evaluar y tratar los riesgos de seguridad de la información dentro del alcance del SGSI para esta investigación será el Proceso de Admisión de Pregrado de la Universidad. La Metodología en mención y sus formatos formaran parte del **Anexo C** de la presente investigación.

- Alinear los lineamientos establecidos por la Ley de Protección de Datos Personales, su reglamento y Directiva de Seguridad con la metodología de análisis y evaluación de Riesgos de Seguridad de la Información.

5.4.2 Marco de Trabajo de la Fase IV

Elaborar los procedimientos y formatos para poder realizar un adecuado análisis y evaluación de Riesgos de Seguridad de la Información.

5.4.3 Desarrollo de la Fase IV

Tabla N° 42: PE04.01.01.01 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO			**Código**:PE04.01.01.01	
				Versión: 1.0	
TIPO:	PROCEDIMIENTO		PROCESO DE NIVEL SUPERIOR:	PE04.01.01.Gestión de Seguridad de la Información	
TÍTULO:	Gestión de Riesgos de Seguridad de la Información				
A. OBJETIVO:	Identificar, evaluar, tratar y realizar seguimiento a los riesgos de seguridad de la información que afectan a los activos de información de los procesos de la Universidad.				
B. UNIDAD RESPONSABLE:	Dirección de Información y Documentación				
C. BASE LEGAL:	Resolución Ministerial 004-2016-PCM, Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, Resolución Ministerial Nº 166-2017-PCM, Modifican el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información, NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición, Ley de Protección de Datos Personales Ley N° 29733Decreto Supremo. Nº 003-2013-JUS Reglamento de la Ley de Protección de Datos Personales, Resolución Directoral Nº019-2013-JUS/DGPDP Autoridad Nacional de Protección de Datos Personales/Ministerio de Justicia y Derechos Humanos, Estatuto, Reglamento General.				
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de designación de Oficial de Seguridad de la Información.				

E. DESCRIPCIÓN DEL PROCEDIMIENTO:		DURACIÓN horas (8h por día)	ÓRGANO/UNIDAD ORGÁNICA	RESPONSABLE	F. REGISTROS
1	Identificar y valorar los activos de información de acuerdo a la Metodología de Riesgos de Seguridad de la Información vigente.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Inventario de Activos de Información
2	Identificar y evaluar amenazas relacionadas a los activos de información conforme a la Metodología de Evaluación de Riesgos de Seguridad de la Información vigente.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Evaluación de Riesgos
3	Realizar evaluación de los riesgos identificados utilizando la Metodología de Evaluación de Riesgos de Seguridad de la Información vigente.		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Evaluación de Riesgos

4	Identificar riesgos sobre los cuales se implementarán controles para su tratamiento, elaborando un plan de tratamiento de riesgos de seguridad de la información		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Evaluación de Riesgos
5	Revisar y aprobar el plan de tratamiento de riesgos de seguridad de la información con los controles propuestos para los riesgos de seguridad de la información determinados en el alcance del SGSI		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de plan de tratamiento de riesgos
6	Ejecutar el plan de tratamiento de los riesgos de seguridad de la información de acuerdo a las acciones definidas implementando los controles indicados		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de plan de tratamiento de riesgos
7	Identificar si se requiere actualizar la declaración de aplicabilidad(SOA) vigente correspondiente al nuevo análisis de riesgo efectuado		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de SOA
	Se realiza cambio en el SOA continuar, caso contrario ir a la actividad 11				
8	Actualizar SOA con los controles aplicables y no aplicables dentro del alcance del SGSI, solicitar la aprobación de la actualización		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de SOA, Oficio
9	Revisar y aprobar el SOA vigente		Dirección de Información y Documentación	Director DID	Registro de SOA, Oficio
10	Informar a la Vicerrectora Académica que se realizara la actualización del SOA		Dirección de Información y Documentación	Director DID	Oficio, Registro de SOA

11	Supervisar la efectividad de los controles implementados y controlar los riesgos residuales como se indica en la Metodología de Evaluación de Riesgos de Seguridad de la Información vigente		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Registro de Seguimiento de Riesgos
12	Informar al Director DID sobre la efectividad de los controles implementados		Dirección de Información y Documentación	Oficial de Seguridad de la Información	Oficio, Registro de Seguimiento de Riesgos

TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:	
H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento
I. ANEXOS:	

ETAPA	RESPONSABLE		FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 128: PE04.01.01.01 (General) - Diagrama BPMN 2.0

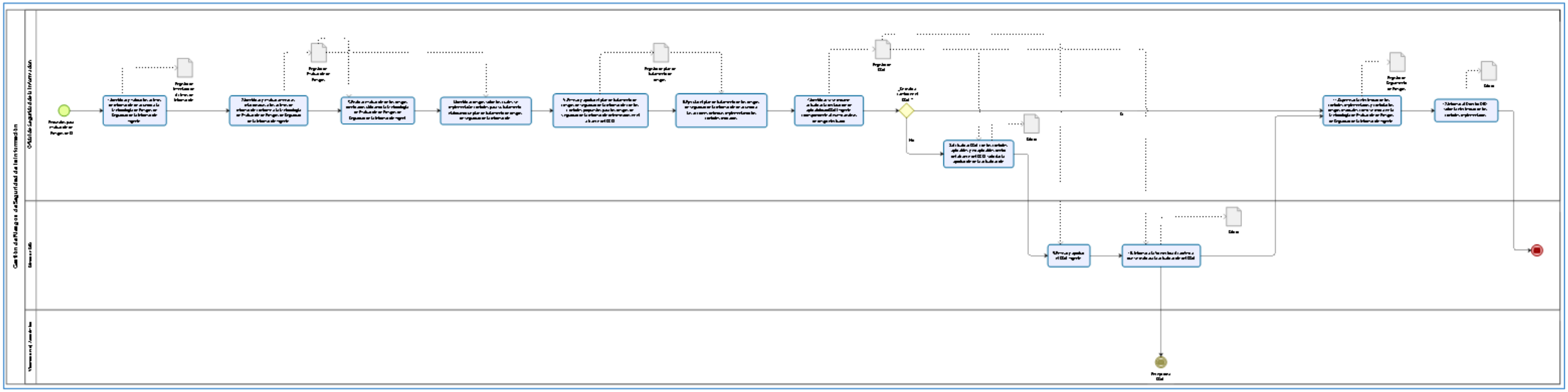


Figura N° 129: PE04.01.01.01 (Parte 1) - Diagrama BPMN 2.0

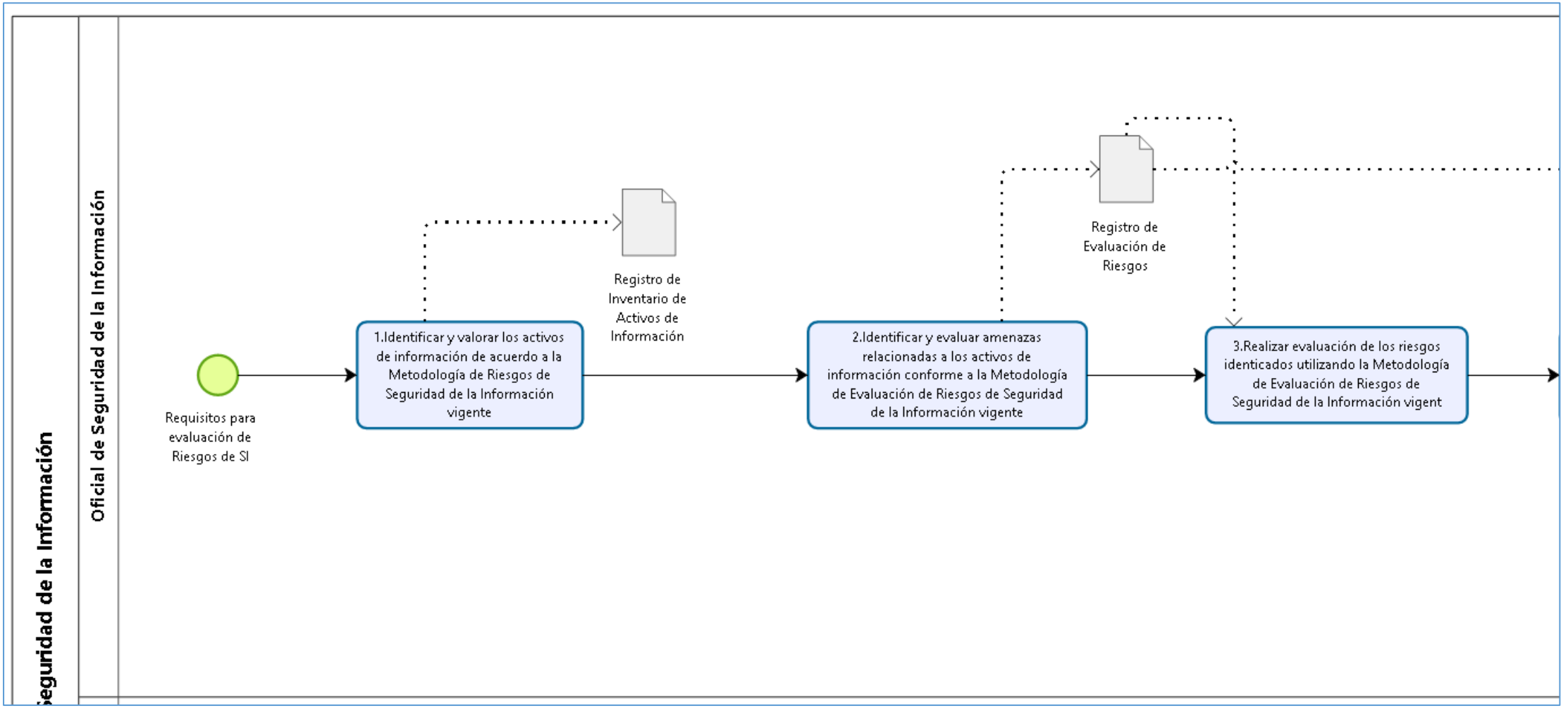


Figura N° 130: PE04.01.01.01 (Parte 2) - Diagrama BPMN 2.0

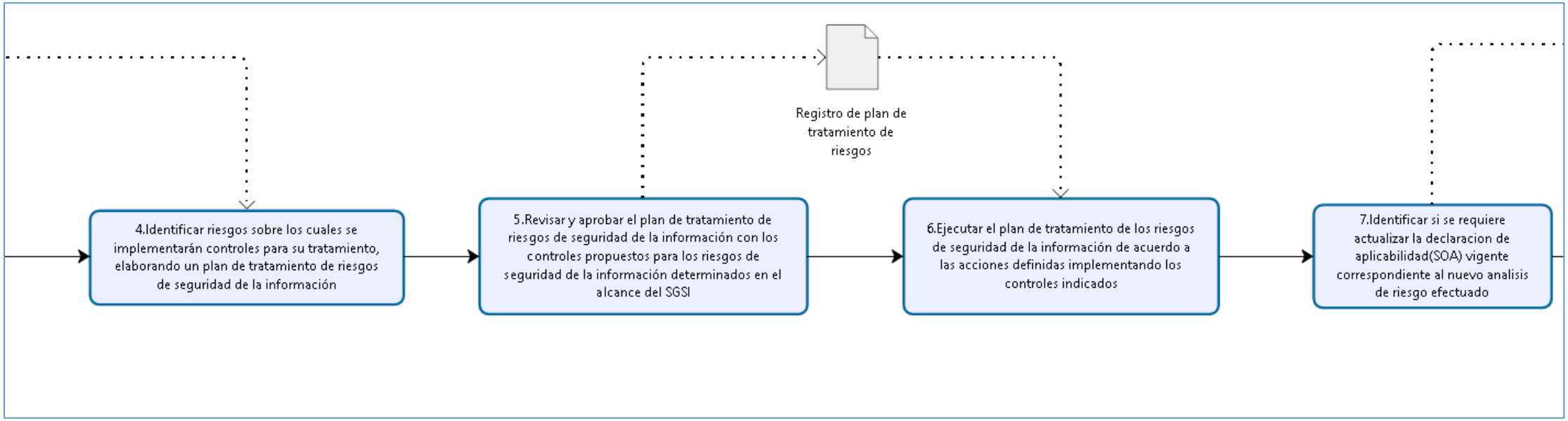


Figura N° 131: PE04.01.01.01 (Parte 3) - Diagrama BPMN 2.0

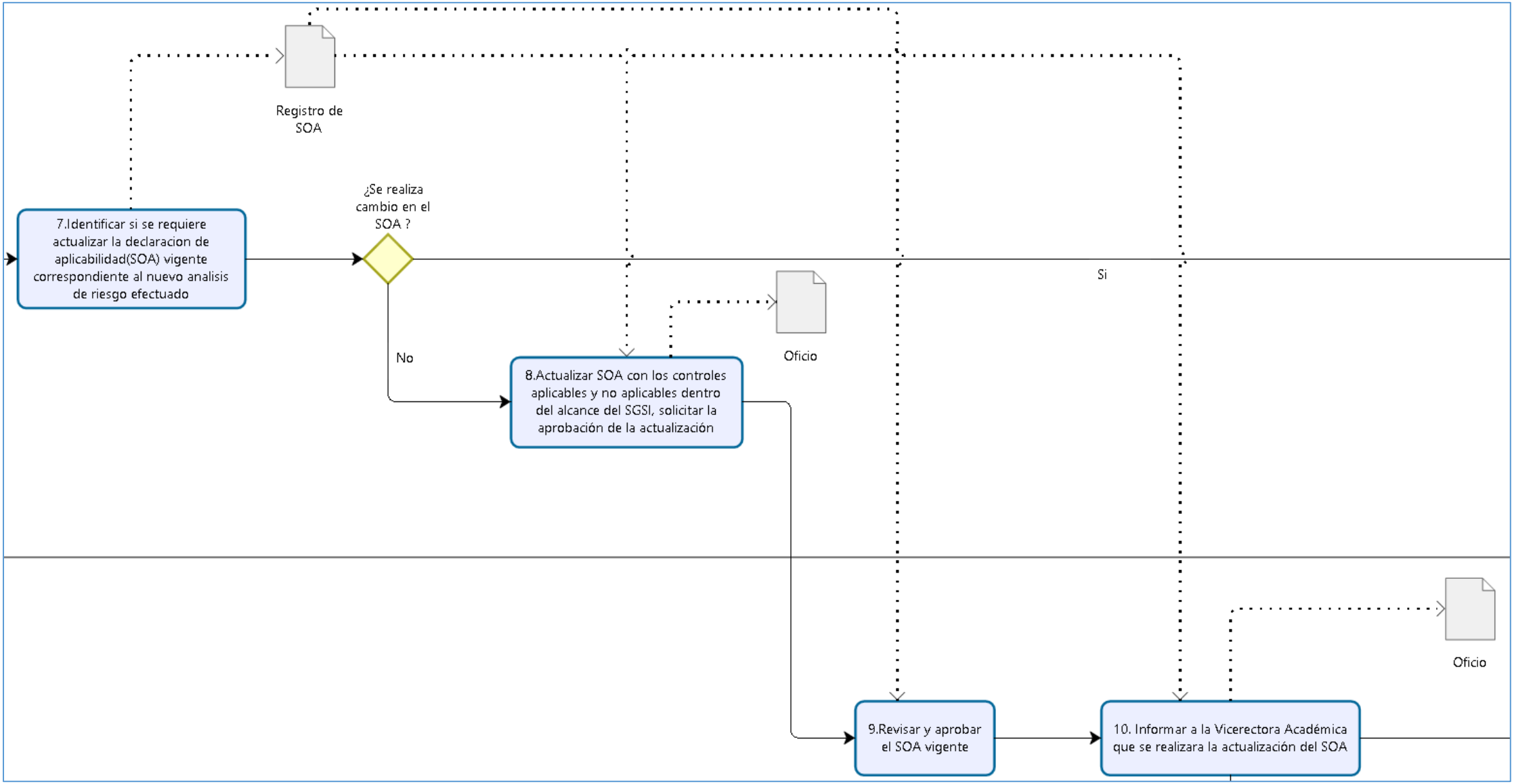


Figura N° 132: PE04.01.01.01 (Parte 4) - Diagrama BPMN 2.0

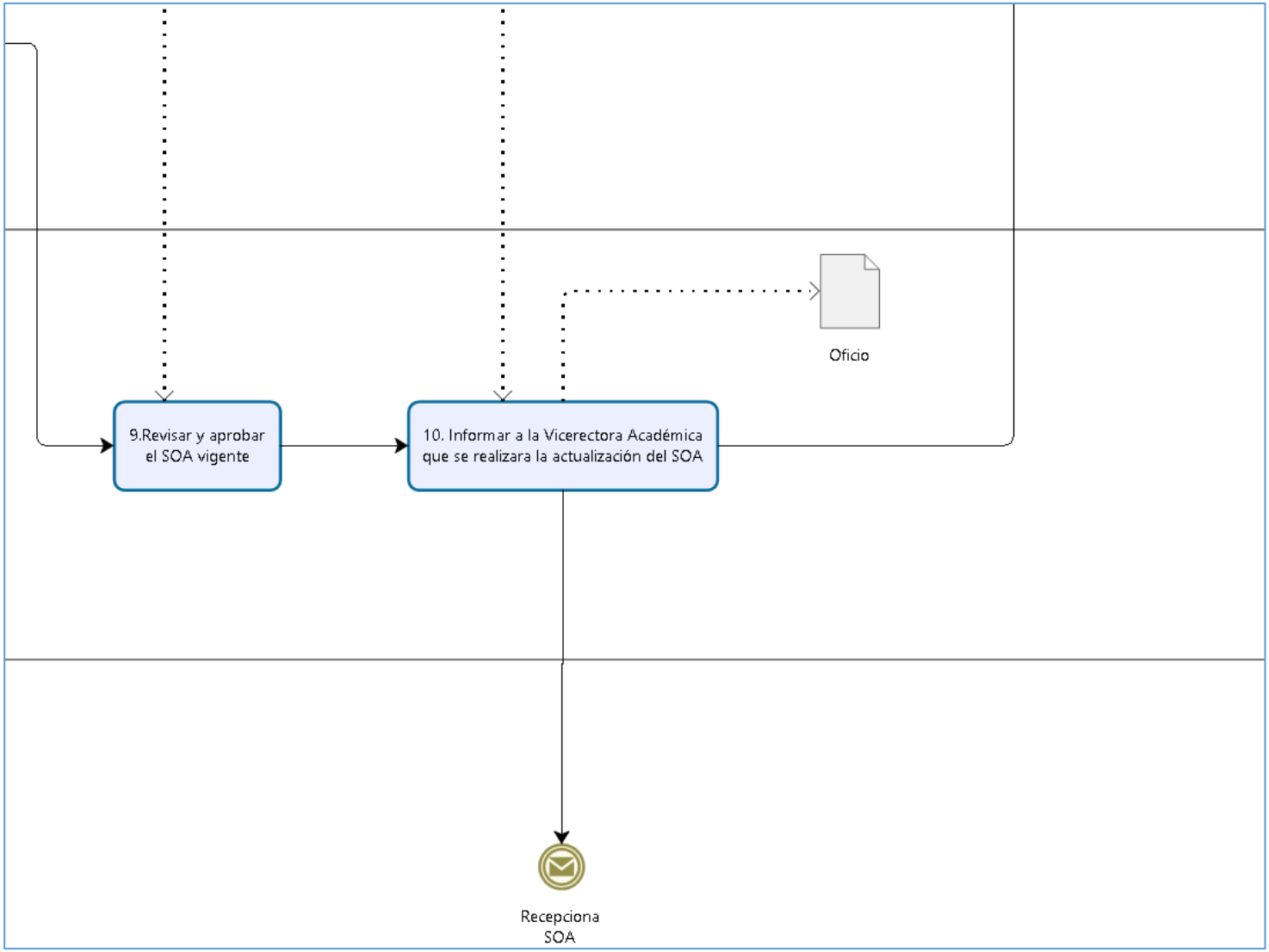
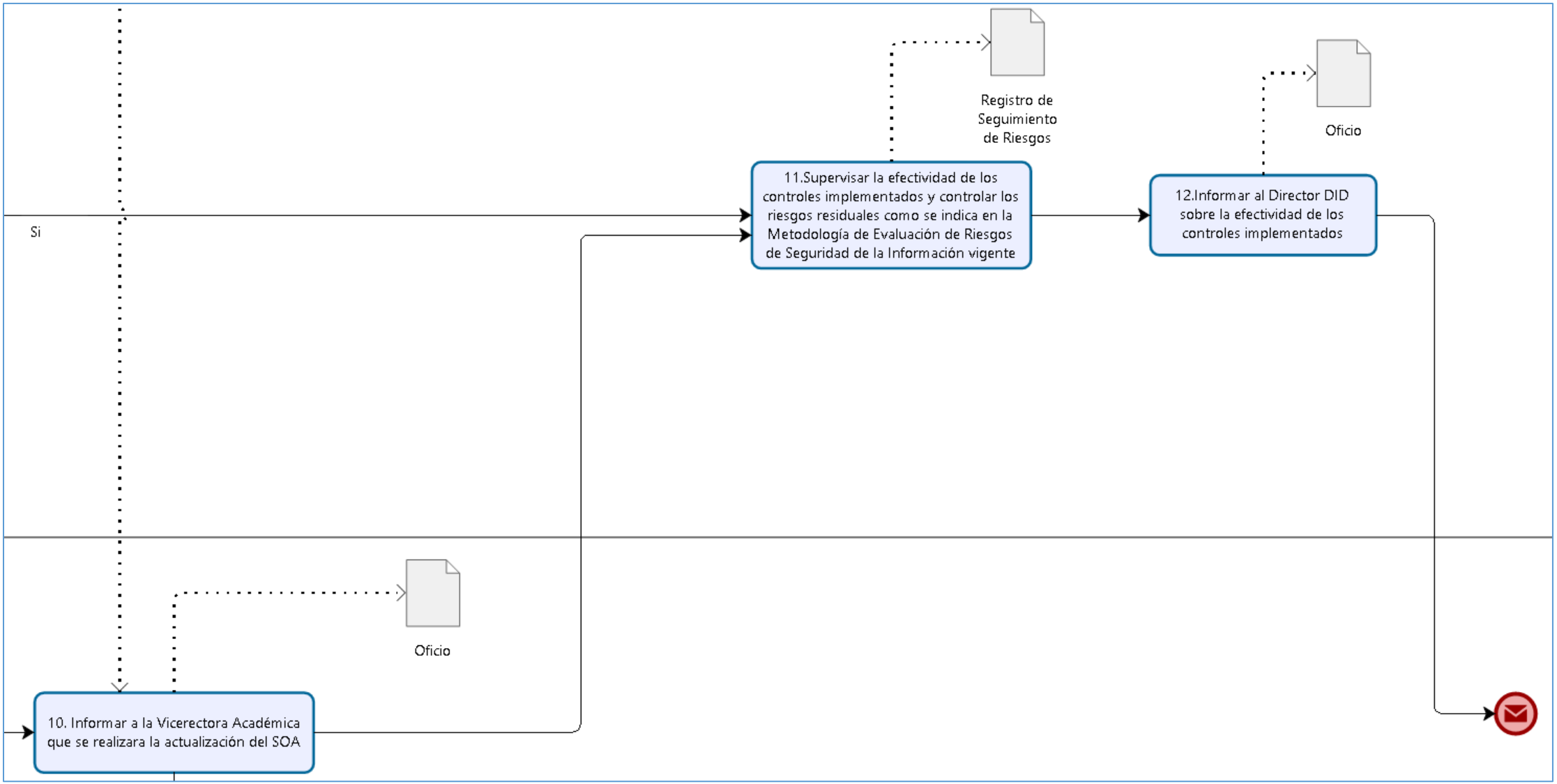


