UNIVERSIDAD DE PIURA

REPOSITORIO INSTITUCIONAL PIRHUA

SISTEMA DE CONTROL BASADO EN COBIT PARA LA CERTIFICACIÓN SOX. CASO: AFP EN PERÚ

Carlos López-Sovero

Piura, agosto de 2015

Facultad de Ingeniería

Maestría en Dirección Estratégica en Tecnologías de la Información

López, C. (2015). *Sistema de Control basado en COBIT para la certificación SOX. Caso: AFP en Perú* (Tesis de máster en Dirección Estratégica de Tecnologías de la Información). Universidad de Piura. Facultad de Ingeniería. Piura, Perú.

Esta obra está bajo una licencia
Creative Commons Atribución-
NoComercial-SinDerivadas 2.5 Perú

Repositorio institucional PIRHUA – Universidad de Piura

U N I V E R S I D A D DE P I U R A

FACULTAD DE INGENIERÍA

Sistema de Control basado en COBIT para la Certificación SOX.

Caso: AFP en Perú.

Tesis para optar el Grado de Magister en Dirección Estratégica de Tecnologías de la Información.

Carlos Enrique López Sovero.

Asesor: Mgtr. Federico Wiesse López.

Piura, Agosto 2015

Dedico el presente trabajo a mis hijos y esposa por quitarles un poco de tiempo y por haberme apoyado en todo momento.

A mis padres, por todos los sacrificios realizados durante toda la vida que me ha permitido alcanzar mis metas.

Prólogo

Debido al crecimiento constante de las tecnologías de información en las distintas organizaciones, es necesario contar con un marco de gobierno de tecnologías de información que permita alcanzar una grado de madurez que conlleve a obtener certificaciones internacionales como en el presente trabajo de aplicar hacia una certificación Ley Sarbanes Oxley más conocido como SOX, con el sustento de herramientas como ITIL, Cobit e ISO 27001.

Resumen

El presente trabajo tiene como objetivo lograr la certificación internacional SOX, para lo cual se realizó en una primera etapa el levantamiento de información para identificar el escenario inicial, esta tarea se llevó a cabo mediante un cuestionario que permite identificar el grado de madurez en controles SOX.

El marco teórico que sirve de apoyo a la sustentación del presente trabajo se basa en las buenas prácticas de ITIL, Cobit e ISO 270001.

Identificados las brechas se realiza un mejoramiento de las políticas y procedimientos, un análisis de la estrategia de tecnología en la organización e identificación de los controles claves.

De la misma manera se observa el tema de gestión de niveles de servicio, configuración de servidores críticos, y finalmente se realiza una autoevaluación para poder mantener los controles en el tiempo.

Índice

Introducción 1
Capítulo 1 Aspectos Generales…… 3
1.1 Situación Actual 3
1.2 Formulación del problema. 5
1.3 Objetivos 7
Capítulo 2 Marco Teórico 9
2.1 Estado de Arte 9
2.2 Situación Actual de la AFP 10
2.3 ITIL Version 3. 12
2.4 ISO 27002. 13
2.5 COBIT. 13
2.6 Marco de Riesgo de TI. 13
Capítulo 3 Diseño Metodológico……. 17
3.1. Antecedentes de la Investigación. 17
3.2. Diseño de la investigación. 18
3.3. Estrategias de implementación. 19
Capítulo 4 Solución Propuesta 23
4.1 Definición de los Procesos de TI y Alineamiento de Estrategias. 23
4.1.1 Alineamiento de Estrategias 25
4.1.2 Procedimiento de Elaboración del Plan Estratégico 26
4.2 Mejoramiento de Procedimientos. 26
4.2.1 Administración de Accesos 26
4.2.2 Administración de Datos 27
4.2.3 Gestión de Control de Cambios 30
4.2.4 Desarrollo, Adquisición y Mantenimiento de Sistemas 31
4.2.5 Gestión de Incidentes de Seguridad 32
4.2.6 Gestión de Incidentes de TI 33
4.2.7 Gestión de Problemas 35
4.2.8 Gestión de Talento Humano 36
4.2.9 Gestión de Desempeño y de la Calidad 39
4.2.10 Marco de Trabajo de los Procesos de Tecnología 40
4.2.11 Monitoreo 42
4.2.12 Operaciones 43

4.2.13 Resiliencia y Seguridad Física. 47
4.2.14 Gestión de Seguridad en Plataforma 48
4.2.15 Gestión de Niveles de Servicio 49
4.2.16 Gestión de Mesa de Ayuda 51
4.2.17 Gestión de Catalogo de Servicio 52
4.2.18 Gestión de Proveedores de TI 53
4.2.19 Gestión de Configuración de Servidores Críticos 55
4.3 Relevamiento e Identificación de Controles Claves de TI 56
4.3.1 Relación de Controles por Aplicativo 56
4.3.2 Checklist de Seguridad de Proveedores Críticos 58
4.3.3 Checklist de Seguridad del Centro de Cómputo Principal y Alterno. 62
4.3.4 Documento de Roles y Responsabilidades 65
4.3.5 Plan de Mitigación de Riesgos 69
4.3.6 Relación de Controles Internos para Proveedores 93
4.3.7 Seguridad en Plataforma – Monitoreo 97
4.4 Implementación de Flujos y Controles. 99
Capítulo 5 Análisis de Resultados 107
5.1 Matriz de Resultados por Proceso y Control 107
5.2 Informe de Brechas Detectadas 119
5.3 Checklist de Autoevaluación 123
5.3.1 Criterio de Autoevaluación. 123
Capítulo 6 Conclusiones 135
Principales Problemas Identificados 135
Conclusiones 136
Bibliografía. 139
Anexos…… 141
Anexo A Matriz por Dominios de COBIT 143
Anexo B Administración de Accesos 149
Anexo C Administración de Datos 156
Anexo D Gestión de Control de Cambios 161
Anexo E Desarrollo, Adquisición y Mantenimiento de Sistemas 169
Anexo F Gestión de Incidentes de Seguridad 174
Anexo G Gestión de Incidentes de TI. 177
Anexo H Gestión de Problemas 179
Anexo I Gestión de Talento Humano 181
Anexo J Gestión de Desempeño y de la Calidad. 186
Anexo K Marco de Trabajo de los Procesos de Tecnología 187
Anexo L Monitoreo 189
Anexo M Operaciones 194
Anexo N Resilencia y Seguridad Física 214
Anexo N Gestión de Seguridad en Plataforma. 217
Anexo O Gestión de los Niveles de Servicio. 220

Anexo P Gestión de Mesa de Ayuda. 225
Anexo Q Gestión del Catálogo de Servicios. 226
Anexo R Gestión de la Configuración de Servidores Críticos. 227
Anexo S Definir un Plan Estratégico.....228