Figura N° 133: PE04.01.01.01 (Parte 5) - Diagrama BPMN 2.0



5.5 Fase V – Elaboración de aviso de privacidad y procedimiento de derechos ARCO

5.5.1 Objetivos de la Fase V

- Elaborar procedimientos documentados para gestionar los derechos ARCO en la Universidad, los formatos mencionados en este procedimiento formaran parte del **Anexo D** de la presente investigación.

- Elaborar un modelo de acuerdo de privacidad del uso de datos personales para los postulantes a los programas de pregrado y posgrado de la Universidad, este documento formara parte del **Anexo E** de la presente investigación.

5.5.2 Marco de Trabajo de la Fase V

Elaborar los procedimientos documentados de gestión para dar cumplimiento a la Ley de Protección de Datos Personales, su reglamento y su directiva de seguridad.

5.5.3 Desarrollo de la Fase V

Tabla N° 43: PE04.01.02.02 - Ficha de Proceso

	FICHA DE PROCEDIMIENTO		**Código**:PE04.01.02.02 **Versión**: 1.0
TIPO:	PROCEDIMIENTO	PROCESO DE NIVEL SUPERIOR:	PE04.01.02.Gestión de Protección de Datos Personales
TÍTULO:	Gestión de derechos ARCO		
A. OBJETIVO:	Atender solicitud de derechos ARCO		
B. UNIDAD RESPONSABLE:	Dirección de Información y Documentación		
C. BASE LEGAL:	Ley de Protección de Datos Personales Ley N° 29733Decreto Supremo. Nº 003-2013-JUS Reglamento de la Ley de Protección de Datos Personales, Resolución Directoral Nº019-2013-JUS/DGPDP Autoridad Nacional de Protección de Datos Personales/Ministerio de Justicia y Derechos Humanos, Estatuto, Reglamento General, Reglamento de Admisión de Pregrado.		
D. REQUISITOS DEL PROCEDIMIENTO:	Plan Operativo Institucional, MOF, Resolución de aprobación de Política y Procedimientos de la Ley de Protección de Datos Personales.		

	E. DESCRIPCIÓN DEL PROCEDIMIENTO:	DURACIÓN horas (8h por día)	ÓRGANO/UNIDAD ORGÁNICA	RESPONSABLE	F. REGISTROS
1	Revisar instructivo de derechos ARCO en el portal web de la Universidad y descargar registro de solicitud.		Solicitante	Solicitante	Registro de solicitud de derechos ARCO, Registro de Portal Web
2	Revisar y llenar información en solicitud de derechos ARCO.		Solicitante	Solicitante	Registro de solicitud de derechos ARCO
3	Enviar solicitud firmada y escaneada a correo electrónico de atención de derechos ARCO.		Solicitante	Solicitante	Registro de solicitud de derechos ARCO
4	Recepcionar y evaluar solicitud e identificar Banco de Datos Personal		Dirección de Asesoría Legal	Director DAL	Registro de solicitud de derechos ARCO, Registro de Correo electrónico
5	Remitir solicitud a Encargado del Banco de Datos Personal.		Dirección de Asesoría Legal	Director DAL	Registro de solicitud de derechos ARCO, Oficio
6	Recepcionar y atender solicitud acorde con los plazos establecidos en el instructivo de solicitud de derechos de arco		Encargado del tratamiento del Banco de Datos Personal	Encargado del tratamiento del Banco de Datos Personal	Registro de solicitud de derechos ARCO, Oficio
7	Remitir atención realizada a la Dirección de Asesoría Legal.		Encargado del tratamiento del Banco de Datos Personal	Encargado del tratamiento del Banco de Datos Personal	Registro de solicitud de derechos ARCO, Oficio
8	Recepcionar, revisar y realizar envío de respuesta a solicitante vía correo electrónico.		Dirección de Asesoría Legal	Director DAL	Registro de solicitud de derechos ARCO, Oficio, Registro de Correo Electrónico
TIEMPO TOTAL EMPLEADO EN EL PROCEDIMIENTO:					

H. HOJA DE CONTROL DE CAMBIOS:	Versión 1.0: Elaboración del Documento		
I. ANEXOS:			
ETAPA	RESPONSABLE	FECHA	FIRMA Y SELLO
Formulado por:	Juan Carlos Guzman Comesaña		
Cargo			
Revisado por:			
Cargo			
Aprobado por:			
Cargo			