Índice de Figuras

Figura 1 Cadena de Valor…….. 4
Figura 2 Organigrama de TI…….. 5
Figura 3 Buenas Prácticas que permiten sostener SOX…… 6
Figura 4 Procesos de Tecnología de Información…… 6
Figura 5 Evolución de Cobit…….…….. 9
Figura 6 Modelo de Madurez……..…….. 12
Figura 7 Ciclo de Gestión de Riesgos de TI…..……..…….. 14
Figura 8 Clasificación del Activo…….. 15
Figura 9 Pilares de Cobit…….……..…… 18
Figura 10 Fases de Implementación…….……..... 19
Figura 11 Mapa de Procesos……..……. 24
Figura B1 Gestión de Accesos – Altas Cuentas de Usuarios……..... 150
Figura B2 Gestión de Accesos – Revisión de Accesos Anual/Trimestral..…..... 152
Figura B3 Gestión de Accesos – Revisión de Accesos Mensual…….…….…..... 153
Figura B4 Gestión de Accesos – Baja Cuenta de Usuario…….……..…….…..... 154
Figura B5 Gestión de Accesos – Acceso a Producción para Personal de Desarrollo…….…..... 155
Figura C1 Eliminación Segura……..... 157
Figura C2 Respaldo……..... 158
Figura C3 Restauración……..…….…..... 160
Figura D1 Cambio Normal……..……..….. 161
Figura D2 Cambio de Emergencia……..... 162
Figura D3 Adquisición de la Solución…….…….…… 163
Figura D4 Desarrollo de la Solución……..…….…… 164
Figura D5 Pruebas a la Solución…..……..……. 165
Figura D6 Pase a Producción……..……..……... 166
Figura D7 Monitoreo del Cambio…….…….…….. 167
Figura D8 Modelo de Gestión de Cambio……...……..……. 168
Figura F1 Gestión de Incidentes de Seguridad de la Información……..…… 174
Figura F2 Proceso de Monitoreo de Seguridad de la Información……. ……..……. 176
Figura G1 Gestión de Incidentes de TI…….…….…….. 177
Figura G2 Validación del Reporte de Mesa de Ayuda…….……..…….…….…… 178
Figura H1 Gestión de Problemas……..... 180
Figura I2 Capacitación de TI. ……...…….……. 181
Figura I3 Concientización de Riesgos Operativos…….…….…….. 182
Figura I4 Concientización de TI…….……. 183
Figura I5 Cambio de Puestos y Funciones …….……. ……..…….. 185
Figura J1 Monitoreo de Desempeño de los Servicios de TI……..……... 186
Figura K1 Gestión y Organización de Procesos de TI……..……..... 187

Figura K2 Validación de Roles de Tecnología……..……..... 188
Figura L1 Monitoreo de Seguridad e Infraestructura ……..……..... 189
Figura L2 Flujo de Hardening……..... 190
Figura L3 Código Seguro……..……. 191
Figura L4 Análisis de Vulnerabilidades……... 192
Figura L5 Ethical Hacking…….. 193
Figura M1 Ambientes Controlados para Pruebas…… …. 194
Figura M2 Actualización de Cronograma.…….. 195
Figura M3 Ejecución de Cronograma…… 196
Figura M4 Elaboración de Inventarios de Activos……..……..... 197
Figura M5 Actualización y Mantenimiento de Inventario de Activos.…..……. 198
Figura N1 Monitoreo de Controles Ambientales y Físicos en el Centro de Computo…… 214
Figura Ñ1 Antivirus……..……..…… 217
Figura Ñ2 Seguridad Perimetral…….. .. 218
Figura Ñ3 Parches de Seguridad……..… 219
Figura O1 Gestión de Niveles de Servicio……..…. 220
Figura O2 Actualización de Niveles de Servicio……..... 221
Figura O3 Implementación del Servicio ……. 222
Figura O4 Niveles de Servicio del Portafolio – Revisión Anual……... 223
Figura O5 Monitoreo de Niveles de Servicio……..... 224
Figura P1 Mesa de Ayuda y Servicio de Campo ……..…….. 225
Figura Q1 Gestión de Niveles de Servicio – Definición -Actualización de Servicio……..... 226
Figura R1 Identificación y mantenimiento de Elementos Configurables……..…. 227
Figura S1 Metodología de Elaboración del PETI…….…. .. 229
Figura S2 Elaboración y Seguimiento del Plan Estratégico de Tecnologías de Información.… 232

Índice de Tablas

Tabla 1 Situación Actual de la AFP…… 11
Tabla 2 Alineamiento Estrategias…… 25
Tabla 3 Clasificación Formal de los Desarrollos……..... 32
Tabla 4 Gestión de Proveedores de TI……. 54
Tabla 5 Aplicaciones a Evaluar ……..... 56
Tabla 6 Criterios del Checklist. …….……..... 57
Tabla 7 Resumen de la Evaluación... ……..… 58
Tabla 8 Checklist de Seguridad de Proveedores Críticos……..... 58
Tabla 9 Zona de Dominio Técnico para Evaluaciones Adquisiciones de TI…..……..….. 59
Tabla 10 Resumen Dominio Técnico…….…….…. 60
Tabla 11 Parámetros de Evaluación Empresa…….…… 60
Tabla 12 Parámetros de Evaluación de Propuestas…….…… 61
Tabla 13 Parámetros de Evaluación de Técnica……. 61
Tabla 14 Parámetros de Evaluación de Técnica HW, SW, Red…….. 61
Tabla 15 Parámetros de Evaluación de Técnica Grupal…….…… 62
Tabla 16 Checklist de Seguridad del Centro de Cómputo Principal y Alterno…….... 62
Tabla 17 Consideraciones de Roles y Responsabilidades……..... 65
Tabla 18 Descripción de los Niveles……..... 66
Tabla 19 Criterios…….…….. 67
Tabla 20 Segregación de Funciones ……..... 68
Tabla 21 Plan de Mitigación de Riesgos – Organización de TI……..... 69
Tabla 22 Plan de Mitigación de Riesgos – Ciclo de Vida del Software...…….. 80
Tabla 23 Plan de Mitigación de Riesgos – Infraestructura Tecnológica……..... 81
Tabla 24 Riesgos de TI cuyos Controles Necesitan Revisión de Terceros…… 93
Tabla 25 Servidores Evaluados ……. 97
Tabla 26 Criterios Cumplimiento…… 97
Tabla 27 Relación de Procesos vs. Controles……. 99
Tabla 28 Resultados por Procesos y Control ……..…… 107
Tabla 29 Ejemplo de Brechas Detectadas...……..…… 121
Tabla 30 Criterios de Autoevaluación……..…… 123
Tabla 31 Checklist de Proceso- Riesgo Asociado……. 125
Tabla 32 Evaluación de Procesos..... 129
Tabla 33 Resumen Auto-evaluación …… 131
Tabla 34 Cronograma de Revisión de Procedimientos……. 133
Tabla A1 Matriz de Dominios de COBIT – Organización de TI……... 143
Tabla A2 Matriz de Dominios de COBIT – Ciclo de Vida de Software…. 145
Tabla A3 Matriz de Dominios de COBIT – Infraestructura Tecnológica……. 146

Tabla C1 Autorización de Uso de Medios 156
Tabla C2 Eliminación Segura de Información..... 158
Tabla E1 Clasificación de Desarrollos..... 169
Tabla E2 Descripción de los Artefactos..... 169
Tabla E3 Tipos de Casos de Prueba..... 170
Tabla E4 Cumplimiento de los Artefactos..... 171
Tabla E5 Verificación de los Artefactos..... 171
Tabla E6 Indicadores de las Revisiones..... 173
Tabla F1 Bitácora de Incidentes de Seguridad de la Información..... 175
Tabla H1 Matriz de Urgencia vs. Impacto..... 179
Tabla H2 Tiempo de Respuesta Según Prioridad..... 179
Tabla I1 Matriz de Técnicas de Concientización de Seguridad de Información..... 184
Tabla I2 Matriz de Técnicas de Concientización de Tecnologías de Información..... 184
Tabla M1 Confidencialidad..... 200
Tabla M2 Integridad..... 202
Tabla M3 Disponibilidad..... 204
Tabla M4 Matriz de Inventario de Activos de TI..... 208
Tabla M5 Formato de Inventario de Servidores Físicos y Virtuales..... 209
Tabla M6 Formato de Inventario de Aplicativos..... 209
Tabla M7 Formato de Inventario de Equipos de Comunicación..... 210
Tabla M8 Formato de Inventarios de Equipos de Seguridad..... 210
Tabla M9 Formato de Inventario de Servicios Genéricos..... 211
Tabla M10 Formato de Inventario de Conexiones Externas..... 212
Tabla M11 Criterios para la Definición de los Niveles de Criticidad de los Activos de TI..... 213
Tabla N1 Control de Acceso al Centro de Cómputo..... 216

Introducción

El alineamiento del área de tecnologías de información hacia los objetivos del negocio, es cada vez más común encontrarlo en las diferentes organizaciones, lo cual demuestra un alto grado de madurez del área de TI soportando procesos críticos de negocio.