Figura N° 134: PE04.01.02.02 (General) - Diagrama BPMN 2.0

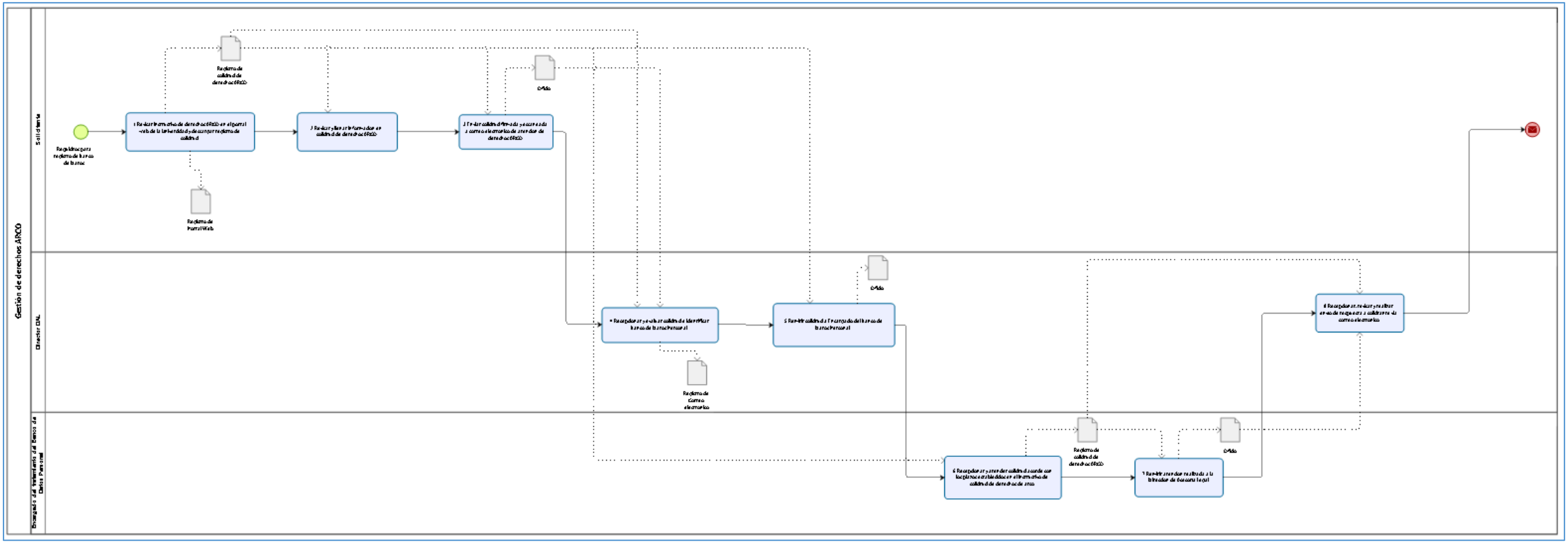


Figura N° 135: PE04.01.02.02 (Parte 1) - Diagrama BPMN 2.0

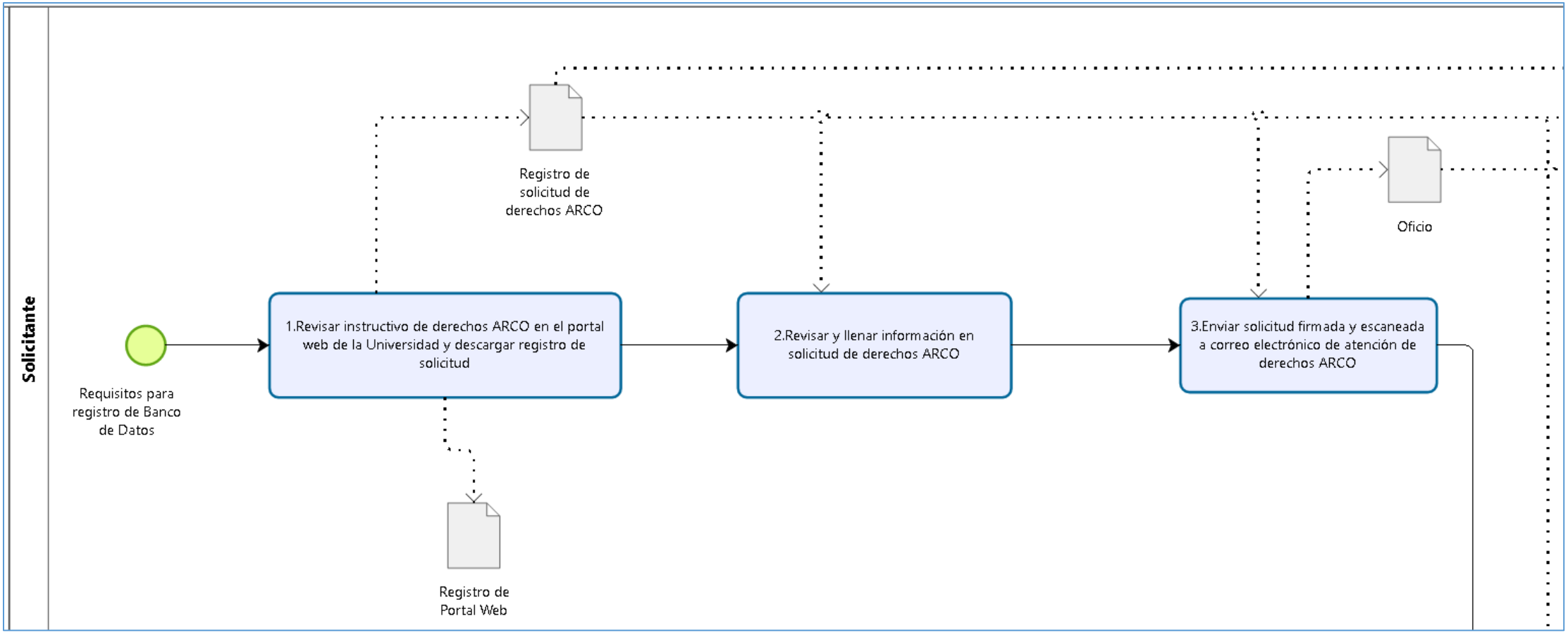


Figura N° 136: PE04.01.02.02 (Parte 2) - Diagrama BPMN 2.0

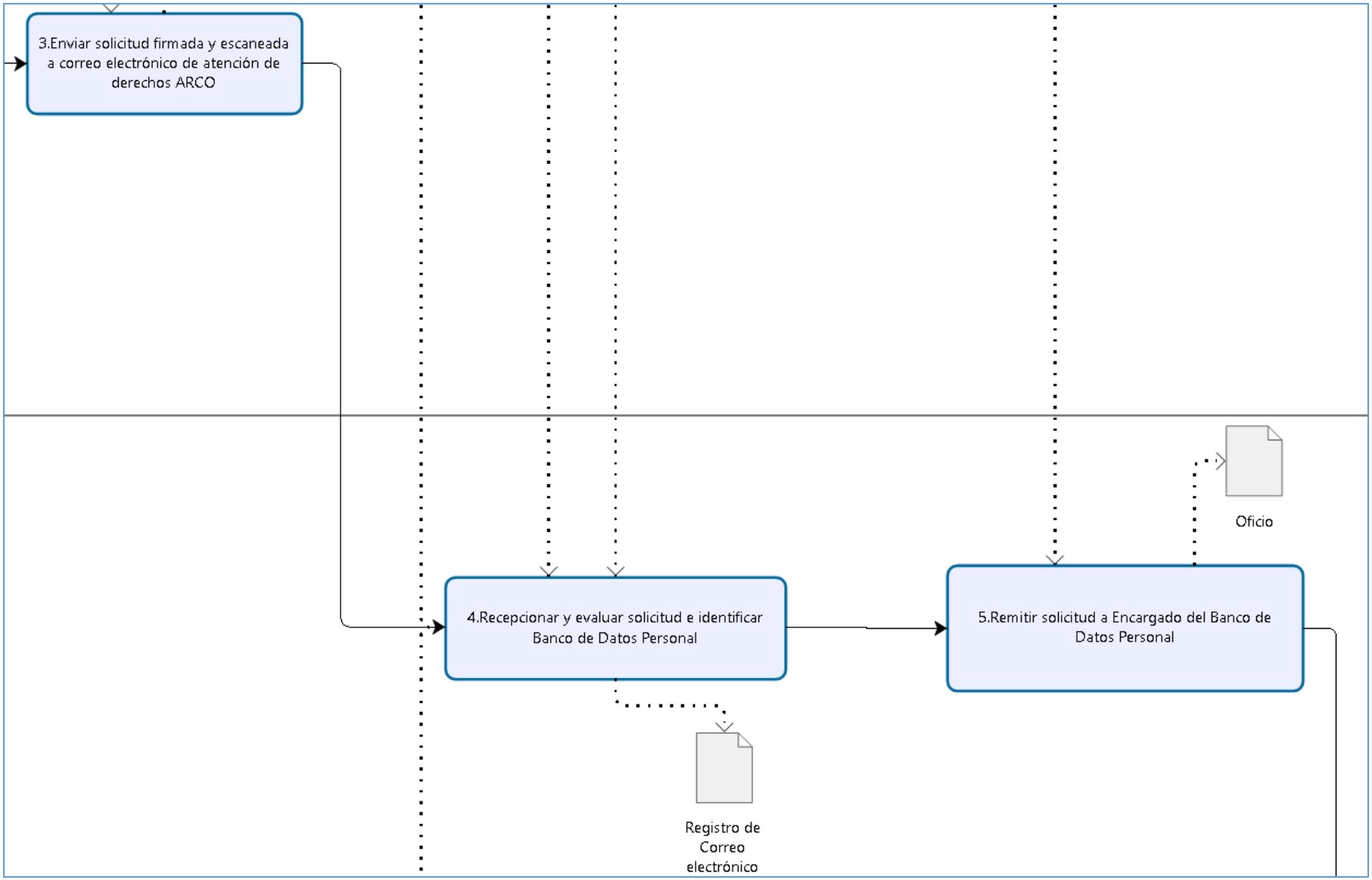


Figura N° 137: PE04.01.02.02 (Parte 3) - Diagrama BPMN 2.0

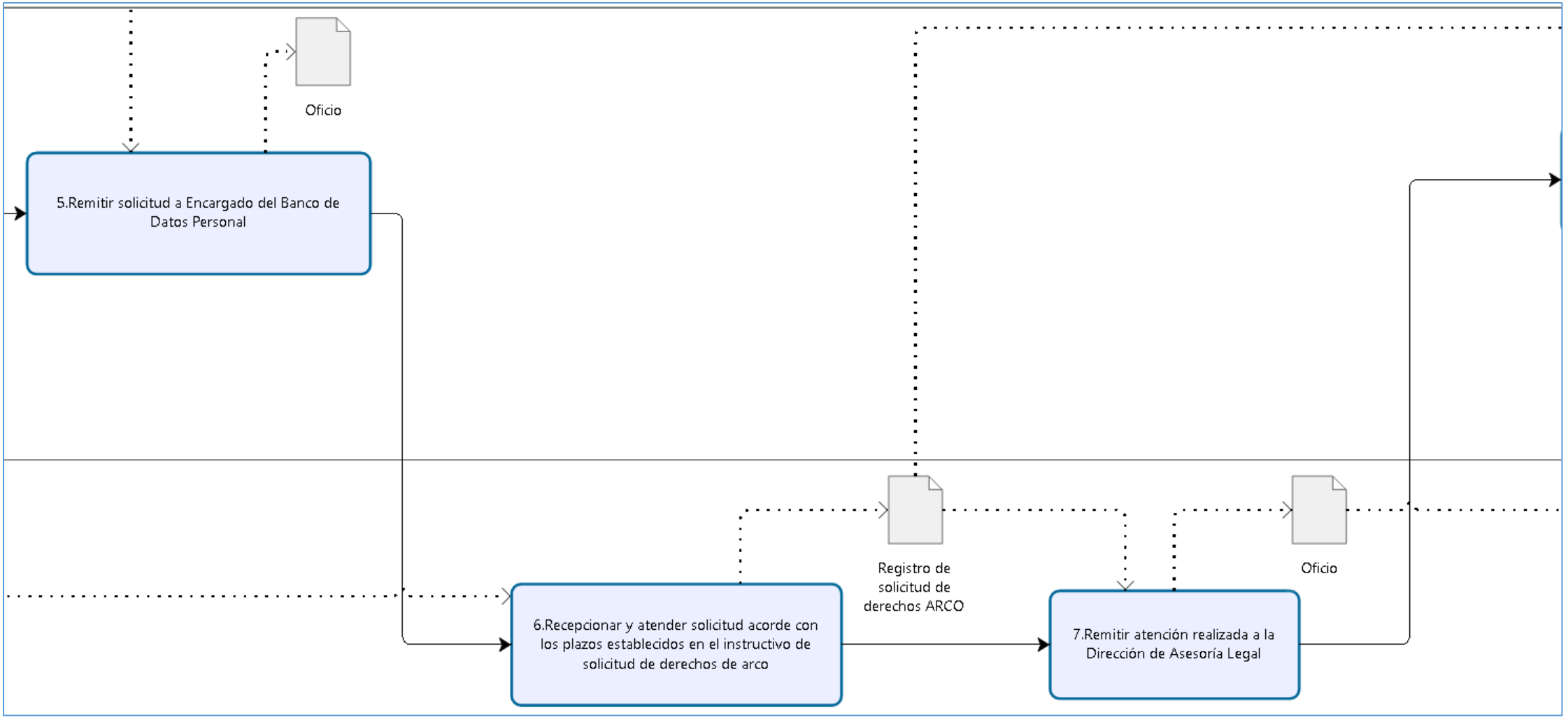
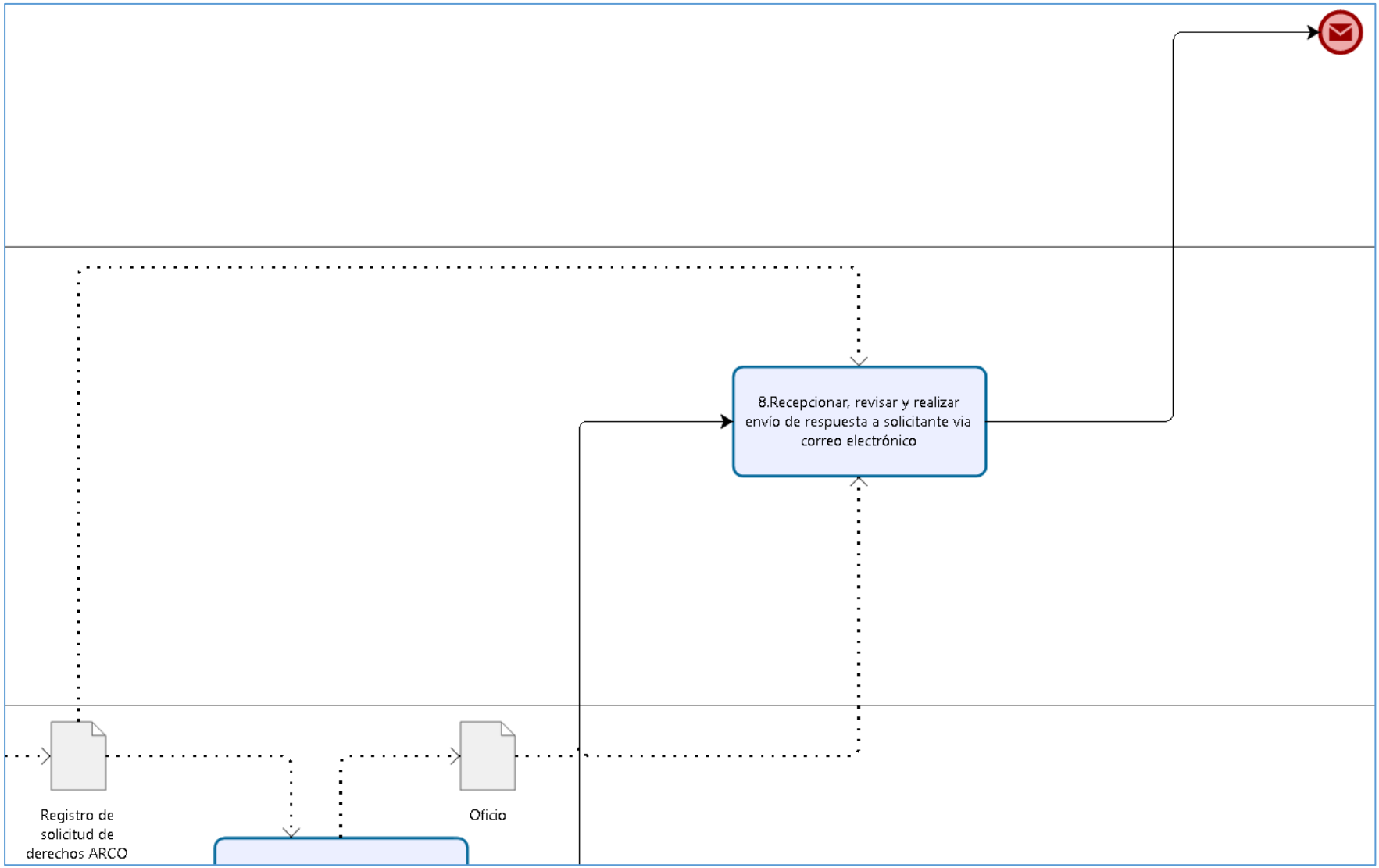


Figura N° 138: PE04.01.02.02 (Parte 4) - Diagrama BPMN 2.0



CAPITULO VI: DISCUSIÓN

6.1. Calidad de la Validez Interna

La presente investigación conto con la participación del Director de Admisión el Ms. Joel Herradda Villanueva quien en compañía de su equipo conformado por el Ing. Manco Pulido (Coordinador Académico) y el Lic. Manuel Chiroque Farfán (Coordinador Administrativo) brindaron las facilidades en sus tiempos disponibles, como evidencia se cuenta con audios de las entrevistas realizadas respecto al Proceso de Admisión de Estudiantes de Pregrado. Finalmente el Director de Admisión expidió una carta validando las actividades de análisis, diseño y documentación del Proceso de Admisión de Estudiantes de Pregrado, la cual forma parte del **Anexo F**.

6.2. Calidad de la Validez Externa

6.2.1. Implementación del Método Delphi

Para la implementación del método Delphi, se tuvo los siguientes considerandos:

A. **La Anonimidad:** Durante la elaboración del método Delphi, los expertos no se conocen entre sí, la cual brinda los siguientes aspectos positivos, como son:

- La imparcialidad de los miembros de influenciar o ser influenciados por otros en su evaluación.
- Permite que un experto pueda cambiar su opinión sin que otro se entere por tanto su imagen profesional no podría ser cuestionada.

B. **Ciclo de repetición:** Los expertos tuvieron la oportunidad de cambiar de opinión en la encuesta, conforme el investigador fue desarrollando el modelo y generando las mejoras comunicadas vía telefónica logrando así validar la información que brindaron o rectificándola, puesto que la encuesta se dejó abierta hasta la fecha de cierre que fue el 04/12/2017.

Para el desarrollo se contó con la participación de Cinco (5) expertos en seguridad de la información, que alimentaron la encuesta online, acorde con los considerandos explicados.

Las coordinaciones se realizaron vía llamadas telefónicas con cada uno de los expertos y se definió una lista de preguntas a utilizar como el insumo principal para comenzar el proceso del método Delphi para validar el modelo, de las entrevistas telefónicas surgió un banco de preguntas que se constituiría en un total de Nueve (9) preguntas distribuidas en Cinco (5) Bloques enviados a los expertos para su evaluación. A continuación se detalla:

Tabla N° 44: Formato de Encuesta Método Delphi

Encuesta para Juicio de Expertos para validar Proyecto de Tesis		Resultados		
		Experto 1	Experto 2 …	Experto 5
Bloque I	**I. Gestión por procesos BPMN 2.0**			
Preguntas	**Descripción**			
1	¿El Marco de Referencia cumple con el Estándar BPMN 2.0 para la gestión por procesos?			
Bloque II	**II. Banco de Datos Personales**			
Preguntas	**Descripción**			
2	¿El Marco de Referencia permite la identificación de los Bancos de Datos Personales acorde con la Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad?			
Bloque III	**III. Análisis de Brechas**			
Preguntas	**Descripción**			
3	¿El Marco de Referencia permite la identificación de brechas de cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013?			
4	¿El Marco de Referencia permite la identificación de brechas de cumplimiento de los Controles de la Norma ISO/IEC 27002:2013?			
5	¿El Marco de Referencia permite integrar los Controles de la Norma ISO/IEC 27002:2013 y los de la Directiva de Seguridad de Protección de Datos Personales?			
Bloque IV	**IV. Gestión de Riesgos de Seguridad de la Información**			
Preguntas	**Descripción**			
6	¿El Marco de Referencia permite una adecuada identificación de activos de información mediante la Metodología de Riesgos de Seguridad de la Información propuesta?			
7	¿El Marco de Referencia permite una adecuada identificación, evaluación, tratamiento y seguimiento de los riesgos mediante la Metodología de Riesgos de Seguridad propuesta?			
Bloque V	**V. Procedimientos para cumplir con la Ley de Protección de Datos Personales**			
Preguntas	**Descripción**			
8	¿El Marco de Referencia propone un acuerdo de privacidad, considera que cumple con lo estipulado por la Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad?			
9	¿El Marco de Referencia propone un procedimiento para el ejercicio de derechos ARCO, considera que cumple con lo estipulado por la Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad?			

Se implementó una encuesta web anónima, haciendo uso del formato de encuesta acorde con el método Delphi definido y de la herramienta google forms, la cual forma parte del **Anexo G** de la presente investigación. Finalmente para la interpretación de resultados se propuso, una valoración cualitativa, basada en una escala de Likert de cinco (5) niveles la cual a continuación se detalla:

Tabla N° 45: Valoración de Escala Likert

Denominación	Nivel de Aceptación
Totalmente en desacuerdo	Muy Bajo
En desacuerdo	Bajo
Ni de acuerdo ni en desacuerdo	Medio
De acuerdo	Alto
Totalmente de acuerdo	Muy Alto

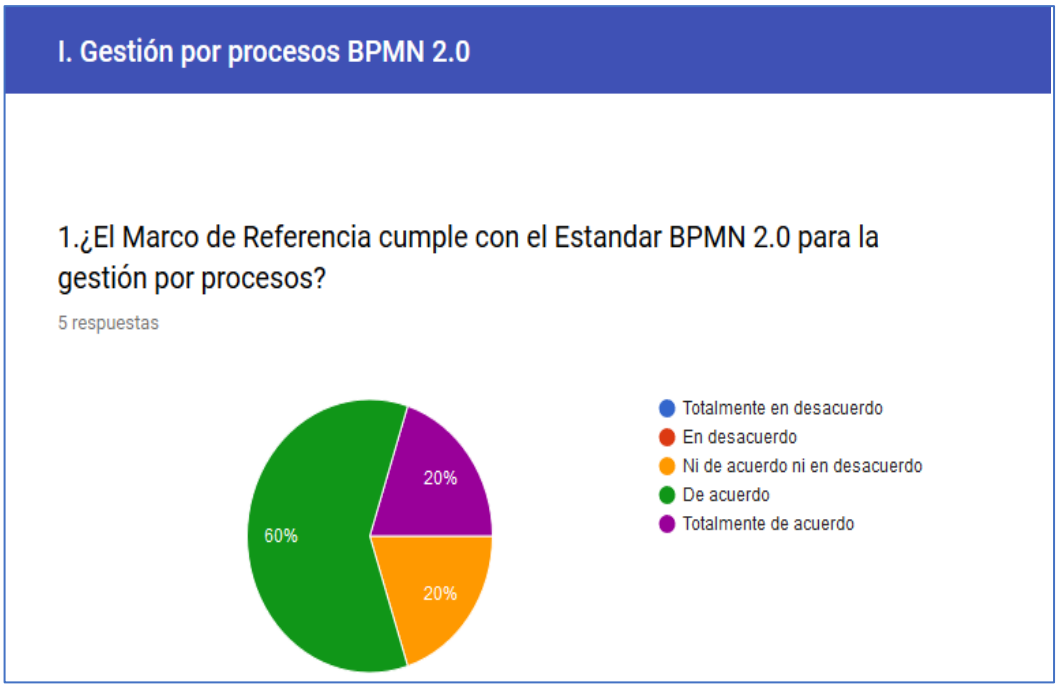
La valoración por pregunta a tomar como válida corresponderá **al resultado superior al 50%.**

6.2.2. Resultados del Método Delphi

A continuación se muestra los resultados obtenidos por la aplicación de encuestas ***anónimas*** desarrollada con google forms.

A. Bloque I.

Figura N° 139: Bloque I-Pregunta N°1

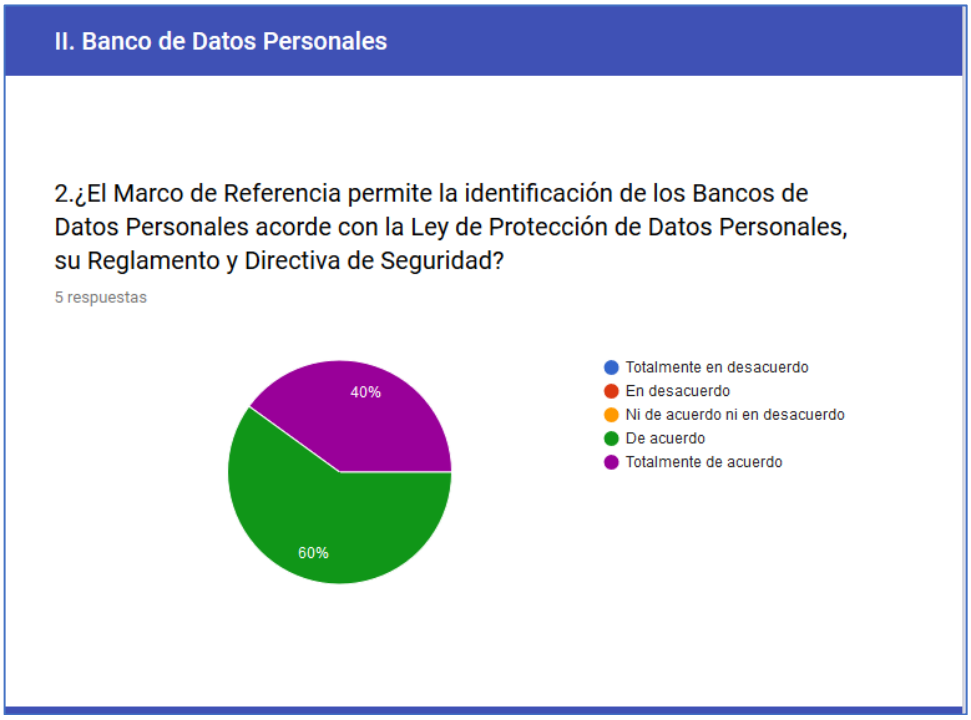


Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°1 se obtiene un 60 % con respuesta "De acuerdo", por tanto de nivel de aceptación es "Alto".

B. Bloque II

Figura N° 140: Bloque II-Pregunta N°2

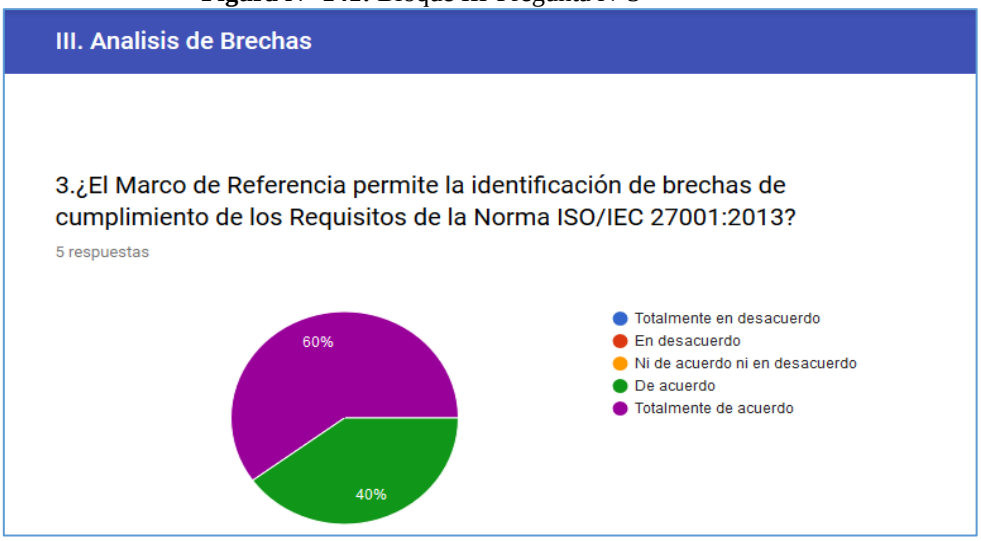


Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°2 se obtiene un 60 % con respuesta "De acuerdo", por tanto de nivel de aceptación es "Alto".

C. Bloque III

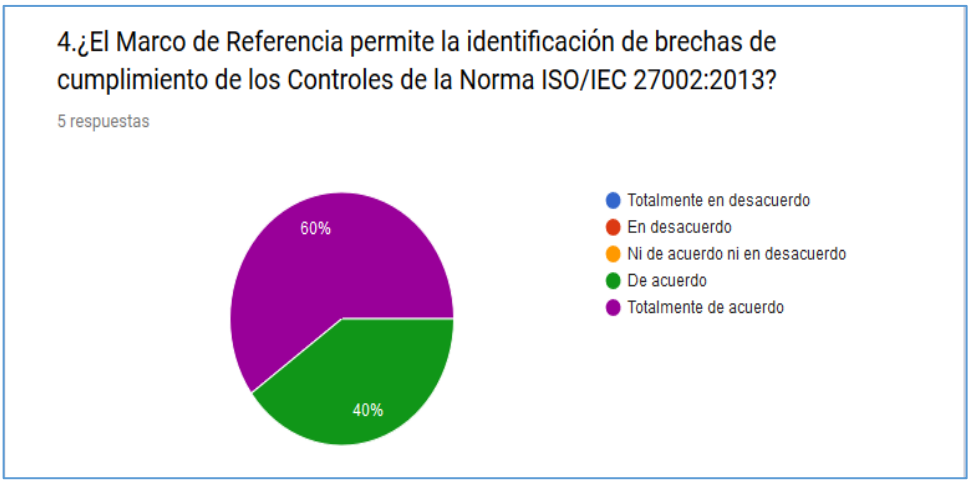
Figura N° 141: Bloque III-Pregunta N°3



Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°3 se obtiene un 60 % con respuesta "Totalmente de acuerdo", por tanto de nivel de aceptación es "Muy Alto".

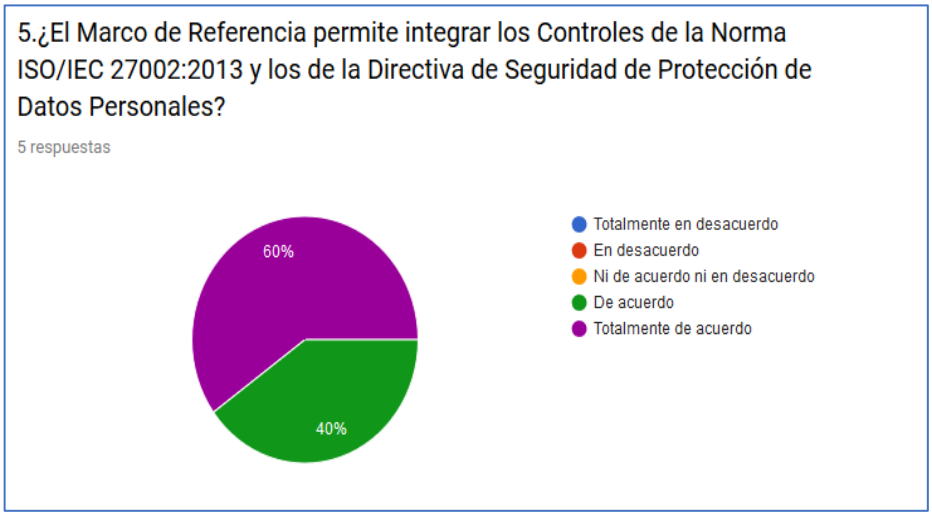
Figura N° 142: Bloque III-Pregunta N°4



Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°4 se obtiene un 60 % con respuesta "Totalmente de acuerdo", por tanto de nivel de aceptación es "Muy Alto".

Figura N° 143: Bloque III-Pregunta N°5

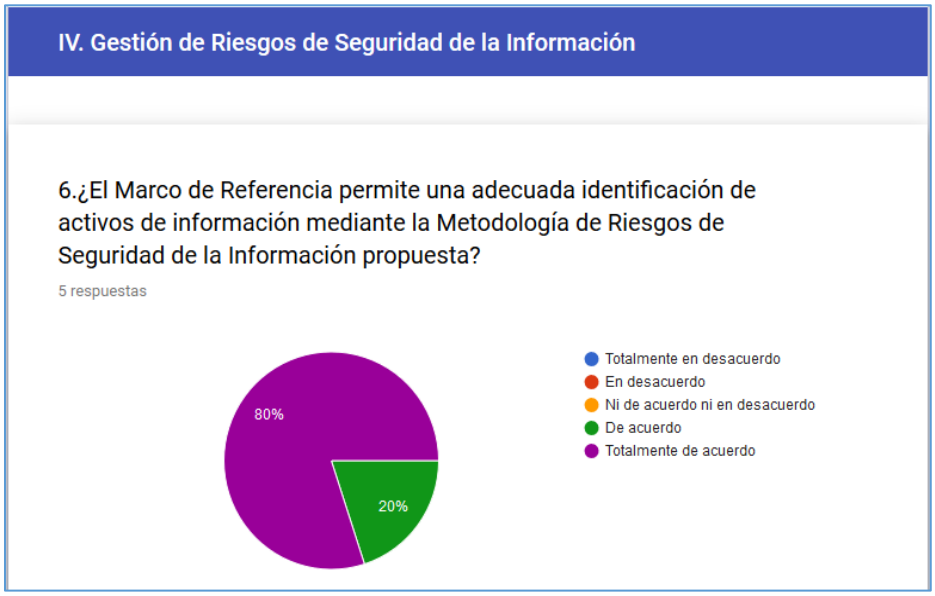


Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°5 se obtiene un 60 % con respuesta "Totalmente de acuerdo", por tanto de nivel de aceptación es "Muy Alto".

D. Bloque IV

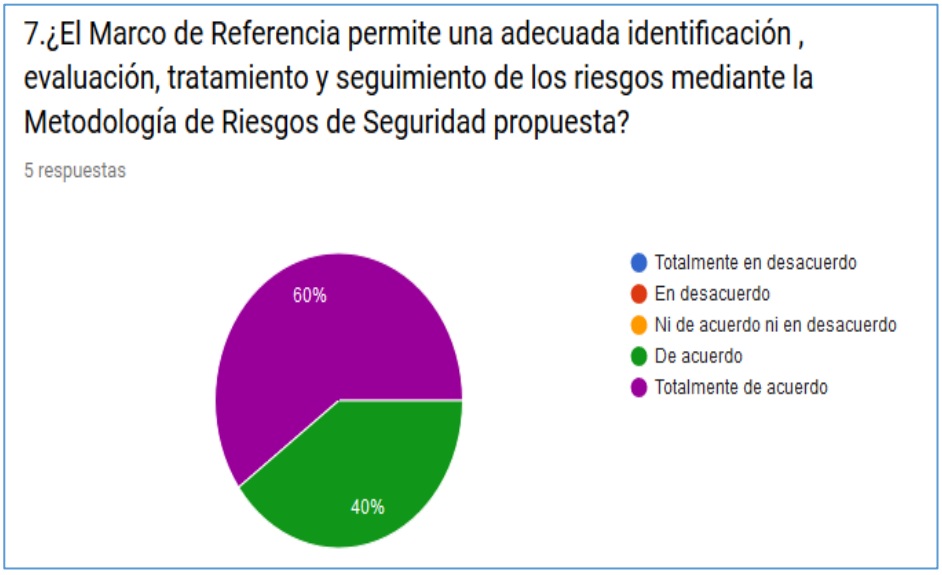
Figura N° 144: Bloque IV-Pregunta N°6



Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°6 se obtiene un 80 % con respuesta "Totalmente de acuerdo", por tanto de nivel de aceptación es "Muy Alto".

Figura N° 145: Bloque IV-Pregunta N°7



Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°7 se obtiene un 60 % con respuesta "Totalmente de acuerdo", por tanto de nivel de aceptación es "Muy Alto".

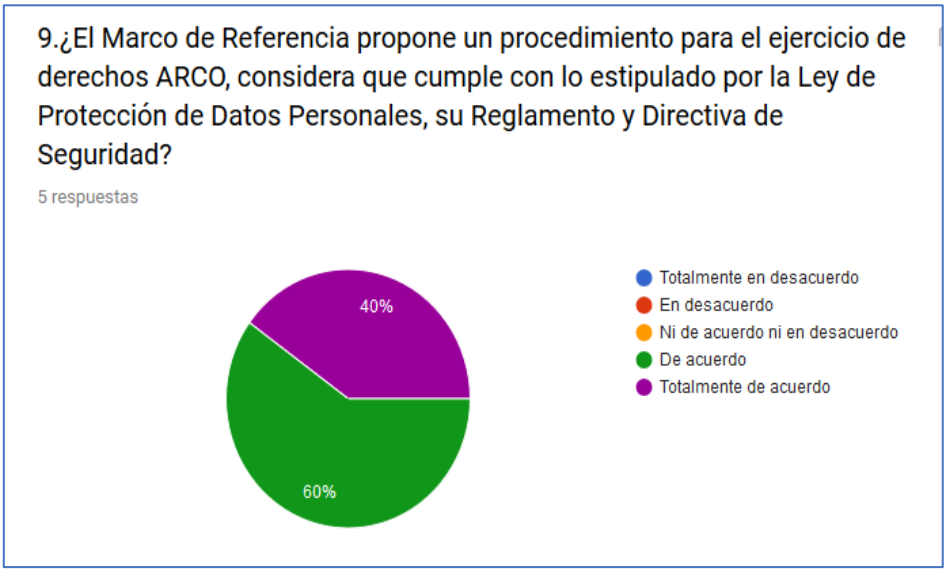
E. Bloque V

Figura N° 146: Bloque V-Pregunta N°8

Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°8 se obtiene un 60 % con respuesta "Totalmente de acuerdo", por tanto de nivel de aceptación es "Muy Alto".

Figura N° 147: Bloque V-Pregunta N°9



Fuente: Resultados de la Encuesta aplicada a los expertos en seguridad de la información, noviembre-diciembre del 2017.

Interpretación: Para la pregunta N°9 se obtiene un 60 % con respuesta "De acuerdo", por tanto de nivel de aceptación es "Alto".

6.2.3. Listado de Expertos

Tabla N° 46: Registro de Expertos

Apellidos y Nombres	Grado Académico	Certificaciones	Años de Experiencia en Seguridad de la Información	Cargo Actual	Correo Electrónico de Contacto
Yan Carranza, Freddy	Ingeniero Informático	ISO 27001 LI, 27001 LA, ISO-LCSM 27032	8 años	Oficial de Seguridad de la Información, Ministerio de Defensa del Perú	freddyyancarranza@gmail.com
Alvarado Lachira, Arnaldo Martín	Ingeniero de Sistemas	ISO 27001 LI, ISO-LCSM 27032	8 años	Analista de Seguridad y Continuidad de Caja Municipal de Ahorro y Crédito de Piura	alvaradoarnaldo13@gmail.com
Quesada Ramos, Rómulo	Ingeniero de Sistemas	COBIT5,ITIL	6 años	Auditor Supervisor TI en la Caja Metropolitana de Lima	rquesadaramos@gmail.com
Núñez Cueva, Luis Carlos	Ingeniero Informático	ISO 27001 LI,ISO 27002 F, ITIL	2 años	Oficial de Seguridad de la Información, Gobierno Regional de Lambayeque	luisncueva@gmail.com
Rigante, Franco	Magister en Dirección Estratégica y Tecnológica (Argentina)	CISA,CRISC,PMP,MBCI, ISO-LRM ISO 31000, ISO-LCSM 27032	20 años	Consultor de IT - GRC Especialista, Docente de ISACA, Instructor aprobado por el BCI	franco.rigante@gmail.com

CONCLUSIONES

- Se implementó y válido el Proceso de Admisión de Pregrado utilizando el estándar BPMN 2.0 en la Dirección de Admisión de la Universidad Nacional del Santa, obteniéndose un Inventario de Procesos con un total de: **Un (1) Macro Proceso, Dos (2) Procesos, Seis (6) Subprocesos y Veinte y tres (23) procedimientos**, lo que permitió a esta Dirección gestionar de forma oportuna sus funciones, recursos y servicios.

- Se implementó el procedimiento para la clasificación de Bancos de Datos Personales, basado en esté, sé determino y registro el Banco de Datos de Postulantes a los Programas de Pregrado y Posgrado de la Universidad Nacional del Santa, el cual fue evaluado con la matriz de apoyo elaborada en base a la directiva de seguridad de la Ley de Protección de Datos Personales, obteniéndose **un nivel crítico de clasificación para la privacidad de la información**, por tanto en cumplimiento por lo estipulado por esta directiva se requiere que **la Universidad de forma obligatoria realice la implementación de un SGSI basado en la Norma ISO/IEC 27001:2013**.

- Se realizó el análisis de brechas para evaluar el nivel de cumplimiento de las Normas: Para la ISO/IEC 27001:2013 se obtuvo que el **85% de los requisitos** requeridos están en un nivel de madurez **inexistente**; asimismo la ISO/IEC 27002:2013 y los controles de la Directiva de Seguridad los cuales fueron integrados de la cual de un total de Ciento Catorce (114) Controles se obtuvo un nivel de madurez de un **45% inexistente,** un **28 % limitados** y un **21 % iniciados.** De estos resultados se determina que con respecto a la seguridad de la información la Universidad debe realizar un trabajo arduo para la implementación de un SGSI.

- Se elaboró una metodología para el análisis, evaluación y tratamiento de los Riesgos de Seguridad de la Información basado en las Normas ISO/IEC 31000:2009 y la Norma ISO/IEC 27005:2011, la cual **permitirá de forma adecuada y práctica realizar la gestión de riesgos de seguridad** en la Universidad se debe precisar que esta metodología comprende: **Dos (2) Procedimientos Documentados y Cinco (5) formatos de registro**.

- Se elaboró procedimientos documentados para el ejercicio de los Derechos ARCO acorde con la Ley de Protección de Datos Personales. Asimismo se elaboró un modelo de Aviso de Privacidad para el Banco de Datos de Postulantes a Programas de Pregrado y Posgrado. Estos documentos son un total de**: Dos (2) procedimientos y Una (1) política, los cuales permitirán de forma adecuada implementar la Ley de Protección de Datos Personales**.

RECOMENDACIONES

- Implementar la Gestión por Procesos en la Universidad basándose en la Norma ISO 9001:2015 y el Estándar BPMN 2.0.

- Determinar y clasificar los Bancos de Datos Personales de la Universidad Nacional de la Santa, **faltantes**. Así mismo se debe registrar dichos Bancos de Datos en el Ministerio de Justica a fin de ***evitar multas*.**

- Designar y definir responsabilidades para el Comité de Seguridad de la Información y las del Oficial de Seguridad de la Información en cumplimiento a *la* ***Resolución Ministerial Nº 004-2016-PCM***, que aprueba el **uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información y su modificatoria la *Resolución Ministerial Nº 166-2017-PCM*** la cual modifica el artículo 5 de la anterior resolución referente al Comité de Gestión de Seguridad de la Información.

- Definir **cronograma, asignar recursos y determinar plazos para la Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)** basado en la **Norma ISO/IEC 27001:2013** (equivalente en el Perú la NTP ISO/IEC 27001:2014).

REFERENCIAS BIBLIOGRÁFICAS

A. P. (Noviembre de 2013). *Ministerio de Justicia.* Recuperado el 19 de Julio de 2017, de Ministerio de Justicia: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

Alcántara Flores, J. (2015). *Guía de Implementación de la Seguridad basado en la Norma ISO/IEC 27001 , para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del norte P.N.P en la ciudad de Chiclayo.* Chiclayo: Universidad Católica Santo Toribio de Mogrovejo. Recuperado el 2017 de Junio de 20, de http://tesis.usat.edu.pe/handle/usat/539

Amendola, L. (18 de Abril de 2017). Recuperado el 20 de Noviembre de 2017, de https://es.linkedin.com/pulse/propuesta-de-un-modelo-madurez-para-las-espa%C3%B1olas-amendola

Ávila Baray, H. (2006). *Introduccion a La Metodologia de La Investigacion.* Chihuahua, Chihuahua, Mexico. Recuperado el 25 de Mayo de 2017, de http://biblioteca.udgvirtual.udg.mx/eureka/pudgvirtual/introduccion%20a%20la%20metodologia%20de%20la%20investigacion.pdf

Bernal, C. (s.f.). Metodologia de la Investigacion cientifica. En C. A. Bernal, *Metodologia de la Investigacion cientifica* (pág. 124). Colombia: Pearson Colombia LTD. Recuperado el 15 de Mayo de 2017

Congreso de la República. (19 de Julio de 2017). *Ministerio de Justicia.* Recuperado el 19 de Julio de 2017, de Ministerio de Justicia: https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

Contreras Esguerra, L. (2017). *Diseño de un Sistema de Gestión de Seguridad de la Informacion basado en la norma ISO/IEC 27001 para la Dirección de Sistemas de la Gobernación de Boyacá.* Bogotá, Colombia: Universidad Nacional Abierta y a Distancia. Recuperado el 19 de Julio de 2017, de http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11895/1/33367604.pdf

Google. (17 de Julio de 2017). *Crea formularios atractivos*. Recuperado el 21 de Mayo de 2017, de https://www.google.com/intl/es/forms/about/

Hernández Sampieri, R., Baptista Lucio, P., & Fernández Collado, C. (2014). Metodología de la Investigación Científica. En R. Hernández Sampieri, P. Baptista Lucio, & C. Fernández Collado, *Metodología de la Investigación Científica* (pág. 155). Santa Fe, Colombia: Mc Graw Hill. Recuperado el 20 de Mayo de 2017

HITPASS, B. (2007). *BPM: Business Process Management Fundamentos y Conceptos de Implementación.* Chile: BHH Ltda.

INDECOPI. (2014). *NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos.* Lima: INDECOPI.

Justicia, M. d. (s.f.). Recuperado el 26 de Noviembre de 2017, de https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf.

Justicia, M. d. (s.f.). *Ministerio de Justicia.* Recuperado el 26 de Noviembre de 2017, de https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf

Network Security Advisors. (s.f.). Recuperado el 30 de Noviembre de 2017, de http://www.network-sec.com/gobierno-TI/auditoria-CMM

ONGEI. (08 de Enero de 2016). *El Peruano.* Recuperado el 19 de 07 de 2017, de El Peruano: http://busquedas.elperuano.com.pe/download/url/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1

ONGEI. (20 de Junio de 2017). *El Peruano.* Recuperado el 19 de Julio de 2017, de El Peruano: http://busquedas.elperuano.com.pe/download/url/modifican-el-articulo-5-de-la-rm-n-004-2016-pcm-referente-resolucion-ministerial-no-166-2017-pcm-1535494-2

PCM, S. G. (9 de Enero de 2013). *Secretaría Gestión Publica.* Obtenido de http://sgp.pcm.gob.pe/gestion-por-procesos/

Personales, A. N. (22 de Marzo de 2013). *Ministerio de Justicia.* Recuperado el 19 de Julio de 2017, de Ministerio de Justicia: https://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf

PÚBLICAS, M. D. (2012). *MAGERIT - versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información.* Madrid: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS.

Ramos, J. M. (2014). *Sistema de Gestión para mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina.* Nuevo Chimbote: Universidad Nacional del Santa. Recuperado el 19 de Julio de 2017

Reguant Álvarez, M., & Torrado Fonseca , M. (7 de Enero de 2016). El método Delphi. *REIRE, Revista d'Innovació i Recerca en Educación*, 87-102. doi:10.1344/reire2016.9.1916

República, C. d. (19 de Julio de 2017). *SUNEDU.* Obtenido de SUNEDU: https://www.sunedu.gob.pe/wp-content/uploads/2017/04/Ley-universitaria-30220.pdf

STANDARDIZATION, I. O. (2009). *IEC 31010:2009 Gestión de Riesgo. Técnicas de Apreciación del Riesgo.* Suiza: ISO.

STANDARDIZATION, I. O. (2009). *ISO 31000:2009 Gestión del Riesgo. Principios y Directrices.* Suiza: ISO.

STANDARDIZATION, I. O. (2010). *ISO/IEC 27003:2010 Tecnología de Información. Técnicas de Seguridad.Directrices para la implementación de un sistema de gestión de seguridad de información.* Suiza: ISO.

STANDARDIZATION, I. O. (2011). *ISO/IEC 27005:2011 Tecnología de Información. Técnicas de Seguridad.Gestión del Riesgo en Seguridad de Información.* Suiza: ISO.

STANDARDIZATION, I. O. (2013). *SO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad.* Suiza: ISO.

STANDARDIZATION, I. O. (2014). *ISO/IEC 27000:2014 Tecnología de Información - Técnicas de Seguridad -Sistemas de Gestión de Seguridad de Información - Descripción y vocabulario.* Suiza: ISO.

Transitoria, A. U. (19 de Julio de 2017). *Transparencia de la Universidad Nacional del Santa.* Obtenido de Transparencia de la Universidad Nacional del Santa: https://www.uns.edu.pe/archivos/estatuto_uns_vigente_para_web.pdf

Universitario, C. (19 de Julio de 2017). *Transparencia de la Universidad Nacional del Santa.* Obtenido de Transparencia de la Universidad Nacional del Santa: https://uns.edu.pe/#/transparencia/13d/reglamentos

Varela Ruiz, M., Díaz Bravo, L., & García Durán, R. (12 de Enero de 2012). Descripción y usos del método Delphi en investigaciones del área de la salud. *Investigación en Educación Médica,UNAM*, 90-95. Recuperado el 20 de Mayo de 2017, de http://riem.facmed.unam.mx/sites/all/archivos/V1Num02/07_MI_DESCRIPCION_Y_USOS.PDF

ANEXOS

Anexo A

Matriz de Análisis Brechas ISO/IEC 2700:2013

Sección	Requisitos ISO/IEC 27001:2013	Brecha	Nivel de Madurez Actual
4	Contexto de la organización		
4.1	Contexto Organizacional		
4.1	Determinar los objetivos organizacionales del SGSI y cuestiones que podrían afectar su efectividad	La UNS no cuenta con objetivos en su PEI 2017-2019, respecto a la implementación del SGSI.	Inexistente
4.2	Partes Interesadas		
4.2.a	Identificar partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	La UNS no ha determinado sus partes interesadas, esta en proceso la implementación en su SGC.	Inexistente
4.2.b	Determinar sus requerimientos relevantes de seguridad de la información y obligaciones		Inexistente
4.3	Alcance del SGSI		
4.3	Determinar y documentar el alcance del SGSI	La UNS no ha determinado el alcance de su SGSI.	Inexistente
4.4	SGSI		
4.4	Establecer, implementar, mantener y mejorar continuamente un SGSI acorde al estándar	La UNS no ha determinado las actividades para implementar su SGSI.	Inexistente
5	Liderazgo		
5.1	Liderazgo y compromiso		
5.1	Alta dirección debe demostrar liderazgo y compromiso con el SGSI	La Alta Dirección no ha conformado una Comisión Especial para el SGSI	Inexistente
5.2	Política		
5.2	Documentar la política de seguridad de la información	La UNS , no cuenta con una política de Seguridad de la Información.	Inexistente
5.3	Roles organizacionales, responsabilidades y autoridades		
5.3	Asignar y comunicar roles y responsabilidades de la seguridad de la información	La Alta Dirección no ha asignado un responsable de seguridad de la Información, se cuenta con iniciativas en la Oficina de Tecnología pero estas no han sido formalizadas.	Inexistente
6	Planificación		
6.1	Acciones para dirigir riesgos y oportunidades		
6.1.1	Diseñar/planificar el SGSI para satisfacer los requerimientos, direccionar riesgo y oportunidades	No se ha planificado el SGSI de la UNS,por tanto no se ha llevado a cabo una evaluación, ni el tratamiento de los riesgos de seguridad de la información	Inexistente
6.1.2	Definir y aplicar un proceso de evaluación del riesgo de seguridad de la información		Inexistente
6.1.3	Documentar y aplicar un proceso de tratamiento del riesgo de la seguridad de la información		Inexistente
6.2	Objetivos de la seguridad de la información y planes		
6.2	Establecer y documentar los objetivos de seguridad de la información y planes	No se han definido objetivos de seguridad de la información.	Inexistente
7	Soporte		
7.1	Recursos		
7.1	Determinar y establecer recursos para el SGSI	La UNS ha adquirido equipos para mejorar la seguridad la información el cuál es administrado por la Oficina de Tecnología de Información y Comunicaciones, pero no ha asignado recursos para la implementación del SGSI.	Inicial
7.2	Competencia		