El presente trabajo busca cubrir la carencia de encontrar una metodología práctica para la certificación SOX, no muy común en nuestro país debido a que no todas las instituciones necesitan cotizar en la bolsa de Nueva York., sin embargo las buenas prácticas, estándares y marcos de trabajo nos hace alinearnos a esta tendencia.

Podemos considerar tres pilares fundamentales para la implementación de SOX: Cobit, ISO27002 e ITIL, cada una de ellas aportando componentes que se convertirán en controles a evidenciar en lo largo del proceso.

Las fases de implementación usadas las podemos dividir en cuatro, iniciando con una identificación de los procesos de TI y alineamiento de estrategias, en este punto podemos definir tres macro procesos: organización de tecnologías de información, gestión de riesgos tecnológicos y gestión de tecnología. Luego tenemos el mejoramiento de procedimientos actuales o creación de nuevos en caso de no existir, posteriormente identificando los controles claves los cuales nos permitirán generar evidencias SOX y finalmente desarrollando flujos e identificando controles dentro de los mismos, que al igual que los controles claves permitirán la generación de evidencias.

Capítulo 1
Aspectos Generales

1.1 Situación Actual

El presente trabajo hace referencia a una empresa Administradora de Pensiones, que es parte del Sistema de Privado de Pensiones en el Perú (SPP) dicho sistema fue creado en el año 1993 bajo la ley 25897.

Visión

"Ser reconocidos en el Perú como el mejor aliado en la construcción del futuro financiero de nuestros clientes a través del ahorro mandatorio y voluntario"

Misión

"En AFP trabajamos para ofrecer a nuestros clientes productos y servicios innovadores que respondan a sus necesidades, apoyándolos en la construcción de su futuro financiero a lo largo de ciclo de vida"

Cadena de Valor

El siguiente cuadro muestra las principales actividades de la organización mediante la cadena de valor.

El mapa mostrado a continuación posee cuatro componentes principales:

- Procesos del negocio, constituyen la parte central del gráfico.
- Proveedores, graficados al lado izquierdo y que son los que suministran los insumos necesarios a la para que realicen sus actividades.
- Clientes, colocados en la parte derecha del gráfico.
- Entidades externas, que se ubican en la parte superior del gráfico y lo conforman todos aquellos organismos e instituciones externas con las que interactúa la AFP.

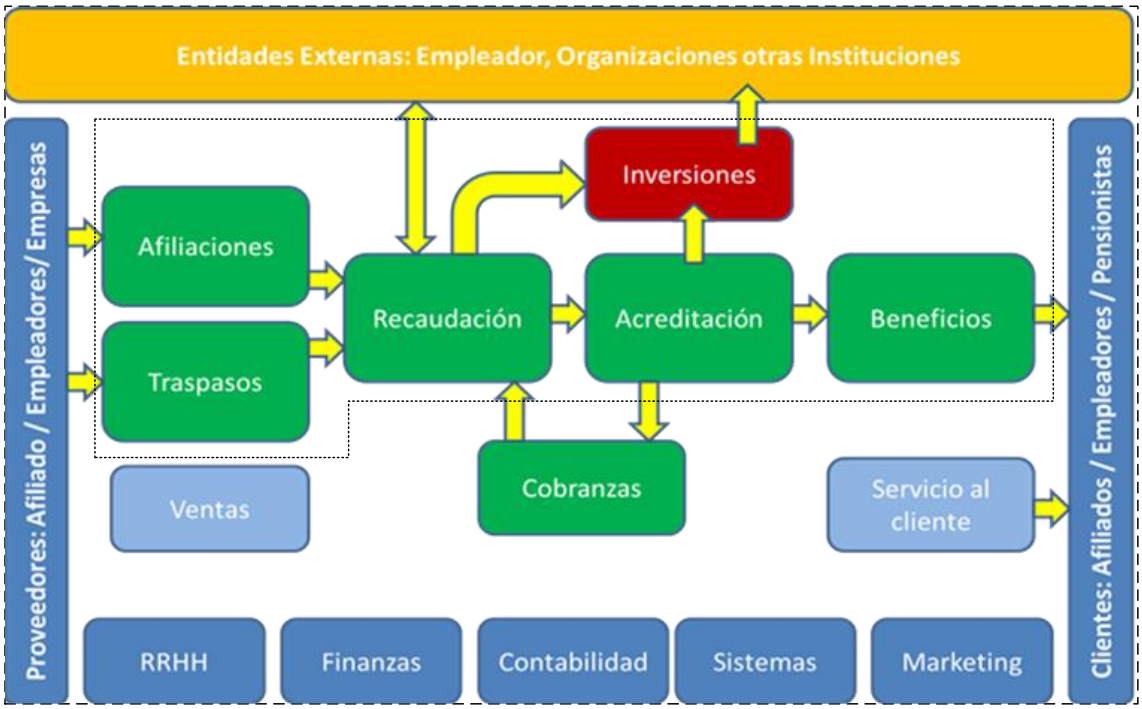


Fig. 1 Cadena de Valor
Fuente: Elaboración propia

Respecto a los procesos del negocio, estos se componen de:

- **Procesos "core":** Se encuentran encerrados mediante una línea punteada en el gráfico y constituyen la cadena de valor de la AFP, es decir, son los responsables de transformar los insumos en los productos que el cliente necesita.

- **Procesos de soporte al "core":** Aquellos que apoyan o dan soporte a los procesos "core" directamente y que en el gráfico se identifican mediante las flechas que las muestran en interacción con dichos procesos.

- **Proceso de servicio al cliente:** Aquellos procesos que interactúan directamente con el cliente, es decir, que sólo se realizan cuando el cliente tiene una interacción con él.

  En el gráfico se muestra como un recuadro independiente con una flecha que muestra su interacción con el cliente

  Es necesario aclarar que algunos de los procesos "core" tienen relación con el cliente, pero por ser ya parte del "core", no estarían comprendidos como procesos de servicio.

- **Procesos de soporte:** Todos aquellos procesos que brindan servicio o apoyo a los demás y que se identifican como recuadros horizontales en la parte inferior central del gráfico.

  El ordenamiento gráfico de los procesos del negocio permite observar cómo la AFP interactúa con sus proveedores para brindar sus servicios al cliente, cuáles procesos

son los que se encargan de la transformación de estos insumos, de qué manera se relacionan con el cliente y qué procesos dan el soporte a los mismos, además de indicar un alto grado de interacción con entidades externas, principalmente organismos gubernamentales como la ONP, SBS y las diferentes empresas – denominadas Empleadores - que proveen del insumo básico a la AFP que son los empleados.

Es necesario indicar que existen otros procesos como legal, auditoria, riesgos entre otros, que no han sido colocados en el mapa ya que no formarían parte de los procesos críticos.