7.2	Determinar, documentar y hacer disponibles las competencias necesarias	La UNS no ha evaluado las competencias de su personal respecto a la seguridad de la información asimismo se ha realizado una capacitación el año 2016 al respecto al personal de la Oficina de Tecnología de Información y Comunicaciones.	Inicial
7.3	Concientización		
7.3	Establecer un programa de concienciación de la seguridad	No se cuenta con un SGSI, por tanto no se realizado campañas de conciencia al respecto al personal de la Oficina de Tecnología de Información y Comunicaciones ha establecido una cultura de conciencia de seguridad de la información	Inicial
7.4	Comunicación		
7.4	Determinar las necesidades para comunicación interna y externa relevante a el SGSI	No se cuenta con un SGSI, por tanto no se determinado los medios de comunicación, la OTIC cuenta con políticas de uso y de seguridad sus Servicios pero están desactualizadas.	Inicial
7.5	Información Documentada		
7.5.1	Proveer documentación requerida por el estándar más lo que requiere la organización	No se cuenta con un SGSI, por tanto no hay información documentada al respecto.	Inexistente
7.5.2	Proveer títulos de documentos, autor, etc formato consistente y revisarlos y aprobarlos		Inexistente
7.5.3	Controlar apropiadamente la documentación		Inexistente
8	**Operación**		
8.1	Plan operacional y control		
8.1	Planear, implementar, controlar y documentar el proceso del SGSI para gestión de riesgos	No se han definido operaciones para el proceso del SGSI.	Inexistente
8.2	Evaluar el riesgo de la seguridad de la información		
8.2	Documentar regularmente los activos y los riesgos de seguridad de la información y sus cambios	No se han realizado evaluaciones de riesgos para el SGSI.	Inexistente
8.3	Tratamiento del riesgo de la seguridad de la información		
8.3	Implementar un plan de tratamiento del riesgo y documentar los resultados	No se han realizado un plan de tratamiento de riesgos para el SGSI.	Inexistente
9	**Evaluación del desempeño**		
9.1	Monitorear, medir, analizar y evaluar		
9.1	Monitorear, medir, analizar y evaluar el SGSI y los controles	No se cuenta con un SGSI, por tanto no hay evaluación del desempeño.	Inexistente
9.2	Auditoría Interna		
9.2	Planear y conducir auditorías internas del SGSI	No se cuenta con un SGSI, por tanto no se han realizado auditorías internas.	Inexistente
9.3	Revisión de la Dirección		
9.3	Emprender revisiones de la dirección regulares del SGSI	No se cuenta con un SGSI, por tanto no se cuenta con revisiones por la alta dirección.	Inexistente
10	**Mejora**		Inexistente
10.1	No conformidades y acciones correctivas		
10.1	Identificar, reparar y tomar acciones para prevenir recurrencia de no conformidades, documentando las acciones	No se cuenta con un SGSI, por tanto no se cuenta con revisiones por la alta dirección.	Inexistente
10.2	Mejora continua		
10.2	Mejorar continuamente el SGSI	No se cuenta con un SGSI, por tanto no se cuenta con un proceso de mejora continua.	Inexistente

Anexo B

Matriz de Brechas ISO/IEC 27002 y de la Directiva de Seguridad de LPDP

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA										
Tipo	**Código**	**Dominio / Objetivo / Control ISO/IEC 27002:2013**	**Directiva de Seguridad de la Ley de Protección de Datos Personales Ley N°29733**						**Brecha**	**Nivel de Madurez Actual**
DOMINIO	**A.5**	**Políticas de seguridad de la información**	**#Directiva Organizativa**	**Detalle Directiva Organizativa**	**#Directiva Técnicas**	**Detalle Directiva Técnicas**	**#Directiva Legales**	**Detalle Directiva Legales**		
OBJETIVO	A.5.1	Dirección de la gerencia para la seguridad de la información								
CONTROL	A.5.1.1	Políticas para la seguridad de la información	1.3.1.1 1.4.1 1.3.1.7 2.1.2	1.3.1.1 Determinar y dar a conocer una política de protección de datos personales: Una declaración breve y directa que demuestre el compromiso institucional y el involucramiento de sus autoridades con la protección de los datos personales en el tratamiento que se de a los datos personales contenidos en el banco de datos personales bajo su titularidad. 1.4.1 a) Ser clara y comprensible, tanto para el personal involucrado en el tratamiento como para los titulares de datos personales que hayan consentido el tratamiento. b) Ser apropiada para los objetivos de la organización. c) Proporciona un lineamiento de alto nivel organizacional y objetivos claros que sirven de dirección para la					No existe documento de Políticas para la seguridad de la información.	**Inexistente**
CONTROL	A.5.1.2	Revisión de las políticas para la seguridad de la información								**Inexistente**
DOMINIO	**A.6**	**Organización de la seguridad de la**								
OBJETIVO	A.6.1	Organización interna								
CONTROL	A.6.1.1	Roles y responsabilidades para la seguridad de la información	2.b 2.1.1	2. b) El titular del banco de datos personales debe designar un responsable de seguridad del banco de datos personales, quien coordinará en la institución la aplicación de la presente directiva. El rol de responsable de seguridad del banco de datos personales debe asignarse a una persona que tenga las capacidades y autoridad					No existe en los MOF, responsabilidades inherentes a la seguridad de la información.	**Inexistente**
CONTROL	A.6.1.2	Segregación de funciones							No existe segregación de tareas de seguridad de la información debidamente formalizadas, se debe precisar que la OTIC cuenta con buenas prácticas al respecto pero no están aprobadas.	**Limitado**

CONTROL	A.6.1.3	Contacto con autoridades							No se cuenta con un procedimiento documentado de comunicación con la alta dirección en caso de incidentes de seguridad.	**Inicial**
CONTROL	A.6.1.4	Contacto con grupos especiales de interés							No se cuenta con un listado de especialistas o entidades apropiadas que permita absolver cualquier duda de seguridad o que informe a la Universidad sobre eventos de seguridad oportunamente	**Inexistente**
CONTROL	A.6.1.5	Seguridad de la información en la gestión de proyectos.							No se integra la Seguridad de la información en la Gestión de proyectos.	**Inexistente**
OBJETIVO	A.6.2	Dispositivos móviles y teletrabajo								
CONTROL	A.6.2.1	Política de dispositivos móviles							No hay establecida una política, ni medidas de seguridad adecuadas para la protección contra riesgos asociados al uso de recursos almacenados en dispositivos móviles.	**Inexistente**
CONTROL	A.6.2.2	Teletrabajo							No hay establecida una política, ni medidas de seguridad adecuadas para la protección contra riesgos asociados al teletrabajo.	**Inexistente**
DOMINIO	**A.7**	**Seguridad de los recursos humanos**								
OBJETIVO	A.7.1	Antes del empleo								
CONTROL	A.7.1.1	Selección							En los procesos de contratación, no se realizan revisiones de verificación de los antecedentes penales a los candidatos a postulaciones administrativos y docentes, ni de contratistas respecto a la clasificación de la información a la cual va a tener acceso y riesgos percibidos.	**Inexistente**
CONTROL	A.7.1.2	Términos y condiciones del empleo					2.2.2	2.2.2 Adecuación de los contratos del personal relacionado con el tratamiento de datos personales, incluyendo la coherencia con el requisito 1.3.1.8.	No se tienen implementados acuerdos de confidencialidad en los contratos laborales y/o con terceros.	**Inexistente**
OBJETIVO	A.7.2	Durante el empleo								
CONTROL	A.7.2.1	Responsabilidades de la gerencia							No existen responsabilidades de gestión de la seguridad de la información, asociadas a los MOF,ROF de la Universidad.	**Inexistente**

CONTROL	A.7.2.2	Conciencia, educación y capacitación, sobre la seguridad de la información.	2.1.8	2.1.8 Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.					Se cuenta con una capacitación en SI en la OTIC, pero no se han realizado campañas de concienciación sobre seguridad de la información en ningún nivel de la Universidad.	**Limitado**
CONTROL	A.7.2.3	Proceso disciplinario							No existe la figura de proceso disciplinario respecto a seguridad de la información.	**Inexistente**
OBJETIVO	A.7.3	Terminación y cambio de empleo								
CONTROL	A.7.3.1	Terminación o cambio de responsabilidades del empleo.					2.2.2	2.2.2 Adecuación de los contratos del personal relacionado con el tratamiento de datos personales, incluyendo la coherencia con el requisito 1.3.1.8.	Solo existen mecanismos de seguridad asociados al cese de cuenta en el caso de cambio de puestos de trabajo a los sistemas de información por parte de la OTIC, pero no ha sido documentado ni formalizado.	**Definido**
DOMINIO	**A.8**	**Gestión de activos**								
OBJETIVO	A.8.1	Responsabilidad por los activos								
CONTROL	A.8.1.1	Inventario de activos							La Universidad no cuenta con un listado global de activos de información, se debe mencionar que la OTIC cuenta con un inventario de activos de información pero no ha sido revisado y formalizado.	**Limitado**
CONTROL	A.8.1.2	Propiedad de los activos			2.3.4.1	2.3.4.1 El banco de datos personales no automatizado debe mantener los datos personales independizados de forma individual, de modo que pueda referirse unívocamente a un titular de datos personales sin exponer información de otro			Aunque lo dueños de cada activo de información son conocidos y/o deducibles, no se han identificado formalmente.	**Limitado**
CONTROL	A.8.1.3	Uso aceptable de los activos	1.3.1.8	1.3.1.8 Desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales (artículo 17 de la Ley N° 29733), aplicable al personal relacionado con el tratamiento de datos personales.					Debido a que no se han definido formalmente a los dueños de los activos de información y no se cuenta con política de gestión de estos, las responsabilidades del personal sobre dichos activos de información no se encuentran formalmente establecidas, lo cual no permite un adecuado seguimiento o atención en caso de algún incidente de SI.	**Limitado**

CONTROL	A.8.1.4	Retorno de activos							Actualmente, no se ha establecido un procedimiento formal de monitoreo para la gestión de devolución de activos en casos de cese o cambios de personal (docente y administrativo), por lo cual no se puede asegurar que todos los activos actualmente hayan sido debidamente devueltos, se debe precisar que la Oficina de Control Patrimonial cuenta con formatos de bienes asimismo la Oficina de Tecnología cuenta con formatos para entrega de equipos.	**Definido**
OBJETIVO	A.8.2	Clasificación de la información								
CONTROL	A.8.2.1	Clasificación de la información							Aunque se cuenta con una clasificación de activos formalmente establecida por parte de la Oficina de Control Patrimonial, no se puede asegurar que esta se encuentre debidamente implementada ya que no se cuenta con algún inventario que permita conocer dichas clasificaciones para cada activo de información de la Universidad.	**Limitado**
CONTROL	A.8.2.2	Etiquetado de la información			2.3.2.4	2.3.2.4. Las copias o reproducciones de los documentos deben tener una marca que identifique el periodo de validez de las mismas.			No existen procedimientos de etiquetado y manipulación de la información, pero se cuenta con buenas prácticas de gestión de SI en la Oficina de Tecnología.	**Inicial**
CONTROL	A.8.2.3	Manejo de activos	2.d 2.e 2.1.7	2. d) Limitar los bancos de datos personales a los datos estrictamente necesarios para cumplir la finalidad para la cual fueron acopiados. 2. e) Evaluar la posibilidad de implementar mecanismos de	2.3.4.1	2.3.4.1 El banco de datos personales no automatizado debe mantener los datos personales independizados de forma individual, de modo que pueda referirse unívocamente a un titular de datos personales sin exponer información de otro			No existen políticas asociadas a la manipulación de activos de la información, pero se cuenta con buenas prácticas de gestión de SI en la Oficina de Tecnología.	**Inicial**
OBJETIVO	A.8.3	Manejo de los medios								
CONTROL	A.8.3.1	Gestión de medios removibles			2.3.2.2, 2.3.4.5,	2.3.2.2. b) Los datos contenidos en soporte informático deben transportarse previa encriptación y un mecanismo de verificación de la integridad (checksum MD5, firma digital o similar). 2.3.4.5. Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando			No existen políticas para la gestión de soportes extraíbles.	**Inexistente**
CONTROL	A.8.3.2	Disposición de medios							No se cuenta con procedimientos de eliminación de soportes de almacenamiento.	**Inexistente**

CONTROL	A.8.3.3	Transferencia de medios físicos			2.3.2.1, 2.3.2.2	2.3.2.1. Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del titular del banco de datos personales o quien éste designe para ello. 2.3.2.2. a) Los datos en soporte físico deben estar contenidos en un contenedor que evite su			No se cuenta con procedimientos con políticas y lineamientos sobre la transferencia de información a través de medios físicos, actualmente no se puede asegurar un adecuado cumplimiento.	**Inexistente**
DOMINIO	**A.9**	**Control de acceso**								
OBJETIVO	A.9.1	Requisitos de la empresa para el control de acceso								
CONTROL	A.9.1.1	Política de control de acceso	2.1.11	2.1.11 Desarrollar un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso.					No se cuenta con una política de control de acceso, pero se cuenta con un reglamento del uso de servicios TI formulado por la OTIC aprobado pero esté esta desactualizado asimismo los Sistemas Informáticos cuenta con controles de derechos de acceso.	**Limitado**
CONTROL	A.9.1.2	Acceso a redes y servicios de red			2.3.4.5, 2.3.4.6	2.3.4.5. Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad. 2.3.4.6 La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad			Se encuentran implementados controles de acceso a las redes y servicios asociados, pero no se cuenta con políticas y procedimientos formales de encriptación, otorgamiento y retiro de acceso a carpetas compartidas.	**Definido**
OBJETIVO	A.9.2	Gestión de acceso a usuario								
CONTROL	A.9.2.1	Registro y baja de usuarios	2.1.11	2.1.11 Desarrollar un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso.	2.3.1.5	2.3.1.5. El titular del banco de datos personales, o quien este designe, debe autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse.			Se cuenta con una rutina en los sistemas de información de la OTIC para las altas/bajas en el registro/acceso de usuarios, pero no se cuenta con políticas y procedimientos formalizados al respecto.	**Limitado**

CONTROL	A.9.2.2	Aprovisionamiento de acceso a usuario	1.3.1.4 1.4.2 1.4.3 1.4.4 2.1.3 2.1.11	1.3.1.4 Implementar y mantener los siguientes procedimientos documentados. 1.4.2 b) Registros de personal con acceso autorizado. 1.4.3 b) Registros de acceso. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733. 2.1.3 Llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento (Trazabilidad).	2.3.1.4, 2.3.1.5	2.3.1.4. Cuando se utilicen mecanismos informáticos para el tratamiento de datos personales se debe proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados. 2.3.1.5. El titular del banco de datos personales, o quien este designe, debe autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse.			Se gestionan los derechos de acceso a los usuarios de acuerdo a demanda pero no se cuenta con procedimientos y políticas documentadas, ni formalizadas.	**Limitado**
CONTROL	A.9.2.3	Gestión de derechos de acceso privilegiados			2.3.2.5	2.3.2.5. El titular, o quien éste designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: Usuario, privilegio asignado, Fecha y hora de asignación y/o			No se cuenta con procedimientos formales para la gestión de modificaciones de permisos de usuarios privilegiados en los Sistemas de Información.	**Limitado**
CONTROL	A.9.2.4	Gestión de información de autentificación secreta de usuarios			2.3.1.1	2.3.1.1 a) Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.			Se cuenta con registro de entrega de contraseñas, pero no están soportados en procedimientos para la gestión de la información confidencial de autenticación de usuarios.	**Limitado**
CONTROL	A.9.2.5	Revisión de derechos de acceso a usuarios			2.3.1.2	2.3.1.2. Se debe revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado. Esta revisión debe generar un registro de revisión que evidencie la realización de dicha			Existe control de autenticación a nivel de sistemas de información y perfiles de usuario, pero no se cuenta con procedimientos programados de revisión.	**Limitado**
CONTROL	A.9.2.6	Remoción o ajuste de derechos de acceso			2.3.1.5, 2.3.2.5	2.3.1.5. El titular del banco de datos personales, o quien este designe, debe autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse. 2.3.2.5. El titular, o quien éste designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: Usuario, privilegio asignado, Fecha y horade asignación y/o retiro de privilegios, usuario que realiza la asignación y/o retiro de privilegios			Se cuenta con actividades de cancelación y ajuste automatizado, pero no se cuenta con un documento que demuestre dichas actividades.	**Limitado**
OBJETIVO	A.9.3	Responsabilidades de los usuarios								

CONTROL	A.9.3.1	Uso de información de autentificación secreta			2.3.1.1	2.3.1.1. d) Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.			Los administradores de los sistemas crean contraseñas haciendo uso de buenas prácticas, pero que no hay un procedimiento y evidencias de socialización con los usuarios.	**Limitado**
OBJETIVO	A.9.4	Control de acceso a sistema y aplicación								
CONTROL	A.9.4.1	Restricción de acceso a la información			2.3.1.4	2.3.1.4. Cuando se utilicen mecanismos informáticos para el tratamiento de datos personales se debe proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.			No existe política de control de acceso definida, por lo que las restricciones de acceso que se aplican no se basan en la misma sino en las buenas prácticas realizadas por la Oficina de Tecnología.	**Limitado**
CONTROL	A.9.4.2	Procedimientos de ingreso seguro			2.3.1.1, 2.3.1.4	2.3.1.1. b) Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada. 2.3.1.4. Cuando se utilicen mecanismos informáticos para el tratamiento de datos personales se debe proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales			No existe política de control de acceso definida por tanto no se cuenta con un procedimiento de acceso seguro.	**Limitado**
CONTROL	A.9.4.3	Sistema de gestión de contraseñas			2.3.1.1	2.3.1.1. c) Permitir que el usuario cambie la contraseña asignada cuando lo considere necesario. 2.3.1.1. d) Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial. 2.3.1.1. e) Cuando el acceso al sistema esté expuesto en entornos públicos (intranet, internet o similares), se debe bloquear al usuario luego de cinco (05) intentos fallidos de			Las contraseñas para acceso a los sistemas de información de la universidad son gestionadas por la Oficina de Tecnología, pero no se cuenta con una herramienta que verifique la calidad de las contraseñas cambiadas por los usuarios, no se cuenta con una política y procedimiento de gestión de estas.	**Limitado**
CONTROL	A.9.4.4	Uso de programas utilitarios privilegiados							No se hace seguimiento de dichos programas, no se cuenta con una política y procedimiento de uso del software en la Universidad.	**Limitado**

CONTROL	A.9.4.5	Control de acceso al código fuente de los programas							El acceso es restringido pero no se existe un procedimiento de revisiones de los accesos a código fuente de los principales sistemas de información.	**Limitado**
DOMINIO	**A.10**	**Criptografía**								
OBJETIVO	A.10.1	Controles criptográficos								
CONTROL	A.10.1.1	Política sobre el uso de controles criptográficos			2.3.4.5	2.3.4.5. Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.			No existe política de uso de controles criptográficos. La Oficina de Tecnología usa cifrado de información de la Base de Datos, sin embargo deberán ser desplegados sobre los activos de información que requieran de dichos controles.	**Inicial**
CONTROL	A.10.1.2	Gestión de claves							Se realizan buenas prácticas de gestión de claves criptográficas en la Oficina de Tecnología, pero no se cuenta con políticas y procedimientos de gestión, asimismo no se evidencia que estén implementadas en los activos de información que requieran de dichos controles.	**Inicial**
DOMINIO	**A.11**	**Seguridad física y ambiental**								
OBJETIVO	A.11.1	Áreas seguras								
CONTROL	A.11.1.1	Perímetro de seguridad física			2.3.1.3	2.3.1.3. Proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.			No existe un procedimiento formal para la implementación y monitoreo de controles físicos y ambientales en el Data Center y/o instalaciones principales de procesamiento de información de la Universidad.	**Inicial**
CONTROL	A.11.1.2	Controles de ingreso físico			2.3.1.3	2.3.1.3. Proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.			Se cuenta con controles de entrada insuficientes para garantizar que solo el personal autorizado dispone de permiso de acceso puesto que se evidencia en la visita a los cuartos de comunicaciones principales de la Universidad para dar atención a alumnos, administrativos, docentes y terceros.	**Inicial**
CONTROL	A.11.1.3	Asegurar oficinas, áreas e instalaciones			2.3.1.3	2.3.1.3. Proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.			Se cuenta con un sistema de acceso al Data Center de la Universidad y de videocámaras, pero no se ha identificado ni implementado en otras oficinas, salas e instalaciones de la organización.	**Inicial**

CONTROL	A.11.1.4	Protección contra amenazas externas y ambientales			2.3.1.3	2.3.1.3. Proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.			El Data Center de la Universidad cuenta con controles ambientales tales como detectores de humo o sensores de humedad, pero se evidencia la presencia de material inflamable, como cajas de cartón, dentro de él asimismo no se cuenta con luces de emergencia finalmente no se ha identificado ni implementado en otras oficinas, salas e instalaciones de la organización.	**Inicial**
CONTROL	A.11.1.5	Trabajo en áreas seguras			2.3.4.10	2.3.4.10 Restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales salvo autorización del titular del			No existen procedimientos para el desarrollo de trabajos en áreas seguros, puesto que estas no han sido determinadas.	**Inicial**
CONTROL	A.11.1.6	Áreas de despacho y carga							Se cuenta con personal de vigilancia pero no se ha implementado un procedimiento de control identificando y clasificando los principales centros de procesamiento de la Universidad.	**Limitado**
OBJETIVO	A.11.2	Equipos								
CONTROL	A.11.2.1	Emplazamiento y protección de los equipos							Se cuentan con mecanismos de control de acceso al Data Center de la Universidad , pero no se ha determinado e implementado en las oficinas y laboratorios. Se cuenta con extintores antiincendios y los edificios construidos en los últimos años son antisismicos,pero no se cuenta con evidencias del estado de las instalaciones donde se realiza procesamiento de información.	**Limitado**