Organigrama del Área de Tecnología

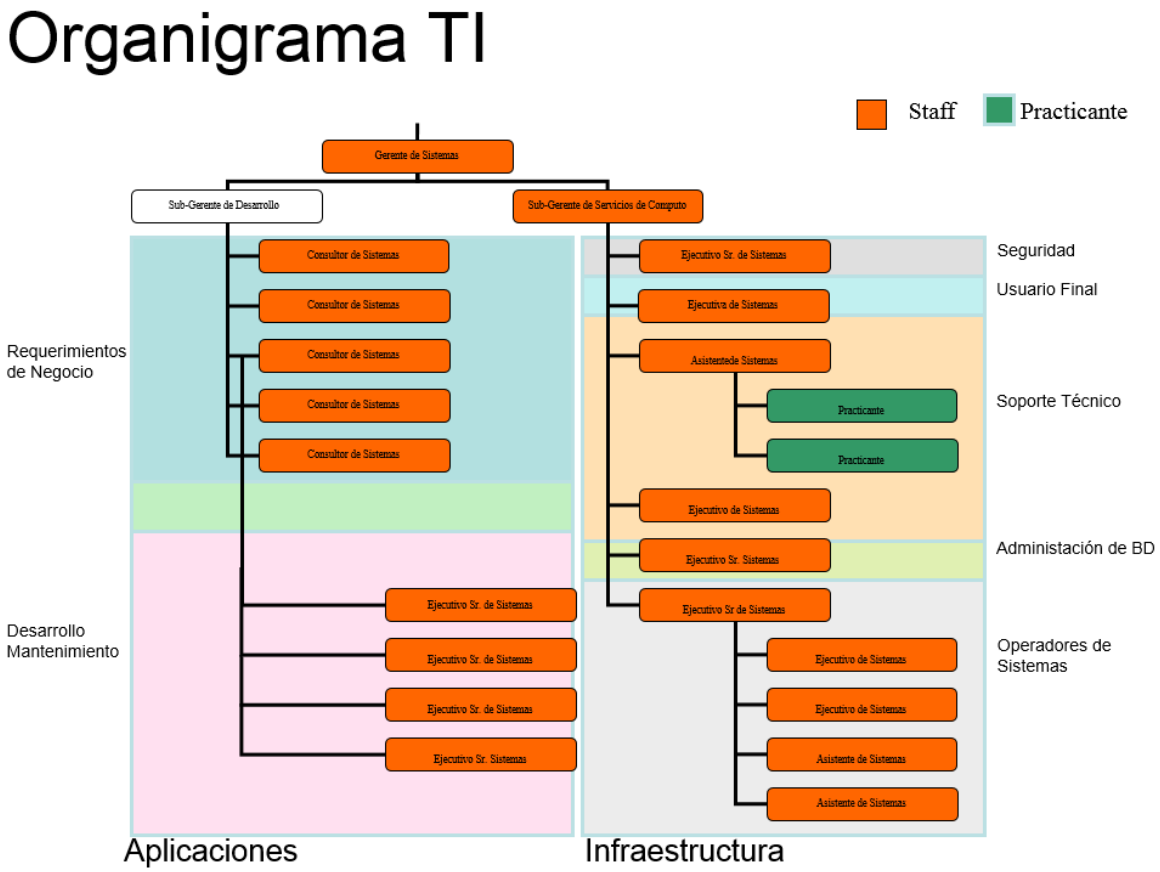


Fig. 2 Organigrama TI.
Fuente: Elaboración propia

1.2 Formulación del problema.

Identificación del Problema

La elevada competencia que se origina en el sistema privado de pensiones luego de 20 años de ser creadas hace que las AFPs busquen nuevas formas de invertir para alcanzar una mayor rentabilidad. Una de estas opciones es invertir en la Bolsa de Valores de Nueva York (NYSE New York Stock Exchange).

Para poder invertir en NYSE es necesario aplicar a la certificación SOX que no sólo hace mención a temas financieros sino también a temas tecnológicos, para nuestro caso expondremos el tema desde el punto de vista de tecnología para lo cual se necesita alcanzar un grado de madurez adecuado en el gobierno de tecnologías de información.

Descripción del Problema

Debido a la aplicación de la certificación SOX, los procesos actuales de tecnología no cubren el nivel de madurez adecuado en el gobierno de tecnologías de información, motivo por el cual es necesario la implementación de controles utilizando las buenas prácticas del ISO 27002, COBIT (Control Objectives for Information and Related Technology - Objetivos de Control para Información y Tecnologías Relacionadas) e ITIL.

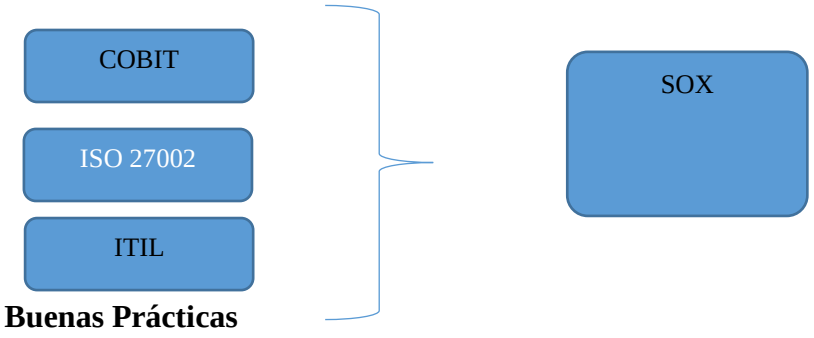


Fig. 3 Buenas prácticas que permite sostener SOX
Fuente: Elaboración propia

Planteamiento del Problema

Los procesos actuales definidos en el área de tecnología que se muestran a continuación, no cubren todos los procesos requeridos de acuerdo a SOX, otro punto a tratar es la implementación de nuevos controles que por su naturaleza de implementación pueden ocasionar inadecuadas segregación de funciones en el área de tecnología es también un obstáculo para la implementación de SOX en la organización.

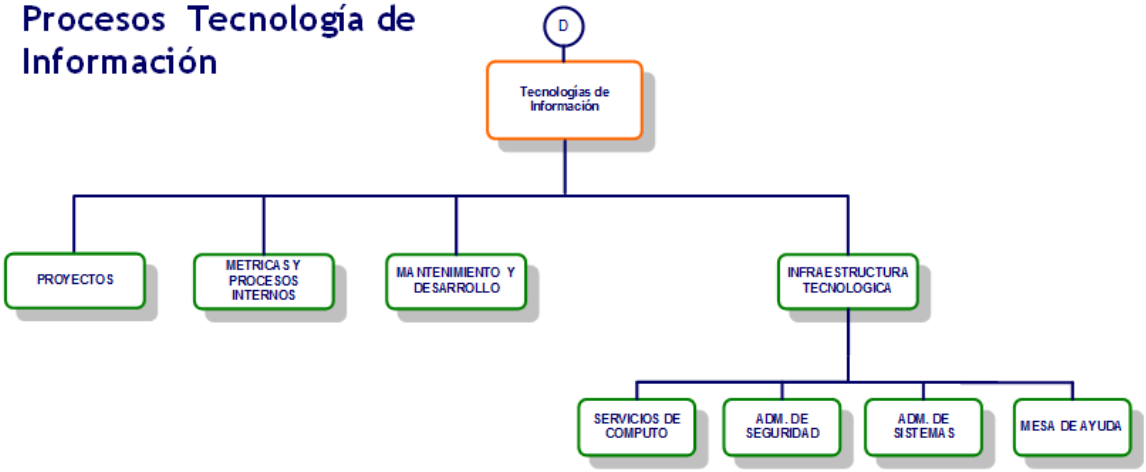


Fig. 4 Procesos Tecnología de Información.
Fuente: Elaboración propia

1.3 Objetivos

1.3.1 **Objetivos generales.**

- Mostrar madurez en el Gobierno Corporativo.
- Mejorar las conductas y comportamientos éticos.
- Mayores exigencias en la gestión de información confidencial.

1.3.2 **Objetivos específicos.**

- Tener un marco de referencia para la administración de controles.
- Identificación de procesos de tecnología.
- Elevar el nivel de madurez de los controles basados en “Control Objectives for Information and Related Technology” (COBIT).

Capítulo 2
Marco Teórico

El presente capítulo toma el modelo de gobierno de COBIT y mediante uso de cuestionarios realiza una revisión del modelo de madurez actual en la que se encuentra la AFP, considerando los tres principales pilares:

- Organización de TI.
- Ciclo de Vida del Software.
- Infraestructura Tecnológica.

De esta manera podemos identificar las brechas a trabajar utilizando el marco de gobierno de Cobit, acompañado de las buenas prácticas de ITIL (*Information Technology Infraestructure Library*), ISO 27002 (*International Organization for Standardization*) y el marco de riesgos de TI.

2.1 Estado de Arte

El gobierno de TI actualmente es la base para que las áreas de tecnología se encuentren alineadas al negocio y no sea considerado como un área más dentro de las organizaciones.

La evolución de COBIT se muestra a continuación:

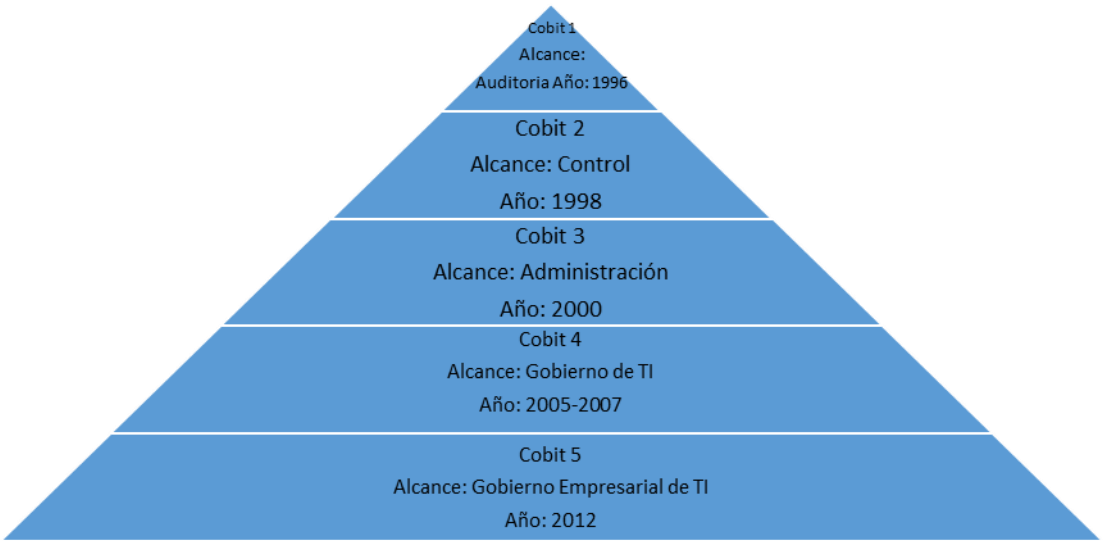


Fig. 5 Evolución de Cobit. Fuente: ISACA.

Realizando una comparación de los diversos trabajos realizados en la AFP, podemos mencionar que se practican tres auditorías al área de tecnología una realizada por el ente supervisor SBS “Superintendencia de Banca y Seguro”, otra auditoria interna realizada por el área de control interno – Auditoria y otra externa realizada por E&Y “Ernest and Young”, en todos los casos los alcances llegan a cubrir COBIT 1, 2 y 3.

Las tareas realizadas en estos tipos de auditoria alcanzan muchos controles basados en ITIL, ISO 27002/27001 y en la propia gestión de riesgos. Cabe mencionar que en todos los casos los resultados de los informes de auditorías tienen como calificación “Satisfactorio”.

Sin embargo estas auditorías no alcanzan a cubrir el gobierno de TI, que es lo que busca COBIT y es el motivo del presente trabajo.

En el marco nacional tenemos entre las principales organizaciones que cumplen con requerimientos SOX basados en COBIT a:

- Graña y Montero.
- BBVA.
- Telefónica.
- Banco de Crédito.

Todas ellas son empresas certificadas en SOX y tienen la posibilidad de interrelacionarse con la Bolsa de Valores de Nueva York.

Por otro lado ISACA (*Information Systems Audit and Control Association*), realizó una encuesta en los últimos 12 meses, la cual tiene como resultado:

- 48 % de las empresas que respondieron experimentaron sobrecostos en proyectos
- 41 % tuvo un costo alto de TI con un retorno de la inversión bajo o desconocido
- 38 % dijo que había una desconexión entre las estrategias de la empresa y de TI
- 22 % experimentó una falla de seguridad
- 21 % reportó desafíos relacionados con la seguridad de los dispositivos móviles.

Como podemos apreciar COBIT, ITIL, ISO 27001/270002 cubren esas brechas presentadas, por consiguiente conseguir un marco de referencia de buen gobierno de TI no excluye a otros marcos sino es la combinación de ellas, el nivel de grado de madurez auditado es un punto importante a mencionar debido a que a una organización que no ha tenido auditorias previas de este nivel es imposible solicitarle un nivel de madurez alto para un control debido a que la relación costo/beneficio de dicho control no será factible su implementación.

2.2 Situación Actual de la AFP

De acuerdo a la información recopilada en las tablas 21 - 22 – 23, podemos identificar las siguientes brechas de acuerdo al dominio de COBIT:

Tabla 1 Situación Actual de la AFP.

Dominios COBIT	Valor de Madurez Esperado	Avance
Organización de TI		
PO1 Definir un Plan Estratégico de TI	3	57.14%
PO4 Definir los Procesos, Organización y Relaciones de TI	3	44.44%
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	3	66.67%
PO7 Administrar los Recursos Humanos de TI	2	25.00%
PO9 Evaluar y Administrar los Riesgos de TI	3	7.14%
AI6 Administrar los cambios	4	5.56%
ME1 Monitorear y Evaluar el Desempeño de TI	2	12.50%
ME2 Monitorear y Evaluar el Control Interno	3	42.86%
ME3 Garantizar el Cumplimiento con Requerimientos Externos	3	0.00%
ME4 Proporcionar Gobierno de TI	3	57.26%
Ciclo de Vida del Software		
PO8 Administrar la Calidad	2	100.00%
Infraestructura Tecnológica		
AI3 Adquirir y Mantener Infraestructura Tecnológica	3	0.00%
AI4 Facilitar la Operación y el Uso	2	0.00%
AI7 Instalar y Acreditar Soluciones y Cambios	3	0.00%
DS1 Definir y Administrar los Niveles de Servicio	3	50.00%
DS2 Administrar los servicios de terceros	3	8.33%
DS5 Garantizar la Seguridad de los Sistemas	4	16.67%
DS8 Administrar la Mesa de Servicio y los Incidentes	3	35.71%
DS9 Administrar la Configuración	3	60.00%
DS10 Administración de Problemas	3	25.00%
DS11 Administración de Datos	3	28.57%
DS12 Administración del Ambiente Físico	3	0.00%
DS13 Administración de Operaciones	3	12.50%

Fuente: Elaboración propia.

Nomenclatura:

PO: Planear y Organizar.
AI: Adquirir e Implementar.
ME: Monitorear y Evaluar.
DS: “Delivery and Support” - Entregar y dar Soporte.

En el anexo A “Matriz por Dominios de Cobit”, podemos observar las matrices de acuerdo a los tres dominios de Cobit: Organización de TI, Ciclo de Vida de Software e Infraestructura Tecnológica.

Estas matrices permitirán tener una visibilidad a nivel de requerimientos de control y cumplimiento del mismo, la cual facilitará la evaluación en el momento de la certificación, incluye las siguientes partes:

- Requerimiento del Control.
- Soporte Documental de los controles implementados.
- Control- descripción.
- Tipo de Control.
- Naturaleza del Control.
- Frecuencia.
- Evidencia – Medio de Retención.
- Responsable – área responsable del control.
- Riesgos mitigados.

Modelo de Madurez

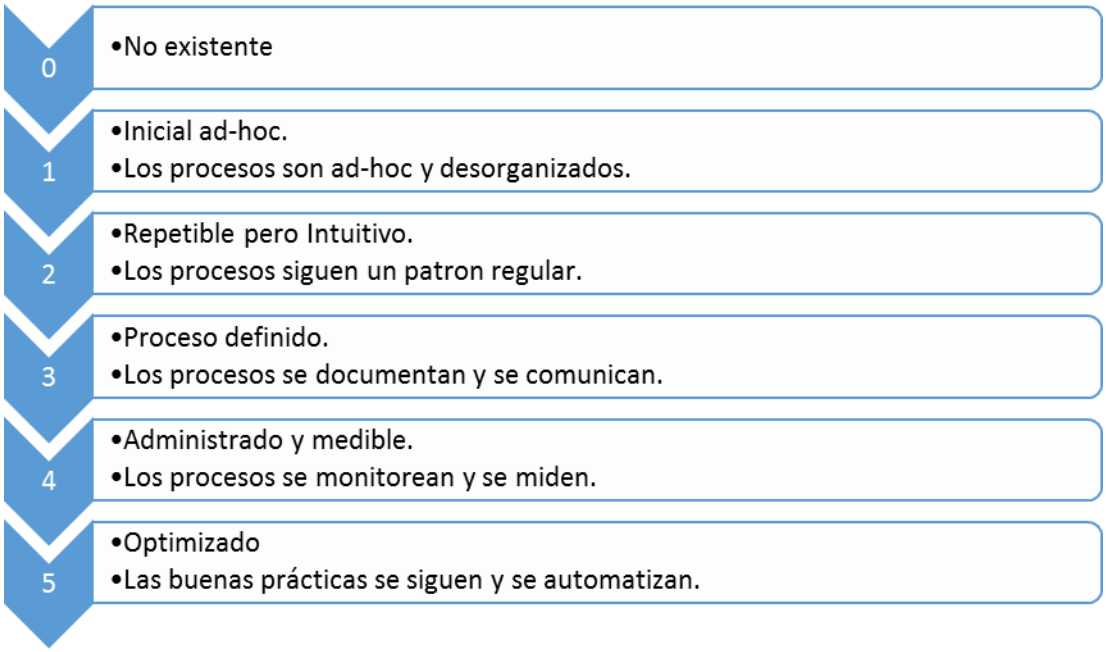


Fig. 6 Modelo de Madurez
Fuente: ITIL

2.3 ITIL Version 3.

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL, Information Technology Infraestructure Library) proporciona un planeamiento sistemático para la provisión de servicios de TI con calidad.

ITIL[1] fue desarrollado en la décadas de los 80 y 90 por la CCTA (Central Computer and Telecomunications Agency, ahora Office of Government Commerce, OGC), bajo contrato

[1] Título: Gestión de Servicios de TI basado en ITIL V3.
ISBN: 978 90 87531065 Autores: Jan van Bon, Arjem de Long, Axel Kolthof, Mike Pieper, Ruby Tjassing, Annelies van der Veen, Tineke Verheijem Copyright: @Van Haren Publishing

directo del Gobierno Británico. Desde entonces, ITIL ha demostrado ser no sólo un marco basado en mejores prácticas, sino también un planteamiento y una filosofía compartidos por la personas que los utilizan en la práctica. ITIL ha sido actualizado en dos ocasiones: la primera en 2000-2002 (v2) y la segunda en 2008 (v3).

2.4 ISO 27002.

Originalmente viene del ISO 17799, consiste en la guía de buenas prácticas que toda organización debe seguir referente a la seguridad de información.

Cubre lo siguiente:

- Políticas de Seguridad
- Organización de la Seguridad de la Información.
- Seguridad en los Recursos Humanos.
- Administración de Activos.
- Control de Activos.
- Seguridad Física
- Seguridad en las Operaciones.
- Seguridad en la Comunicaciones.
- Sistemas de Información, Adquisición, Desarrollo y Mantenimiento.
- Relaciones con Proveedores.
- Administración de Incidentes de Seguridad.
- Aspectos de Seguridad de Información en Continuidad de Negocios.
- Cumplimiento Normativo

2.5 COBIT.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®[2]) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

2.6 Marco de Riesgo de TI.

La evaluación de riesgos es una parte importante de la administración de riesgos informáticos. Esta práctica da lugar a la toma de conciencia de los aspectos de seguridad, proporciona un método para entender estos aspectos y apoya la implementación de salvaguardas para la protección contra incidentes de seguridad.

Esta norma aborda dos formas de evaluación de riesgos:

- **La Autoevaluación de Riesgos y Control (R&CSA[3] – Risk Control and Self Assesment)**, proporciona un medio para identificar un nivel aceptable (controlado) de riesgo y lograr un nivel mínimo de riesgos no identificados. Esta evaluación la realiza el

[2] Autor: IT Governance Institute COBIT 4.1

[3] R&CSA - ISACA Web: http://www.isaca.org/Journal/Past-Issues/2001/Volume-1/Pages/Risk-and-Control-Self-Assessment-RCSA-.aspx

negocio en sí. Por lo menos el 90% de evaluaciones de riesgos en AFP deben realizarse mediante el sistema R&CSA.

- **La Evaluación de Riesgos Técnicos**, se aplica a proyectos muy grandes y problemas complejos que deben ser cubiertos por un grupo de trabajo de analistas de riesgos.

El ciclo de gestión de riesgos lo podemos identificar mediante IMC "Identificar- Medir y Controlar" de acuerdo a la siguiente figura:

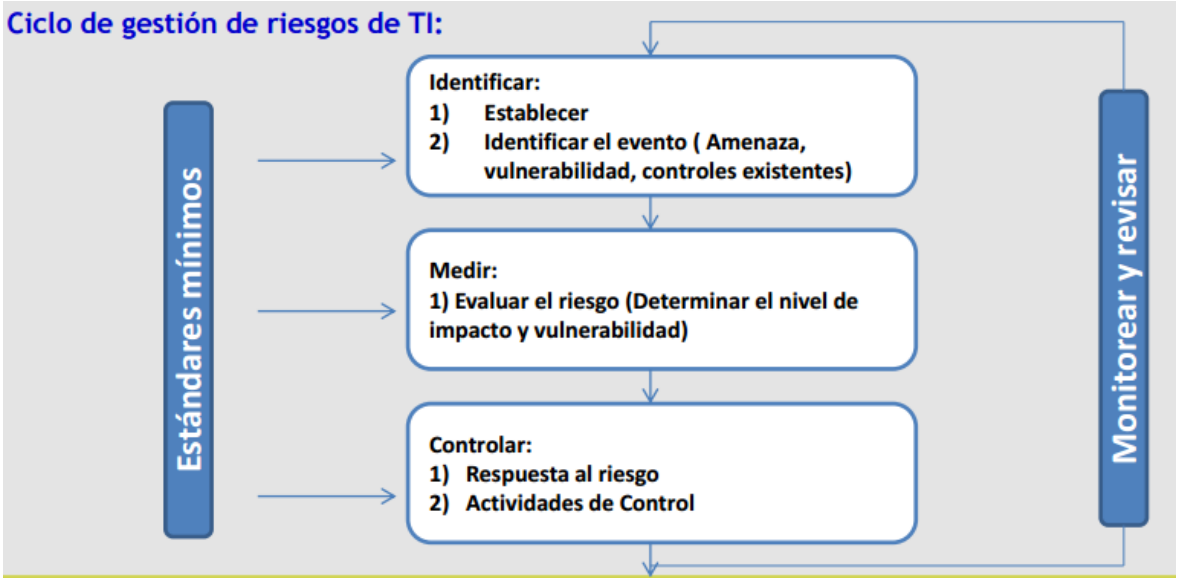


Fig. 7 Ciclo de Gestión de Riesgos de TI.
Fuente: ISACA.

Las evaluaciones de riesgo se realizan de acuerdo a la Confidencialidad, Integridad y Disponibilidad y la criticidad se obtendrá de acuerdo a la criticidad.