CONTROL	A.11.2.2	Servicios de suministro							No todos los equipos cuentan con reguladores de electricidad en las instalaciones de la Universidad, aunque sí los servidores y cuartos de comunicaciones. No existe un procedimiento de inspección del estado de estos servicios, no se cuenta con un luces de emergencia en los principales centros de procesamiento de la información.	**Limitado**
CONTROL	A.11.2.3	Seguridad del cableado							Se cuenta con zonas en la Universidad donde los cables de datos y/o de electricidad son accesibles a ataques a la disponibilidad.	**Inicial**
CONTROL	A.11.2.4	Mantenimiento de equipos			2.3.4.3	2.3.4.3. Los equipos deben recibir mantenimiento preventivo y correctivo de acuerdo a las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad. El mantenimiento de los equipos debe ser realizado por personal autorizado.			No existen procedimientos de mantenimiento preventivo y correctivo para los equipos que conforman la infraestructura informática de la Universidad. La Oficina de Tecnología realiza actividades de mantenimiento a demanda.	**Inicial**
CONTROL	A.11.2.5	Remoción de activos			2.3.2.1	2.3.2.1. Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del titular del banco de datos personales o quien éste designe para ello.			Se cuenta con registros para la salida de activos fuera de las dependencias, previa autorización por parte del responsable del activo y de la Oficina de Control Patrimonial.	**Gestionado**
CONTROL	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones			2.3.2.1	2.3.2.1. Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del titular del banco de datos personales o quien éste designe para ello.			Se cuenta con evidencias de autorización para la salida de equipos, pero no se ha identificado si se cuenta con seguros que cubran posibles robos y daños en los equipos y activos que se trasladan fuera de las instalaciones de la Universidad.	**Limitado**

CONTROL	A.11.2.7	Disposición o reutilización segura de equipos			2.3.2.3	2.3.2.3. Cuando se requiera eliminar la información contenida en un medio informático removible se deben utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio; de forma tal que, no permitan la recuperación de los datos. El titular del banco de datos personales debe designar a las personas autorizadas a eliminar la información de datos personales contenida en los medios informáticos removibles			No existe un procedimiento formal para la eliminación y re-uso de equipos (servidores, estaciones de trabajo).	**Inexistente**
CONTROL	A.11.2.8	Equipos de usuario desatendidos.							No se cuenta con los procedimientos que garanticen la protección adecuada en estos casos.	**Inexistente**
CONTROL	A.11.2.9	Política de escritorio limpio y pantalla limpia.			2.3.2.4	2.3.2.4. Seguridad en la copia o reproducción de documentos: Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales: a) Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados. b) Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.			No existe una política de escritorio y pantalla limpia, por tanto no se cuentan con revisiones de escritorio limpio.	**Inexistente**
DOMINIO	**A.12**	**Seguridad de las operaciones**								
OBJETIVO	A.12.1	Procedimientos y responsabilidades operativas.								
CONTROL	A.12.1.1	Procedimientos operativos documentados.							La documentación con la que se cuenta es insuficiente para algunos procedimientos de operación.	**Inicial**
CONTROL	A.12.1.2	Gestión de cambio							No se cuenta con procedimientos de gestión de cambios.	**Inexistente**
CONTROL	A.12.1.3	Gestión de la capacidad							No se evidencia un seguimiento al uso de los recursos y proyecciones de requisitos de capacidad en el futuro para servidores y equipos activos.	**Inexistente**
CONTROL	A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones							No se cuenta con una segregación de funciones entre los ambientes de desarrollo y producción debidamente documentada y formalizada.	**Limitado**
OBJETIVO	A.12.2	Protección contra código maliciosos								

CONTROL	A.12.2.1	Controles contra códigos maliciosos			2.3.4.4	2.3.4.4. Los equipos utilizados para el tratamiento de los datos personales deben contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los datos personales. El software de protección debe ser actualizado frecuentemente de acuerdo a las recomendaciones y especificaciones del proveedor.			Se cuenta con controles para la detección y prevención de malware, pero no para la recuperación en caso de daños asimismo no se cuenta con una política formal del uso de software no autorizado.	**Limitado**
OBJETIVO	A.12.3	Respaldo								
CONTROL	A.12.3.1	Respaldo de la información			2.3.3.1, 2.3.3.2, 2.3.3.3	2.3.3.1,. Se deben realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción. 2.3.3.2. Toda recuperación de datos personales, desde su copia de respaldo, debe contar con la autorización del encargado del banco de datos personales. 2.3.3.3. Se deben realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido.			Se cuenta con los procedimientos para copias de seguridad de respaldo de la Base de Datos del SIIGAA de la Oficina de Tecnología se evidencia respaldos realizados en unidad externa pero no se cuenta con registros de pruebas. Asimismo no se puede asegurar que se realiza un adecuado monitoreo sobre la ejecución exitosa de los respaldos de información actualmente configurados en los servidores asimismo no se evidencia que este implementado estrategias de respaldo y pruebas en otras dependencias de la Universidad.	**Limitado**
OBJETIVO	A.12.4	Registro y monitoreo								
CONTROL	A.12.4.1	Registro de eventos	1.3.1.4 1.4.3 1.4.4 2.1.3	1.3.1.4 Implementar y mantener los siguientes procedimientos documentados. 1.4.3 c) Registro de auditorías. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733. 2.1.3 Llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento (Trazabilidad).	2.3.1.6, 2.3.2.5	2.3.1.6. Implementar un registro de accesos el cual debe contener al menos los siguientes campos: Fecha y hora del acceso., persona que realiza el acceso., identificador del titular de los datos personales a tratar, motivo del acceso. 2.3.2.5. El titular, o quien éste designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: Usuario, privilegio asignado, Fecha y horade asignación y/o retiro de privilegios, usuario que realiza la asignación y/o retiro de privilegios.			Se realizan actividades de revisión a demanda de los registros de eventos de actividad del usuario, excepciones, fallas y de seguridad (pistas de auditoría), a nivel de sistemas de información y servidores como buena práctica en la Oficina de Tecnología pero no se lleva un registro de control de estos eventos ni se cuenta con un procedimiento formal, asimismo no se evidencia estas actividades a nivel de equipos de trabajo.	**Limitado**
CONTROL	A.12.4.2	Protección de información de registros							Se respalda información de los logs de la Base de Datos del SIIGAA de la Oficina de Tecnología, la cuál cuenta con buenas prácticas de protección, pero no se puede evidenciar a nivel de servidores y equipos.	**Limitado**

CONTROL	A.12.4.3	Registro del administrador y operador							No se han realizado revisiones de pistas de auditoría sobre los usuarios con altos privilegios en los principales sistemas de información.	**Inexistente**
CONTROL	A.12.4.4	Sincronización del reloj							La Oficina de Tecnología no cuenta con lineamientos documentados para la revisión sobre la sincronización de relojes de los sistemas de información, servidores con una fuente acordada y exacta de tiempo.	**Inexistente**
OBJETIVO	A.12.5	Control del software operacional								
CONTROL	A.12.5.1	Instalación de software en sistemas operacionales							No se cuenta con procedimientos de control de software en los sistemas en producción.	**Inexistente**
OBJETIVO	A.12.6	Gestión de vulnerabilidad técnica								
CONTROL	A.12.6.1	Gestión de vulnerabilidades técnicas							No se han ejecutado revisiones de vulnerabilidades de seguridad sobre la infraestructura de TI, no se pudo verificar que se realice una revisión sobre los sistemas de información de la Universidad.	**Inexistente**
CONTROL	A.12.6.2	Restricciones sobre la instalación de software							No se cuenta con una política de la instalación de software.	**Inexistente**
OBJETIVO	A.12.7	Consideraciones para la auditoría de los sistemas de información								
CONTROL	A.12.7.1	Controles de auditoría de sistemas de información			2.3.4.12, 2.3.4.11	2.3.4.12. Acciones correctivas y mejora continúa. 2.3.4.11. Se debe realizar una auditoría sobre el cumplimiento de la presente directiva, bajo responsabilidad del titular del banco de datos personales.			No se han planificado los requisitos y actividades de auditorías para la verificación de sistemas de información.	**Inexistente**
DOMINIO	**A.13**	**Seguridad de las comunicaciones**								
OBJETIVO	A.13.1	Gestión de seguridad de la red								

CONTROL	A.13.1.1	Controles de la red			2.3.4.5, 2.3.4.6	2.3.4.5. Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad. 2.3.4.6 La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad. Transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros).			Se realiza mediante el uso de un firewall que gestiona los accesos la red corporativa esta actividad se realiza a demanda, no se cuenta con un procedimiento formal.	**Inicial**
CONTROL	A.13.1.2	Seguridad de servicios de red			2.3.4.6	2.3.4.6 La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad.			Se tiene un firewall para la gestión de la seguridad perimetral de la red corporativa el cual cuenta con SLA vigente a la fecha 02/12/2017, pero no se cuenta con procedimientos documentados de administración. EL servicio de internet cuenta con SLA vigente a la fecha 02/12/2017.	**Definido**
CONTROL	A.13.1.3	Segregación en redes							Las redes se encuentran segmentadas según niveles de confianza establecidos por la Oficina de Tecnología, pero no se cuenta con lineamientos de segregación documentados.	**Limitado**
OBJETIVO	A.13.2	Transferencia de información								
CONTROL	A.13.2.1	Políticas y procesamientos de transferencia de la información			2.3.4.7, 2.3.4.6	2.3.4.7. El receptor o importador de datos personales debe implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad. La aceptación de la implementación de las medidas de seguridad por parte del receptor o importador de datos personales debe establecerse por escrito mediante cláusulas contractuales u otro instrumento jurídico. 2.3.4.6. La información de datos			No se evidencia de procedimientos formales de implementación de técnicas de encriptación para la protección de intercambio de información.	**Inexistente**
CONTROL	A.13.2.2	Acuerdo sobre transferencia de información			2.3.4.7.	2.3.4.7. El receptor o importador de datos personales debe implementar las medidas de seguridad definidas por el emisor o exportador de datos			No se cuenta con acuerdos en la transferencia segura de información con terceros.	**Inexistente**

CONTROL	A.13.2.3	Mensajes electrónicos			2.3.4.5, 2.3.4.6	2.3.4.5. Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad. 2.3.4.6. La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad. Transporte electrónico de datos			Se cuenta con software Antispam para el servicio de correo electrónico, pero no existen mecanismos de protección de la información por este medio.	**Inexistente**
CONTROL	A.13.2.4	Acuerdos de confidencialidad o no divulgación			2.3.2.4	2.3.2.4. Seguridad en la copia o reproducción de documentos: - El titular del banco de datos personales debe designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales. - Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales: a) Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados. b) Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo. c) Retirar los documentos			No se cuenta con acuerdos de confidencialidad por parte de la Universidad para los empleados a fin de que reflejen el cumplimiento obligatorio para la protección de la información.	**Inexistente**
DOMINIO	**A.14**	**Adquisición, desarrollo y**								
OBJETIVO	A.14.1	Requisitos de seguridad de los sistemas de información								
CONTROL	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información							Cuando se realizan adquisición, desarrollo o mantenimiento de sistemas de información, no se incluyen requisitos relacionados con la seguridad de la información debidamente formalizados.	**Limitado**
CONTROL	A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas			2.3.1.1	2.3.1.1. e) Cuando el acceso al sistema esté expuesto en entornos públicos (intranet, internet o similares), se debe bloquear al usuario luego de cinco (05) intentos fallidos de autenticación consecutivos			No se pudo verificar que en su totalidad los servicios emitidos a través de redes públicas estén siendo monitoreados y que se encuentren configurados de acuerdo a las mejores prácticas.	**Inicial**
CONTROL	A.14.1.3	Protección de transacciones en servicios de aplicación							No se evidencia que los servicios otorgados cumplen con protocolos de seguridad para la transferencia de datos.	**Inexistente**
OBJETIVO	A.14.2	Seguridad en los procesos de desarrollo y soporte								

CONTROL	A.14.2.1	Política de desarrollo seguro							No se cuenta con un política y procedimiento de desarrollo seguro de software en la Universidad.	**Inexistente**
CONTROL	A.14.2.2	Procedimientos de control de cambio del sistema							No se cuenta con procedimientos de control de cambios en los sistemas de información de la Universidad.	**Inexistente**
CONTROL	A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa							No se cuenta con procedimientos formales que establezca la ejecución de pruebas de seguridad luego de algún cambio en el software instalado.	**Inexistente**
CONTROL	A.14.2.4	Restricciones sobre cambios a los paquetes de software							En los servidores bajo responsabilidad de la Oficina de Tecnología se realizan actividades de restricción a los cambios en paquetes, pero esta práctica no se evidencia en los equipos cliente de la Universidad.	**Limitado**
CONTROL	A.14.2.5	Principios de ingeniería de sistemas seguros.							Se cuenta con un procedimiento de arquitectura base la cual no ha sido formalizada ni revisada, asimismo no está alineada a los principios de implementación del SGSI sobre los sistemas de información desarrollados.	**Inicial**
CONTROL	A.14.2.6	Ambiente de desarrollo seguro							Se cuenta con entornos seguros para el desarrollo de software debidamente restringidos, sin embargo los ambientes físicos son susceptibles de acceso de la comunidad universitaria.	**Inicial**
CONTROL	A.14.2.7	Desarrollo contratado externamente							Se realizan labores de supervisión y monitoreo con proveedores, pero no basados en procedimientos no se evidencia la ejecución de pruebas y control de cambios asimismo la aceptación de usuarios no siempre es comunicada a la Oficina de Tecnología.	**Inicial**

CONTROL	A.14.2.8	Pruebas de seguridad del sistema							No se cuenta con procedimientos de gestión de cambios en los sistemas de información que evidencie lineamientos que establezcan la ejecución de pruebas de seguridad como parte del proceso de desarrollo de sistemas.	**Inexistente**
CONTROL	A.14.2.9	Pruebas de aceptación del sistema.							Se cuenta con registros de aceptación de los usuarios, pero no se puede evidenciar que se establezcan programas de prueba con criterios de aceptación de los sistemas, actualizaciones y/o nuevas versiones debidamente detallados.	**Inicial**
OBJETIVO	A.14.3	Datos de prueba								
CONTROL	A.14.3.1	Protección de datos de prueba							No se cuenta con evidencia documentada que se realiza selección de datos de prueba en las implementaciones de desarrollo de software.	**Inexistente**
DOMINIO	**A.15**	**Relaciones con los proveedores**								
OBJETIVO	A.15.1	Seguridad de la información en las relaciones con los proveedores								
CONTROL	A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores			2.3.4.7, 2.3.4.8	2.3.4.7. El receptor o importador de datos personales debe implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad.			No se cuenta con políticas de seguridad para proveedores y terceras personas.	**Inexistente**
CONTROL	A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores			2.3.4.7, 2.3.4.8	2.3.4.7. El receptor o importador de datos personales debe implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad. 2.3.4.8. Seguridad en servicios			Se establecen consideraciones de seguridad de la información con los proveedores, pero no se cuenta con una política que la formalice.	**Inicial**
CONTROL	A.15.1.3	Cadena de suministro de tecnología de información y comunicación			2.3.4.8	2.3.4.7. El receptor o importador de datos personales debe implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad. 2.3.4.8. Seguridad en servicios de tratamiento de datos personales por medios			No se cuenta con requisitos sustentados en una política para abordar riesgos de seguridad asociadas a cadenas de suministro de los servicios y productos de tecnología de información y comunicaciones.	**Inexistente**
OBJETIVO	A.15.2	Gestión de entrega de servicios del proveedor								
CONTROL	A.15.2.1	Monitoreo y revisión de servicios de los proveedores							No se puede verificar que se realice un adecuado seguimiento de proveedores con respecto al uso y traslado de información de la Universidad.	**Inexistente**

CONTROL	A.15.2.2	Gestión de cambios a los servicios de proveedores			2.3.4.8	2.3.4.8. Seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados.			No se realiza la administración de cambios a la provisión de servicios prestados por terceros, no se evidencia procedimiento formal de seguridad de la información al respecto.	**Inexistente**
DOMINIO	**A.16**	**Gestión de incidentes de seguridad de la información**								
OBJETIVO	A.16.1	Gestión de incidentes de seguridad de la información y mejoras								
CONTROL	A.16.1.1	Responsabilidades y procedimientos	2.1.10	2.1.10 Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales.					No se cuenta con políticas para la gestión de incidentes de SI que establezca responsabilidades, lineamientos de monitoreo y una adecuada clasificación de incidentes.	**Inexistente**
CONTROL	A.16.1.2	Reporte de eventos de seguridad de la información	1.3.1.4 1.4.2 1.4.3 1.4.4	1.3.1.4. Implementar y mantener los siguientes procedimientos documentados. 1.4.2 c) Registro de incidentes y medidas adoptadas. 1.4.3 c) Registro de auditorías. d) Registro de incidentes y problemas. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733.	2.3.4.2, 2.3.4.9	2.3.4.2. El titular del banco de datos personales debe informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho. La información mínima que se debe proporcionar incluye: a) Naturaleza del incidente. b) Datos personales comprometidos. c) Recomendaciones al titular de datos personales. d) Medidas correctivas implementadas. 2.3.4.9. Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado			No se cuenta con canales de comunicación de eventos de seguridad de la información debidamente formalizados.	**Inicial**
CONTROL	A.16.1.3	Reporte de debilidades de seguridad de la información	1.3.1.4 1.4.2 1.4.3 1.4.4	1.3.1.4. Implementar y mantener los siguientes procedimientos documentados. 1.4.2 c) Registro de incidentes y medidas adoptadas. 1.4.3 c) Registro de auditorías. d) Registro de incidentes y problemas. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un	2.3.4.9	2.3.4.9. Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado del banco de datos personales. El encargado del banco de datos personales o quien sea designado por el titular del			No se cuenta con canales de comunicación para notificación de vulnerabilidades de seguridad.	**Inexistente**

CONTROL	A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	1.3.1.4 1.4.2 1.4.3 1.4.4	1.3.1.4. Implementar y mantener los siguientes procedimientos documentados. 1.4.2 c) Registro de incidentes y medidas adoptadas. 1.4.3 c) Registro de auditorías. d) Registro de incidentes y problemas. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733.	2.3.4.2, 2.3.4.9	2.3.4.2. El titular del banco de datos personales debe informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho. La información mínima que se debe proporcionar incluye: a) Naturaleza del incidente. b) Datos personales comprometidos. c) Recomendaciones al titular de datos personales. d) Medidas correctivas implementadas. 2.3.4.9. Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad			No se cuenta con un procedimiento de identificación de incidentes, estableciendo su clasificación y niveles de prioridad.	**Inexistente**
CONTROL	A.16.1.5	Respuesta a incidentes de seguridad de la información	1.3.1.4 1.4.2 1.4.3 1.4.4	1.3.1.4. Implementar y mantener los siguientes procedimientos documentados. 1.4.2 c) Registro de incidentes y medidas adoptadas. 1.4.3 c) Registro de auditorías. d) Registro de incidentes y problemas. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733.	2.3.4.2, 2.3.4.9	2.3.4.2. El titular del banco de datos personales debe informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho. La información mínima que se debe proporcionar incluye: a) Naturaleza del incidente. b) Datos personales comprometidos. c) Recomendaciones al titular de datos personales. d) Medidas correctivas implementadas. 2.3.4.9. Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad			No se cuenta con procedimientos documentados para respuesta a incidentes de seguridad.	**Inexistente**
CONTROL	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	1.3.1.4 1.4.4	1.3.1.4. Implementar y mantener los siguientes procedimientos documentados. 1.4.2 c) Registro de incidentes y medidas adoptadas. 1.4.3 c) Registro de auditorías. d) Registro de incidentes y problemas. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un registro de control de acceso, según el artículo 39 del reglamento de la Ley N° 29733	2.3.4.12	2.3.4.12. Acciones correctivas y mejora continúa.			No se documentan las resoluciones de incidentes de seguridad.	**Inexistente**
CONTROL	A.16.1.7	Recolección de evidencia	1.3.1.4 1.4.2 1.4.3 1.4.4	1.3.1.4. Implementar y mantener los siguientes procedimientos documentados. 1.4.2 c) Registro de incidentes y medidas adoptadas. 1.4.3 c) Registro de auditorías. d) Registro de incidentes y problemas. 1.4.4 Procedimientos documentados requeridos en el Sistema de Gestión de la Seguridad de la Información - SGSI, incluyendo además un	2.3.4.9	2.3.4.9. Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado del banco de datos personales. El encargado del banco de datos personales o quien sea designado por el titular del			No se cuenta con procedimientos debidamente formalizados que identifique y preservan información que pueda servir de evidencia ante un ataque a la seguridad de la información en servidores.	**Inicial**
DOMINIO	**A.17**	**Aspectos de seguridad de la**								

OBJETIVO	A.17.1	Continuidad de seguridad de la información								
CONTROL	A.17.1.1	Planificación de continuidad de seguridad de la información							No se evidencia que se han implementado estrategias para garantizar continuidad de la seguridad de la información y su gestión durante situaciones adversas tales como crisis y desastres, cabe precisar que la Oficina de Tecnología esta desarrollando un BIA a nivel de sus servicios.	**Inicial**
CONTROL	A.17.1.2	Implementación de continuidad de seguridad de la información							No se cuenta con un procedimientos formales para garantizar la continuidad de la seguridad de la información en situaciones adversas.	**Inicial**
CONTROL	A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información.							No se han implementado controles a evaluar para la continuidad de la seguridad de la información.	**Inexistente**
OBJETIVO	A.17.2	Redundancias								
CONTROL	A.17.2.1	Instalaciones de procesamiento de la información			2.3.3.3	2.3.3.3. Se deben realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido.			Se cuenta con redundancia en servidores a nivel de caja a caja del Data Center bajo resposabilidad de la Oficina de Tecnología , pero no a nivel instalaciones de procesamiento de información en correspondencia con los requisitos de disponibilidad.	**Limitado**
DOMINIO	**A.18**	**Cumplimiento**								
OBJETIVO	A.18.1	Cumplimiento con requisitos legales y contractuales								
CONTROL	A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables							La Oficina de Tecnología cuenta con información respecto a la legislación aplicable y normativa acerca de seguridad de la información, pero no ha establecido fecha para dar inicio del cumplimiento de estos requisitos.	**Inicial**

CONTROL	A.18.1.2	Derechos de propiedad intelectual			2.3.2.4	2.3.2.4. Seguridad en la copia o reproducción de documentos: - El titular del banco de datos personales debe designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales. - Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales: a) Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados.			No se cuenta con procedimientos para el cumplimiento de los requisitos de salvaguarda de los derechos de propiedad intelectual de productos de software, asimismo no se cuenta con políticas en los equipos que no permitan instalar software sin autorización.	**Inexistente**
CONTROL	A.18.1.3	Protección de registros							No se han identificado los registros críticos que deben contar con un tratamiento especifico, por tanto no se hay evidencia de actividades para salvaguardarlos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados.	**Inexistente**
CONTROL	A.18.1.4	Privacidad y protección de datos personales	1.3.1.1 1.4.1 2.a	1.3.1.1 Determinar y dar a conocer una política de protección de datos personales: Una declaración breve y directa que demuestre el compromiso institucional y el involucramiento de sus autoridades con la protección de los datos personales en el tratamiento que se de a los datos personales contenidos en el banco de datos personales bajo su titularidad. 1.4.1 e) Incluir compromiso de respeto a los principios de la Ley N° 29733, Ley de Protección de Datos Personales. 2. a)Para los tratamientos determinados como complejos o críticos, se deben implementar los controles adecuados de un sistema de gestión de seguridad de la información bajo los requisitos y controles de la NTP-ISO/IEC 27001 EDI en su edición vigente, incorporando a los bancos de datos personales dentro del alcance del SGSI, asegurando como mínimo el cumplimiento					La medidas de seguridad para el cumplimiento de la ley de protección de datos personales Ley 29733 vigente, a la fecha no se encuentran implementadas.	**Inexistente**
CONTROL	A.18.1.5	Regulación de controles criptográficos			2.3.4.5	2.3.4.5. Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.			No se cuenta con Políticas, directivas o procedimientos que regulen el uso de controles criptográficos en la Universidad.	**Inexistente**
OBJETIVO	A.18.2	Revisiones de seguridad de la información								

CONTROL	A.18.2.1	Revisión independiente de la seguridad de la información	2.1.4 2.1.9	2.1.4 Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales. 2.1.9 Desarrollar un procedimiento de auditoría	2.3.4.11	2.3.4.11. Se debe realizar una auditoría sobre el cumplimiento de la presente directiva, bajo responsabilidad del titular del banco de datos personales.			No se cuenta con procedimientos formales para la revisión de la gestión de la seguridad de la información por entidades independientes.	**Inexistente**
CONTROL	A.18.2.2	Cumplimiento de políticas y normas de seguridad	2.1.4 2.1.9	2.1.4 Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales. 2.1.9 Desarrollar un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una	2.3.4.11	2.3.4.11. Se debe realizar una auditoría sobre el cumplimiento de la presente directiva, bajo responsabilidad del titular del banco de datos personales.			Las Dependencias de la Universidad no realizan una identificación de los requisitos de seguridad de la información a nivel de los requerimientos regulatorios y normativos internos.	**Inexistente**
CONTROL	A.18.2.3	Revisión del cumplimiento técnico							No se cuenta con evidencia de planificación de test de vulnerabilidades, técnicas y/o test de penetración a bases de datos, sistemas de aplicación y aplicaciones de la Universidad.	**Inexistente**

Anexo C

Metodología de Análisis, Evaluación de Tratamiento de Riesgos de Seguridad de la Información

<table>
<tr><td rowspan="4">UNS</td><td>METODOLOGIA</td><td colspan="2">CÓDIGO: SGSI-METO-01</td></tr>
<tr><td colspan="3">TITULO:
IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS</td></tr>
<tr><td colspan="2">Aprobado por:</td><td>Fecha Aprobación:</td></tr>
<tr><td>Reemplaza a:</td><td>N° Páginas
22</td><td>Fecha Publicación:</td></tr>
</table>

METODOLOGÍA

IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

UNS

SGSI-METO-01

INDICE

1. OBJETIVO 3
2. ALCANCE 3
3. DEFINICIONES 3
4. DOCUMENTOS A CONSULTAR 4
5. RESPONSABILIDADES 4
6. DESARROLLO DE LA METODOLOGÍA 5
6.1. Identificación de Activos 5
6.2. Identificación de las Amenazas 5
6.3. Identificación de Vulnerabilidades 6
6.4. Determinación del Impacto 6
6.5. Determinación de la Probabilidad de Ocurrencia 13
6.6. Determinación del Riesgo Efectivo 13
7. TRATAMIENTO DEL RIESGO 15
8. REGISTROS Y ANEXOS 16
9. CONTROL DE CAMBIOS 24

1. OBJETIVO

Establecer una metodología de identificación, análisis y evaluación de los riesgos de seguridad de la información.

2. ALCANCE

Aplica a la evaluación de riesgos de seguridad de la información de los Procesos que forman parte del alcance del SGSI de la Universidad.

3. DEFINICIONES

3.1. **Activo:** Todo aquello que tenga valor para la UNS.

3.2. **Confidencialidad:** Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados.

3.3. **Disponibilidad:** Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

3.4. **Estimación del Riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

3.5. **Identificación de Riesgos:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

3.6. **Impacto:** Es la consecuencia de la explotación de una vulnerabilidad por una amenaza debido a la falta o falla de controles, generando pérdida en confidencialidad, integridad y disponibilidad de la información u otros activos.

3.7. **Integridad:** Propiedad de salvaguardar la exactitud y completitud de los activos.

3.8. **Inventario de Activos:** Es un registro conformado por los activos de información que tienen valor para la UNS y que están dentro del alcance del SGSI.

3.9. **Probabilidad:** Es la posibilidad de que un evento cualquiera ocurra o no. A mayor probabilidad del evento existe más posibilidad de que ocurra, es decir, existen buenas razones para creer que sucederá.

3.10. **Propietario:** Identifica a la persona o la entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

3.11. **Riesgo:** Es la probabilidad de que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.

4. DOCUMENTOS A CONSULTAR

4.1. Norma ISO/IEC 27001:2013.

4.2. Norma ISO/IEC 27002:2013.

4.3. Norma ISO/IEC 27005:2011.

4.4. Norma ISO/IEC 31000:2009.

5. RESPONSABILIDADES

5.1. Los Propietarios de los Activos de Información

- Dar cumplimiento a este procedimiento.
- Promover la participación activa del personal en la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Revisar y dar la conformidad a la matriz de riesgos.

5.2. El Comité de Gestión de Seguridad de Información

- Aprobar el resultado de la evaluación de riesgos.

5.3. El Oficial de Seguridad de la Información

- Verificar el cumplimiento del presente documento.
- Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Compilar información remitida por los propietarios relacionada a la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Presentar a los propietarios de procesos el resultado del análisis de riesgos.
- Presentar al Comité de Gestión de Seguridad de Información el resultado del análisis de riesgos para su aprobación.

6. DESARROLLO DE LA METODOLOGÍA

El proceso de Análisis de Riesgos está sujeto a métodos de valorización cualitativos y está orientado a los activos de información, que soportan los procesos de la Universidad.

Para el desarrollo del análisis de riesgos nos apoyaremos del procedimiento de Inventario de Activos de Información, para luego utilizar el formato SGSI-FORM-2 Análisis y Evaluación de Riesgos.

6.1. Identificación de Activos

La identificación y valorización de activos de información, se realizará según lo indicado en el procedimiento SGSI-PROC-01 Clasificación de Activos de Información y el formato SGSI-FORM-1 Inventario de Activos.

Una vez valorizados los activos, solo se realizará el análisis de riesgos a los activos de información cuyo valor sea ***alto***, los mismos que se incluirán en el formato SGSI-FORM-2 Análisis y Evaluación de Riesgos.

6.2. Identificación de las Amenazas

Amenaza: es un evento que potencialmente puede causar daño. Para la identificación de las amenazas se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 01 - Tabla de Amenazas) como referencia.

ACTIVO	AMENAZA

6.3. Identificación de Vulnerabilidades

Vulnerabilidad: es una debilidad que puede ser explotada por una amenaza. Para la identificación de las vulnerabilidades se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 02 - Tabla de Vulnerabilidades) como referencia.

ACTIVO	AMENAZA	VULNERABILIDAD

6.4. Determinación del Impacto

Para determinar como la amenaza afecta la preservación de la Confidencialidad, Integridad y Disponibilidad (CID) del activo, se evaluará cada uno de los criterios.

ACTIVO	AMENAZA	VULNERABILIDAD	¿Qué afecta en los activos de información?				RIESGO EFECTIVO
			C	I	D	VALOR CID	IMPACTO

6.4.1. Evaluación del Criterio CID

Primero se evaluará cada uno de los criterios CID, se tomarán los siguientes valores:

Para cada caso utilizaremos las siguientes tablas:

a. Tabla de Valorización de Confidencialidad

Valor	Clasificación	Definición	Consecuencia
3	**Alta**	Es la información o recurso que debe ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	La divulgación no autorizada produce: - Pérdida de la ventaja competitiva. - Uso malicioso en contra de la UNS. - Pérdidas financieras que no pueden ser absorbidas por la UNS. - Demandas legales que dañan la imagen y confianza pública de la UNS.
2	**Media**	Es la información que debe ser divulgada sólo al personal de las áreas que la manejan y modificada sólo por personas autorizadas e individualizadas.	La divulgación no autorizada produce: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por la UNS. - No se producen demandas legales.
1	**Baja**	Es la información que puede ser divulgada al público en general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para la UNS.

b. Tabla de Valorización de Integridad

Valor	Clasificación	Criterio	Consecuencia
3	**Alta**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud.	La falta de integridad produce daños de gran magnitud los que se pueden expresar como: - Pérdidas económicas (pérdida, incumplimiento de metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable). - Daño de la imagen de la UNS (daño a nivel nacional e internacional que no se puede reparar en el corto plazo). - Pérdida de la confianza de los usuarios.
2	**Media**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud los que se pueden expresar como: - Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable). - Daño de la imagen de la UNS (daño a nivel nacional, se puede reparar en el corto plazo). - No se pierde la confianza de los usuarios.
1	**Baja**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: - Pérdidas económicas (no impacta las ganancias, se cumplen las metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo pero este es manejable). - Daño de la imagen de la UNS (daño a nivel nacional que puede no ser

Valor	Clasificación	Criterio	Consecuencia
			percibido y se puede reparar prontamente). - No se pierde la confianza de los usuarios.

c. Tabla de Valorización de Disponibilidad

Valor	Clasificación	Definición	Consecuencia
3	**Alta**	Es información o activo indispensable para la continuidad de la UNS. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: - Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. - Perjuicios legales que afectan la imagen de la UNS. - Perjuicios económicos que no pueden ser absorbidos por la UNS. - Problemas sindicales.
2	**Media**	La disponibilidad de la información es necesaria para la continuidad de la UNS, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable. El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de	La falta de disponibilidad produce: - Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. - Perjuicios legales que no comprometen la imagen de la UNS. - Perjuicios económicos que pueden ser absorbidos por la UNS. - No hay problemas sindicales.

Valor	Clasificación	Definición	Consecuencia
		tiempo en horarios críticos.	
1	Baja	Es información o activos de apoyo o secundarios para el negocio. La información se encuentra duplicada en varias fuentes. Si no está disponible no compromete procesos operativos importantes	La falta de disponibilidad produce: - Que los niveles de servicio acordados para los procesos operativos importantes, no se ven afectados. - Problemas administrativos y operativos no significativos. - Perjuicios económicos que no son significativos. - No hay perjuicios legales. - No hay problemas sindicales.

6.4.2. Valor CID

Se calcula el valor CID de acuerdo a la siguiente tabla

a. Tabla de Valorización

Aspecto de Seguridad afectado por el riesgo			IMPACTO
C	I	D	
1	1	1	No Significativo
1	1	2	Menor
1	1	3	Significativo
1	2	1	Menor
1	2	2	Moderado
1	2	3	Significativo
1	3	1	Significativo
1	3	2	Significativo
1	3	3	Catastrófico
2	1	1	Menor
2	1	2	Moderado
2	1	3	Significativo
2	2	1	Moderado
2	2	2	Moderado
2	2	3	Significativo
2	3	1	Significativo
2	3	2	Significativo
2	3	3	Catastrófico
3	1	1	Significativo
3	1	2	Significativo
3	1	3	Catastrófico
3	2	1	Significativo
3	2	2	Significativo
3	2	3	Catastrófico
3	3	1	Catastrófico
3	3	2	Catastrófico
3	3	3	Catastrófico

6.4.3. Determinación del Impacto en la Universidad

Finalmente se determina el impacto de acuerdo a la siguiente tabla:

a. Tabla de Valorización del Impacto del Riesgo

Nivel	Descripción	Impacto en la Universidad
5	Catastrófico	Impacta en forma severa en la UNS al punto de comprometer la confidencialidad o integridad de información crítica de la Universidad o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la Universidad y su efecto se siente en todo el personal involucrado.
4	Significativo	Impacta en forma grave a un área o servicio específico de la UNS, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves de la UNS por un tiempo considerable. Su efecto está limitado dentro de la UNS.
3	Moderado	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	Menor	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	No Significativo	No representa un impacto importante para la UNS.

6.5. Determinación de la Probabilidad de Ocurrencia

Finalmente se determina la probabilidad de ocurrencia.

ACTIVO	AMENAZA	VULNERABILIDAD	¿Qué afecta en los activos de información?				RIESGO EFECTIVO	
			C	I	D	VALOR CID	IMPACTO	PROBABILIDAD

Para este caso utilizaremos los siguientes valores:

Valor	Clasificación	Definición
1	Muy Baja	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año.
2	Baja	Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
3	Moderada	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	Alta	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta. 1 vez al mes.
5	Muy Alta	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.

6.6. Determinación del Riesgo Efectivo

El riesgo efectivo es la medida del daño probable causado por una amenaza que se materializa en un activo.

ACTIVO	AMENAZA	VULNERABILIDAD	¿Qué afecta en los activos de información?				RIESGO EFECTIVO				
			C	I	D	VALOR CID	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	NOMBRE DEL RIESGO	CÓDIGO DE RIESGO

Con el valor obtenido del producto del Impacto por la Probabilidad obtenemos el Riesgo, para esta actividad utilizaremos la Tabla de Valorización del Riesgo.

a. Tabla de Valorización del Riesgo

Tabla de Valorización de Riesgos					
Impacto		**Probabilidad**		**Riesgo**	
Catastrófico	5	Muy Alta	5	Extremo	25
Significativo	4	Muy Alta	5	Extremo	20
Moderado	3	Muy Alta	5	Extremo	15
Menor	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Catastrófico	5	Alta	4	Extremo	20
Significativo	4	Alta	4	Extremo	16
Moderado	3	Alta	4	Alto	12
Menor	2	Alta	4	Mediano	8
No Significativo	1	Alta	4	Bajo	4
Catastrófico	5	Moderada	3	Extremo	15
Significativo	4	Moderada	3	Alto	12
Moderado	3	Moderada	3	Alto	9
Menor	2	Moderada	3	Mediano	6
No Significativo	1	Moderada	3	Bajo	3
Catastrófico	5	Baja	2	Alto	10
Significativo	4	Baja	2	Mediano	8
Moderado	3	Baja	2	Mediano	6
Menor	2	Baja	2	Bajo	4
No Significativo	1	Baja	2	No Significativo	2
Catastrófico	5	Muy Baja	1	Mediano	5
Significativo	4	Muy Baja	1	Bajo	4
Moderado	3	Muy Baja	1	Bajo	3
Menor	2	Muy Baja	1	No significativo	2
No Significativo	1	Muy Baja	1	No significativo	1

Nivel de Riesgo:

Del 1 a 2 → No Significativo
Del 3 a 4 → Bajo
Del 5 a 8 → Mediano
Del 9 a 12 → Alto
Del 15 a 25 → Extremo

Los riesgos serán clasificados de acuerdo a niveles, según su grado de exposición, lo cual se muestra en la siguiente tabla:

Nivel de Riesgo	Descripción de las Consecuencias
Extremo	Puede afectar seriamente a la UNS, en términos de paralización de las operaciones, daño a la imagen de la UNS. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
Alto	Puede afectar los niveles de operación y servicio de la UNS, incumplimiento de metas, y divulgación no autorizada de información fuera de la UNS. Requiere una acción correctiva sujeta a la discreción del Responsable del Proceso en términos de plazos y compromisos.
Mediano	Afecta a los activos de información de soporte a los procesos principales, puede afectar la disponibilidad en áreas específicas de la UNS. La divulgación no autorizada no representa perjuicio importante para la UNS. Su aceptación está sujeta a la revisión del Responsable del Proceso.
Bajo	No causa un efecto considerable en la UNS. Usualmente son aceptados sin revisión.
No Significativo	El efecto para la UNS es insignificante. Usualmente no se les considera para la gestión de riesgos.

7. TRATAMIENTO DEL RIESGO

La UNS reconoce los siguientes niveles de riesgos:

"Extremo", "Alto", "Mediano", "Bajo y "No Significativo".

Para la etapa de tratamiento del riesgo, se han considerado como aceptables los riesgos definidos como:

"Mediano", "Bajo" y "No Significativo".

Para los riesgos de nivel "Extremo" y "Alto" se procederán a evaluar las siguientes opciones de tratamiento de riesgo:

Reducir el riesgo, Evitar el riesgo o Transferir el riesgo, los mismos que se incluirán en el formato SGSI-FORM-3 Plan de Tratamiento de Riesgos.

Cabe mencionar que durante la etapa de tratamiento de riesgos, cuando el costo de reducir el riesgo sea mayor, al costo del riesgo y/o al activo que lo produce, entonces también el riesgo se considera aceptable y se incluirán en el formato SGSI-FORM-4 Aceptación de Riesgos.

La decisión sobre el tratamiento de un riesgo se realiza en cada ciclo de evaluación, la cual se realizará una vez al año o cuando ocurran cambios en los procesos del SGSI. Los planes de tratamiento de riesgo, son revisados con periodicidad no mayor a un año por parte del Responsable del Proceso, los nuevos riesgos efectivos son medidos y comparados con los riesgos residuales estimados.

Finalmente se debe tomar en cuenta la elaboración de la Declaración de Aplicabilidad, la cual consiste en listar todos los controles definidos en el Anexo A de la norma ISO/IEC 27001:2013 el cuál se corresponde a detalle en la norma ISO/IEC 27002:2013, y luego precisar qué controles son necesarios y adecuados para implementar en la UNS, así como la argumentación de las inclusiones, si se aplicaran, y la argumentación de las exclusiones si no se aplicaran en el formato SGSI-FORM-5 Declaración de Aplicabilidad.