Fig. 8 Clasificación del Activo
Fuente: ISACA

Análisis de Riesgo

Se realiza por cada activo de información utilizando la siguiente matriz.

Activo de Información	ANÁLISIS DE RIESGOS			PLAN DE ACCIÓN	
	Riesgo	Nivel de Riesgo	Recomendación	Plan de Acción	Fecha

Monitoreo

Los puntos de control identificados a nivel de los procedimientos serán revisados por el Área de Riesgos, para asegurar el cumplimiento del marco de control interno y detectar desviaciones a tiempo para su atención.

El monitoreo se realizará:

- **Mensual**: Reunión de seguimiento con el equipo de TI.
- **Trimestral**: Desarrollo del Informe de Riesgos de Información y Continuidad de negocio en evaluación del nivel de cumplimiento de controles de TI.
- **Anual**: Revisión integral del marco de control interno de TI (Procedimientos / Controles) - Cálculo del riesgo residual.

Capítulo 3
Diseño Metodológico

3.1. **Antecedentes de la Investigación.**

En los últimos años las áreas de tecnología de información han tenido que transformarse para poder alinearse a los objetivos de la organización, de esta manera son parte ahora de la estrategia de la organización y en muchos casos no son considerados como un centro de gastos sino todo lo contrario son consideradas como un centro de inversión, la cual busca ser rentable para la organización. En muchas organizaciones implantar un sistema de Gobierno de Tecnología de Información que se encuentre balanceado con el Gobierno Corporativo no es tarea sencilla, debido a que las áreas de tecnología tienen que hacer frente el día a día de las operaciones, requerimientos regulatorios, auditorias y nuevos requerimientos del negocio, ocasionando de esta manera que esta última se convierta en un área de soluciones de problemas puntuales no planificados.

A nivel nacional existe poca información sobre su aplicación, debido a que no todas las empresas necesitan aplicar a SOX, el alcance es sólo para aquellas organizaciones que deseen cotizar en la Bolsa de Valores de Nueva York (NYSE).

Sin embargo, tenemos algunos "Marcos de Trabajo"[4] que ayudan en parte a la implantación de controles como:

- ISACA (*Information Systems Audit and Control Association*).
- ITGI (*IT Governance Institute).*
- ITSMF (IT Service Management Forum).
- ECGI (European Corporate Governance Institute).
- IT GOVUK (IT Governance UK).

También tenemos organizaciones reguladoras de estándares como:

- ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*)
- BSI (*The British Standards Institution*).

Los aportes de las entidades reguladoras, que vienen emitiendo reportes de absoluto interés y vigencia como son:

---

[4] Revista S&T, 9(17), 23-53. Cali: Universidad Icesi., Gonzalo Ulloa Villegas. Ph.D Decano de la Facultad de Ingeniería

- El Informe Coso –*Internal Control - Integrated Framework*– (Committee on Sponsoring Organizations of the Treadway Commission [COSO], 1992)
- El Informe Cadbury –*Report of the Committee on the Financial Aspects of Corporate Governance*– (Cadbury, 1992).
- El Código Olivencia de Buen Gobierno –*El Gobierno de las Sociedades Cotizadas*– (Olivencia, 1998);
- El Informe Turnbull –*Report of the Committee on the Financial Aspects of Corporate Governance*– (The Financial Reporting Council [FRC], 2005)
- El Informe Winter –*Report of the High Level Group of Company Experts on a Modern Regulatory Framework for Company Law in Europe*– (Winter, 2002)
- El Informe Aldama –*Informe de la Comisión Especial para el fomento de la transparencia y seguridad en los mercados y en las sociedades cotizadas*– (Aldama y Miñon, 2003).
- *El Company Law and Corporate Governance* (European Commission, 2011).
- *Principios de la OCDE para el Gobierno de las sociedades* (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 1999)
- *Enhancing Corporate Governance in Banking Organizations del Bank for International Settlements* (Basel Committee on banking supervision, 2005 &2006) cuyos reportes han tenido origen, entre otros, por los escándalos de Enron (Bryce, 2002; McLean & Elkind, 2005) y Worldcom (Jeter, 2003) donde en últimas se han producido fraudes en la información que presentan las corporaciones, a los accionistas y al mundo, aprovechando la falta de control en las tecnologías de información.

El presente trabajo de investigación se utilizó el marco de trabajo Cobit ("Control Objectives for Information Systems and related Technology") Objetivos de Control para la información y tecnologías relacionadas de ISACA.

Debido a que este marco de trabajo tiene cuatro pilares.

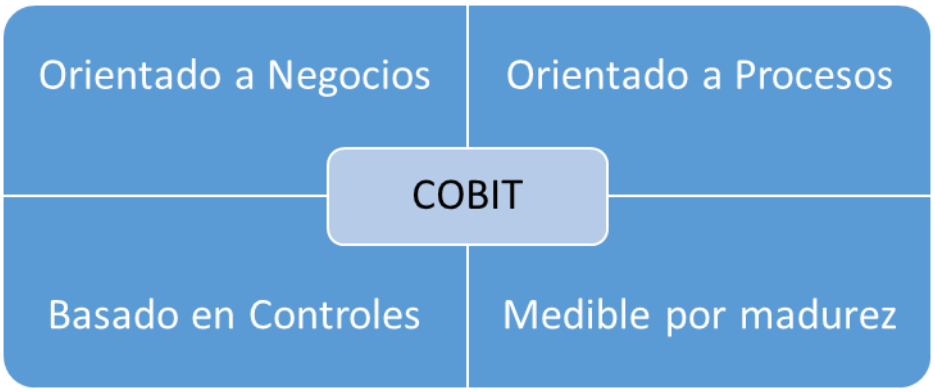


Fig. 9 Pilares de COBIT.
Fuente: Cobit 4.1

3.2. **Diseño de la investigación.**

La fuente de información del presente trabajo se realizó mediante el método del Test al área de tecnología considerando la participación de los líderes de área, cabe mencionar que el test no tiene calificación como tal lo que busca es detectar la situación actual de gobierno de TI.

Las preguntas se basan de acuerdo al marco teórico descrito en el Capítulo 2, utilizando las buenas prácticas de ITIL, ISO 27002, COBIT y el Marco de Riesgo de Tecnología.

La presente investigación se basa en métodos analíticos – sintéticos, va desde la descomposición de los procesos TI para la aplicación de controles y visto como un todo para poder alcanzar el grado de madurez adecuado para lograr la certificación SOX, para identificar el test, consultar el Anexo A.

3.3. **Estrategias de implementación.**

La estrategia de implementación se basa en 4 fases, que toma como línea base los resultados obtenidos en la Tabla 1 Situación Actual de la AFP con respecto al grado de madurez solicitado:

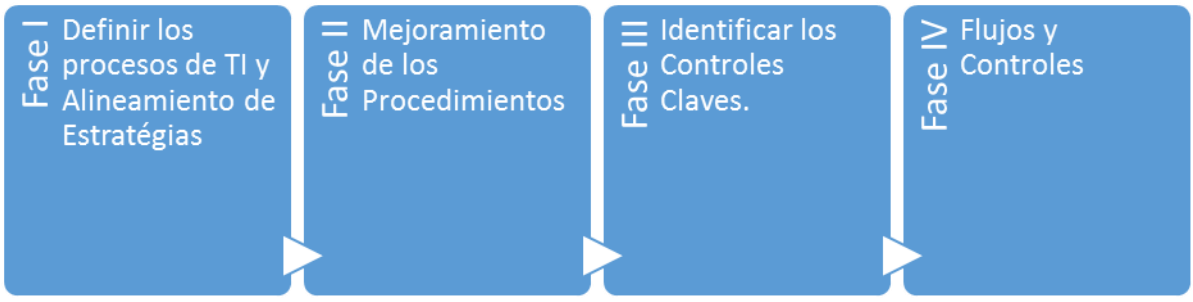


Fig. 10 Fases de Implementación
Fuente: Elaboración propia

Fase I: Definir los procesos de TI, que permitan soportar los nuevos controles a implementar, la estructura actual no hace factible la alineación del área de TI a los requerimientos de la organización. Se deben identificar los procesos que trabajen en conjunto de forma eficaz y eficiente, para esto se agrupan los procesos en:

- Organización de Tecnologías de Información.
- Procesos de Gestión de Riesgos Tecnológicos.
- Procesos de Gestión de Tecnología.

Fase II: Mejoramiento de los Procedimientos relacionados con los nuevos procesos de tecnologías de información.

Procesos y Procedimientos.

Proceso:	Estrategia Tecnológica.
Procedimiento:	Elaboración y seguimiento del plan estratégico de TI

Proceso:	Marco de Trabajo de los Procesos de Tecnología
Procedimiento:	Gestión de proyectos Validación Roles de tecnología Solicitud de accesos de desarrolladores a ambientes en producción Cambio de puestos Gestión y organización de procesos de tecnología Autocontrol Interno

Proceso:	Gestión del Desempeño y de la Calidad
Procedimiento:	Monitoreo del desempeño de los servicios de TI Autocontrol Interno

Proceso:	Arquitectura Tecnológica.
Procedimiento:	Adquisición, implementación y mantenimiento de la infraestructura tecnológica. Elaboración y seguimiento del plan estratégico de TI (Planeamiento de capacidades)

Proceso:	Gestión de Talento Humano
Procedimiento:	Políticas de reclutamiento de personal Procedimiento de selección de personal Procedimiento de Búsqueda y Selección de personal

Proceso:	Cumplimiento de Políticas y Regulaciones
Procedimiento:	Autocontrol Interno

Proceso:	Gestión de Proyectos
Procedimiento:	Gestión de Proyectos

Procesos de Gestión de Riesgos.

Proceso:	Marco de Gestión de Riesgos Tecnológicos
Procedimiento:	Metodología de gestión de riesgos de TI Autocontrol Interno

Proceso:	Políticas de Riesgos Tecnológicos
Procedimiento:	Política de seguridad de la información Autocontrol Interno

Proceso:	Gestión de Riesgos
Procedimiento:	Gestión de proveedores de TI Autocontrol Interno

Proceso:	Monitoreo de Riesgos
Procedimiento:	Autocontrol Interno

Proceso:	Propiedad y Clasificación de los Activos de Información
Procedimiento:	Elaboración, actualización y/o mantenimiento de activos de TI

Proceso:	Comunicación, entrenamiento y concientización
Procedimiento:	Elaboración del plan de capacitación Elaboración del plan de concientización

Procesos de Gestión de Tecnológica

Proceso:	Administración de Accesos
Procedimiento:	Gestión de accesos

Proceso:	Desarrollo, Adquisición y Mantenimiento de Sistemas
Procedimiento:	Gestión de Cambios Gestión de proyectos Elaboración y seguimiento del plan estratégico de TI

Proceso:	Seguridad en Plataforma
Procedimiento:	Monitoreo de Seguridad e Infraestructura Actualización de antivirus Actualización de parches de seguridad Adquisición, implementación y mantenimiento de infraestructura

Proceso:	Control de cambios
Procedimiento:	Gestión de cambios Definición de ambientes controlados para pruebas Migración de datos Respaldo y Restauración Monitoreo de aplicativos en producción- pos implementación

Proceso:	Gestión de activos y configuraciones
Procedimiento:	Gestión de activos y configuraciones

Proceso:	Servicios con Terceros
Procedimiento:	Gestión de proveedores de TI Gestión de niveles de Servicio Monitoreo de niveles de servicio

Proceso:	Niveles de Servicio
Procedimiento:	Gestión de niveles de Servicio Monitoreo de niveles de servicio

Proceso:	Operaciones
Procedimiento:	Adquisición, implementación y mantenimiento de infraestructura Para la definición de ambientes controlados para pruebas Elaboración y difusión de manuales Operativos Respaldo y Restauración Gestión de tareas

Proceso:	Mesa de Ayuda y Servicios de Campo
Procedimiento:	Gestión de mesa de ayuda

Proceso:	Gestión de Incidentes de TI y Seguridad
Procedimiento:	Gestión de incidentes de seguridad de la información Gestión de incidentes de TI Gestión de mesa de ayuda

Proceso:	Monitoreo
Procedimiento:	Monitoreo de Seguridad e Infraestructura

Proceso:	Administración de Datos
Procedimiento:	Respaldo y Restauración Mantenimiento de base de datos

Proceso:	Gestión de Problemas
Procedimiento:	Gestión de mesa de ayuda

Proceso:	Resiliencia y Seguridad Física
Procedimiento:	Monitoreo de controles ambientales y físicos del Centro de Cómputo

Fase III: Identificar los controles claves en cada proceso, con la finalidad de alcanzar el grado de madurez adecuado, por favor referirse a la Tabla 1 del capítulo anterior donde se muestra lo deseado y la brecha a cubrir.

Fase IV: Definición de flujos y controles a implementar, permite tener flujogramas identificando los controles asociados.
La primera obtención de evidencias bajo el presente esquema la podemos mencionar como punto final de control de todo el proceso de implementación y es la prueba de todos los controles implementados.

Capítulo 4
Solución Propuesta

El presente capítulo se inicia con un concepto de James Harrington (1993), “Mejorar un proceso, significa cambiarlo para hacerlo más efectivo, eficiente y adaptable, qué cambiar y cómo cambiar depende del enfoque específico del empresario y del proceso”.

El tema de mejora continua en las organizaciones es un deber motivo por el cual los procedimientos deben estar en constante cambio para poder adecuarse a los nuevos escenarios y retos de la organización.

4.1 Definición de los Procesos de TI y Alineamiento de Estrategias.

Lo que se busca es establecer un marco de trabajo estándar y homologado en la organización para la gestión de tecnología así como también de la gestión de riesgos tecnológicos.

El siguiente mapa de procesos de tecnología de información (Ver Figura 4.1), permite apreciar el gobierno de TI de la organización mediante 3 macro procesos bien definidos:

- Organización de Tecnologías de Información.
- Procesos de Gestión de Riesgos Tecnológicos.
- Proceso de Gestión de Tecnología.

Organización de Tecnología de Información.

Orientada a definir los procesos a nivel estratégico con la finalidad de alinearse a los requerimientos de la organización.

Es la encargada de definir estándares a nivel arquitectura tecnológica con la finalidad de que todo nuevo requerimiento se implemente de acuerdo a los estándares pre establecidos de esta manera podemos reducir el TCO (Total Cost Ownership – Costo Total de Propiedad) del activo involucrado.

Se interrelaciona con el recurso humano, que es uno de los factores determinantes de éxito dentro de la organización consideremos al recurso humano como un activo de información.

Procesos de Gestión de Riesgos Tecnológicos.

El nivel de riesgos de los activos de tecnología es basado en el valor de los negocios y las sumas de la valoración del negocio referente a riesgos operativos, representado esto en la clasificación de los activos por medio de los atributos de Confidencialidad, Integridad y Disponibilidad de los activos.

- Se adoptarán los procesos transversales del modelo de gestión de riesgos tales como (conforme vayan existiendo):
    - Tolerancia y Apetito al riesgo.
    - Aceptación y Excepciones de Riesgos.
    - Monitoreo/Mitigación de riesgos.
    - Análisis de Impacto del Negocio (proceso BIA)
    - Evaluación Integral de Riesgo (IRAP)
    - Gestión e Incidentes.

- Las políticas deberán de contar con la especificación del nivel de aplicación de los controles con