8. REGISTROS Y ANEXOS

8.1. SGSI-FORM-2 Análisis y Evaluación de Riesgos

8.2. SGSI-FORM-3 Plan de Tratamiento de Riesgos

8.3. SGSI-FORM-4 Aceptación de Riesgos

8.4. Anexo N° 1: Tabla de Amenazas

Código	Amenaza	Tipo
AM1	Incendio	Daño físico
AM2	Daño por agua	
AM3	Contaminación	
AM4	Accidente mayor	
AM5	Destrucción del equipo o los medios	
AM6	Polvo, corrosión, congelación	
AM7	Fenómeno climático	Eventos naturales
AM8	Fenómeno sísmico	
AM9	Fenómeno volcánico	
AM10	Fenómeno meteorológico	
AM11	Inundación	
AM12	Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
AM13	Pérdida del suministro de electricidad	
AM14	Falla del equipo de telecomunicaciones	
AM15	Radiación electromagnética	Perturbación debido a radiación
AM16	Radiación térmica	
AM17	Pulsos electromagnéticos	
AM18	Intercepción de señales de interferencia comprometedoras	Compromiso de la información
AM19	Espionaje remoto	
AM20	Interceptación de comunicaciones	
AM21	Robo de medios o documentos	
AM22	Robo de equipos	
AM23	Hallazgo de medios reciclados o descartados	
AM24	Divulgación	
AM25	Datos de fuentes no confiables	
AM26	Adulteración del Hardware	
AM27	Adulteración del software	
AM28	Detección de posición	

Código	Amenaza	Tipo
AM29	Falla de equipo	Fallas técnicas
AM30	Mal funcionamiento del equipo	
AM31	Saturación del sistema de información	
AM32	Mal funcionamiento del software	
AM33	Uso no autorizado del equipo	Acciones no autorizadas
AM34	Copia fraudulenta del software	
AM35	Uso de software falsificado o copiado	
AM36	Corrupción de datos	
AM37	Procesamiento ilegal de datos	
AM38	Error en el uso	Compromiso de funciones
AM39	Abuso de derechos	
AM40	Falsificación de derechos	
AM41	Negación de acciones	
AM42	Ruptura en la disponibilidad del personal	
AM43	Hacking	Hacker, cracker
AM44	Ingeniería social	
AM45	Intrusión en el sistema, incursiones	
AM46	Acceso no autorizado al sistema	
AM47	Crimen informático (acoso cibernético)	Criminal informático
AM48	Acto fraudulento (reproducción de archivos, suplantación, intercepción)	
AM49	Soborno informático	
AM50	Falsificación o usurpación de la dirección	
AM51	Intrusión en el sistema	
AM52	Bomba/Terrorismo	Terrorismo
AM53	Equipo de guerra informática	
AM54	Ataque al sistema (ej. DDOS)	
AM55	Penetración en el sistema	
AM56	Adulteración del sistema	
AM57	Ventaja de defensa	Espionaje
AM58	Ventaja política	

Código	Amenaza	Tipo
AM59	Explotación económica	
AM60	Robo de información	
AM61	Intrusión en la privacidad personal	
AM62	Asalto a un empleado	Gente de adentro de la Universidad (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)
AM63	Chantaje	
AM64	Búsqueda de información propietaria	
AM65	Abuso informático	
AM66	Fraude y robo	
AM67	Soborno por información	
AM68	Ingreso de datos falsificados o corruptos	
AM69	Intercepción	
AM70	Códigos maliciosos (ej. Virus, bomba lógica, troyano)	
AM71	Venta de información personal	
AM72	Disfunciones del sistema (bugs)	
AM73	Intrusión en el sistema	
AM74	Sabotaje al sistema	
AM75	Incorrecta configuración, daño de un componente ocasionado por terceros	
AM76	Incumplimiento de contrato	
AM77	Pérdida de cintas de backup	
AM78	Deterioro de cintas de backup	
AM79	Daño físico al cableado de red ocasionado por terceros	
AM80	Daño físico al cableado eléctrico ocasionado por terceros	
AM81	Daño físico a las instalaciones ocasionado por terceros	
AM82	Acceso no autorizado	
AM83	Caída del servicio de telefonía fija	
AM84	Indisponibilidad del proveedor	
AM85	Caída del servicio de Info Internet	
AM86	Caída del servicio de correo electrónico	
AM87	Movilizaciones	

8.5. Anexo N° 2: Tabla de Vulnerabilidades

Código	Vulnerabilidad	Categoría
VU1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Hardware
VU2	Falta de esquemas de reemplazo periódicos	
VU3	Susceptibilidad a la humedad, al polvo y a la suciedad	
VU4	Sensibilidad a la radiación electromagnética	
VU5	Falta de control eficiente del cambio de configuración	
VU6	Susceptibilidad a variación de voltaje	
VU7	Susceptibilidad a variaciones de temperatura	
VU8	Almacenamiento no protegido	
VU9	Falta de cuidado al descartarlo	
VU10	Copia no controlada	
VU11	Pruebas al software inexistentes o insuficientes	Software
VU12	Errores conocidos en el software	
VU13	No hacer "logout" cuando se sale de la estación de trabajo	
VU14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU15	Falta de evidencia de auditoria	
VU16	Asignación equivocada de derechos de acceso	
VU17	Software ampliamente distribuido	
VU18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
VU19	Interfaz de usuario complicada	
U20	Falta de documentación	
VU21	Seteo incorrecto de parámetros	
VU22	Fechas incorrectas	
VU23	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	

Código	Vulnerabilidad	Categoría
VU24	Tablas de claves no protegidas	
VU25	Mala administración de claves	
VU26	Habilitación de servicios innecesarios	
VU27	Software inmaduro o nuevo	
VU28	Especificaciones no claras o incompletas para los desarrolladores	
VU29	Falta de control de cambios eficaz	
VU30	Descarga y uso incontrolado de software	
VU31	Falta de copias de respaldo	
VU32	Falta de protección física del edificio, puertas y ventanas	
VU33	No producir informes de gestión	
VU34	Falta de pruebas de envió o recepción de mensaje	**Red**
VU35	Líneas de comunicación no protegidas	
VU36	Tráfico delicado no protegido	
VU37	Juntas malas en el cableado	
VU38	Punto de falla única	
VU39	Falta de identificación y autentificación de destinador y destinatario	
VU40	Arquitectura de red insegura	
VU41	Transferencia de claves en claro	
VU42	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
VU43	Conexiones no protegidas de la red publica	
VU44	Ausencia del personal	**Personal**
VU45	Procedimientos inadecuados del reclutamiento	
VU46	Capacitación de seguridad insuficiente	
VU47	Uso incorrecto del software y hardware	
VU48	Falta de conciencia de seguridad	
VU49	Falta de mecanismos de monitoreo	

Código	Vulnerabilidad	Categoría
VU50	Trabajo no supervisado del personal externo o de limpieza	
VU51	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
VU52	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
VU53	Ubicaciones en una área susceptible a las inundaciones	
VU54	Red inestable de energía eléctrica	
VU55	Falta de protección física del edificio, puertas y ventanas	
VU56	Falta de un procedimiento formal para el registro y baja de usuarios	Universidad
VU57	Falta de proceso formal para revisar el derecho de acceso (supervisión)	
VU58	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	
VU59	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	
VU60	Falta de auditorías regulares (supervisión)	
VU61	Falta de procedimientos de identificación y evaluación del riesgo	
VU62	Falta de informes de fallas registradas en los registros del administrador y del operador	
VU63	Respuesta inadecuada del mantenimiento del servicio	
VU64	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
VU65	Falta de procedimiento de control de cambios	
VU66	Falta de procedimiento formal para el control de la documentación de la UNS	
VU67	Falta de procedimiento formal para la supervisión del registro de la UNS	
VU68	Falta de proceso formal para autorización de información pública disponible	
VU69	Falta de asignación apropiada de responsabilidades de seguridad en la información	
VU70	Falta de planes de continuidad	
VU71	Falta de una política de uso de correos electrónicos	
VU72	Falta de procedimientos para introducir software en sistemas operativos	
VU73	Faltas de registro en los historiales del administrador y del operador	
VU74	Falta de procedimientos para manejo de la información clasificada	
VU75	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	

Código	Vulnerabilidad	Categoría
VU76	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
VU77	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	
VU78	Falta de política formal sobre el uso de computadoras portátiles	
VU79	Falta de control de activos que se encuentran fuera del local	
VU80	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
VU81	Falta de autorización al acceso a las instalaciones de procesamiento de la información	
VU82	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	
VU83	Falta de revisiones regulares de la gestión	
VU84	Falta de procedimientos para reportar debilidades en la seguridad	
VU85	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	
VU86	Falla de un dispositivo, componente y/o parte del equipo	
VU87	Ausencia de grupo electrógeno	
VU88	Exclusión en listas de distribución de documento de corte de energía eléctrica	
VU89	Falta de entrenamiento en sus operaciones diarias	
VU90	Falta de planificación y comunicación de las tareas/trabajos que afectan a la infraestructura tecnológica	
VU91	Testeo inadecuado / insuficiente	
VU92	Falta de procedimiento formal de asignación de privilegios administrativos	
VU93	Falta de procedimiento formal de actualización de parches y hotfixes	
VU94	Falta de contrato de mantenimiento y soporte del software para actualización de versiones	
VU95	Falta de entrenamiento en sus operaciones diarias (proveedor)	
VU96	Almacenamiento con condicionales ambientales no adecuadas	
VU97	Protección física inadecuada de ductos y montantes	
VU98	Falla del equipo del proveedor	
VU99	Incumplimiento de pago de servicio	
VU100	Ubicación en un área susceptible a movilizaciones	
VU101	Carencia del servicio de soporte de expertos en el producto para solucionar problemas	

9. CONTROL DE CAMBIOS

DETALLE	VERSIÓN	FECHA	RESPONSABLE
Versión Inicial del Documento	01		

Anexo D

Procedimientos Derechos ARCO

SOLICITE LA ATENCIÓN DE SUS DERECHOS ARCO

Porque nuestro compromiso en proteger sus datos personales es importante, le indicamos los pasos que deberá seguir para ejercer sus derechos PDP (Información, Acceso, Rectificación, Cancelación, Oposición y Revocatoria):

1. Descargue el formulario (Dé clic aquí) y complete todos los datos solicitados.
2. Firme el documento, escanéelo y envíelo a la cuenta de correo: derechosarco@uns.edu.pe **Importante:** Debe adjuntar copia simple de DNI / Carné de Extranjería o Pasaporte.
3. En caso desee entregar los documentos de manera presencial, podrá realizarlo en la siguiente dirección:
   - Av. Pacífico 508 - Nuevo Chimbote-Edificio de Rectorado de la UNS (Dirección de Asesoría Legal)
4. La respuesta a su solicitud se realizará dentro del plazo establecido por Ley.

A continuación el detalle de cada tipo de solicitud:

Tipo de Solicitud	Plazo Máximo de Respuesta (*)	Detalle
Información	8 días hábiles	Disponibilidad para ser informado sobre la finalidad del registro de sus datos personales en nuestros sistemas.
Acceso	20 días hábiles	Disponibilidad para obtener la información de sus datos personales registrados en nuestros sistemas.
Rectificación	10 días hábiles	Corrección de sus datos personales ya registrados en nuestros sistemas que resulten ser parcial o totalmente inexactos, incompletos, erróneos o falsos.
Cancelación	10 días hábiles	Supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados; hubiere vencido el plazo establecido para su tratamiento; se ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al reglamento.
Oposición	10 días hábiles	Toda persona tiene la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.
Revocatoria	5 días hábiles	Toda persona podrá negar o revocar su consentimiento al tratamiento de sus datos personales para finalidades adicionales a aquellas que dan lugar a su tratamiento autorizado, sin que ello afecte la relación que da lugar al consentimiento que sí ha otorgado o no ha revocado.

(*) Plazo establecido por Ley. Los días son contados desde el día siguiente a la presentación de la solicitud vía correo o de forma presencial.

Fecha de Presentación _____

N° Solicitud:

I. MOTIVO DE LA SOLICITUD (se deberá presentar una copia de la presente solicitud como cargo)
Marque con una "X" la casilla que corresponda al procedimiento que solicita:

Información (8 días hábiles)	☐	Acceso (10 días hábiles)	☐
Oposición (10 días hábiles) *	☐	Cancelación (10 días hábiles) **	☐
Impedimento de Suministro (10 días hábiles)	☐	Rectificación (10 días hábiles)	☐
Revocatoria (5 días hábiles)	☐		

(*) La oposición al tratamiento de sus datos personales que no sean parte de una relación contractual o servicios académicos contratados entre usted y la UNS.

(**) La cancelación no procederá cuando los datos personales deban ser conservados como parte de una relación contractual o para servicios académicos contratados entre usted y la UNS.

II. DATOS DEL SOLICITANTE

Solicitante _____ _____ _____
Nombres Apellido Paterno Apellido Materno

Tipo de Documento _____ N° de Documento _____

Domicilio _____

Distrito _____ Provincia _____

Departamento _____ Teléfono _____

Se debe adjuntar copia simple del documento de identidad que identifique al solicitante, así como los documentos sustentatorios necesarios para la aceptación de la solicitud, según sea el caso.

III. TIPO DE TITULAR DEL DATO PERSONAL (hacer referencia al vínculo entre usted y la UNS)

Cliente	Interesados, Postulantes Alumnos, Padres de Familia, Tutores y Responsables Económicos	Colaboradores, Docentes, entre otros	Proveedores y Terceros
☐	☐	☐	☐

IV. CÓMO SE ENTREGARÁ LA RESPUESTA (Marque con una X su elección)

☐ Correo Electrónico Personal _____

☐ Respuesta física:

Domicilio _____

Distrito _____ Provincia _____

Departamento _____ Teléfono _____

V. DETALLE DEL REQUERIMIENTO

1. **DERECHO DE OPOSICIÓN** (si el espacio no es suficiente, puede anexar hojas a esta solicitud)
   Especifique en forma clara y precisa la oposición al tratamiento de los datos personales (de ser necesario detallar los fines específicos):

   _____

   _____

   _____

   _____

2. **DERECHO DE CANCELACIÓN** (si el espacio no es suficiente, puede anexar hojas a esta solicitud)
   Especifique en forma clara y precisa los datos personales de los que solicita su cancelación:

   _____

   _____

   _____

   _____

3. **DERECHO DE RECTIFICACIÓN** (si el espacio no es suficiente, puede anexar hojas a esta solicitud)
   Indique a continuación aquellos datos que desea sean rectificados:

   Dato Incorrecto

   _____

   Dato Correcto

   _____

VI. REVOCACIÓN (Especifique en forma clara el tratamiento a sus datos personales que dese revocar)

Descripción _____

_____

LA UNS resolverá la solicitud de revocatoria en un plazo de 5 días hábiles desde la recepción de la presente solicitud.

Sin perjuicio de ello, la revocación efectuada no afectará el uso que la UNS pueda dar a sus datos personales, con la finalidad de ejecutar, desarrollar y/o cumplir su relación contractual o servicio académico contratado.

_____ _____

Firma de Solicitante Firma de Quien recibe la solicitud

Apellidos y Nombres : ..... **N° Solicitud:**

Documento de Identificación : .....
Tipo de Titular de DP : ..... Derecho Solicitado: .....

Recibido por : ..... Fecha (DD/MM/AA):____/____/_____

Anexo E

Acuerdo de privacidad del uso de datos personales

Acuerdo de privacidad de Protección de Datos Personales

Leer condiciones de tratamiento para mis datos personales

De conformidad con la Ley N° 29733 - Ley de Protección de Datos Personales y su Reglamento aprobado mediante D.S. 003-2013-JUS, el postulante otorga su consentimiento expreso para que los datos personales que facilite a la UNIVERSIDAD NACIONAL DEL SANTA, a través de este medio y/o cualquier otra vía queden incorporados en el Banco de Datos de Postulantes de Pregrado y Posgrado de la UNIVERSIDAD NACIONAL DEL SANTA y sean tratados por esta con la finalidad de evaluar su posible ingreso, absolver sus consultas y brindarles información publicitaria, dándoles usos que incluyen temas referidos a cumplimiento e incumplimiento de obligaciones económicas, análisis de perfiles, publicidad y prospección comercial, fines estadísticos, históricos o científicos, educación, así como seguridad y control de acceso a edificios. El postulante autoriza a que la UNIVERSIDAD NACIONAL DEL SANTA mantenga sus datos personales en el banco de datos referido en tanto sean útiles para la finalidad y usos antes mencionados. El usuario podrá ejercer su derecho de acceso, actualización, rectificación, inclusión, oposición y supresión o cancelación de datos personales descargando el formato solicitud de derechos ARCO desde la página web de la UNS (www.uns.edu.pe/arco) y enviándolo al correo electrónico derechosarco@uns.edu.pe o presentándolo físicamente a la Dirección de Asesoría Legal ubicada en la Av. Pacífico 508 - Nuevo Chimbote-Edificio de Rectorado de la UNS.

☐ **Acepto las condiciones para el tratamiento de mis datos personales.**

DNI del Postulante

Anexo F

Carta de Director de Admisión

UNS
UNIVERSIDAD NACIONAL DEL SANTA

CARTA DE ACEPTACIÓN DE CULMINACIÓN DE INVESTIGACIÓN PARA PROYECTO DE TESIS

A QUIEN CORRESPONDA

Yo Ms. Joel Herradda Villanueva, Director de la Dirección de Admisión de la Universidad Nacional del Santa – Nuevo Chimbote – Perú.

Dejo constancia que el Bach. Juan Carlos Guzman Comesaña, identificado con DNI: Nº 41929661, ha culminado exitosamente el Análisis, Diseño y Documentación del Proceso de Admisión de Estudiantes de Pregrado cabe precisar que este trabajo forma parte de su investigación intitulada "ELABORACIÓN DE UN MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2013 Y LEY DE PROTECCIÓN DE DATOS PERSONALES EN LA DIRECCIÓN DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL DEL SANTA ", el mencionado ha realizado reuniones de trabajo con mi persona, con el Coordinador Académico Ing. Manco Pulido y el Coordinador Administrativo Lic. Manuel Chiroque Farfán demostrando responsabilidad de una manera satisfactoria, desde el 01 de Mayo del 2017 hasta la fecha presente.

Realizando las siguientes tareas:

- Análisis de la Documentación Normativa de la Universidad y del Proceso de Admisión.
- Elaboración y entrega de formatos para el cumplimiento de la Ley de Protección de Datos Personales en la Dirección de Admisión.
- Análisis, Diseño, y Documentación del Proceso de Admisión de Estudiantes de Pregrado.

Además hago constar que ha demostrado actitud de superación, proactividad, iniciativa y responsabilidad.

Nuevo Chimbote, 05 de Diciembre del 2017

UNIVERSIDAD NACIONAL DEL SANTA
DIRECCIÓN DE ADMISIÓN
Chimbote - Perú

Ms. Joel Herradda Villanueva

Director de la Dirección de Admisión de la UNS

Anexo G

Formulario de Encuesta Web

Sección 1 de 6

Encuesta para Juicio de Expertos para validar Proyecto de Tesis

Tesis: Elaboración de un Marco de Referencia para la Implementación de la Norma ISO/IEC 27001:2013 y Ley De Protección de Datos Personales en la Dirección de Admisión de la Universidad Nacional del Santa

Título de la imagen

Autor: Juan Carlos Guzman Comesaña

Descripción (opcional)

Sección 2 de 6

I. Gestión por procesos BPMN 2.0

Descripción (opcional)

1.¿El Marco de Referencia cumple con el Estandar BPMN 2.0 para la gestión por procesos? *

- ○ Totalmente en desacuerdo
- ○ En desacuerdo
- ○ Ni de acuerdo ni en desacuerdo
- ○ De acuerdo
- ○ Totalmente de acuerdo

Sección 3 de 6

II. Banco de Datos Personales

Descripción (opcional)

2.¿El Marco de Referencia permite la identificación de los Bancos de Datos Personales acorde con la Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

Sección 4 de 6

III. Analisis de Brechas

Descripción (opcional)

3.¿El Marco de Referencia permite la identificación de brechas de cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

4.¿El Marco de Referencia permite la identificación de brechas de cumplimiento de los Controles de la Norma ISO/IEC 27002:2013? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

5.¿El Marco de Referencia permite integrar los Controles de la Norma ISO/IEC 27002:2013 y los de la Directiva de Seguridad de Protección de Datos Personales? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

Sección 5 de 6

IV. Gestión de Riesgos de Seguridad de la Información

Descripción (opcional)

6.¿El Marco de Referencia permite una adecuada identificación de activos de información mediante la Metodología de Riesgos de Seguridad de la Información propuesta? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

7.¿El Marco de Referencia permite una adecuada identificación , evaluación, tratamiento y seguimiento de los riesgos mediante la Metodología de Riesgos de Seguridad propuesta? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

Sección 6 de 6

V. Procedimientos para cumplir con la Ley de Protección de Datos Personales

Descripción (opcional)

8.¿El Marco de Referencia propone un acuerdo de privacidad, considera que cumple con lo estipulado por la Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

9.¿El Marco de Referencia propone un procedimiento para el ejercicio de derechos ARCO, considera que cumple con lo estipulado por la Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad? *

- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo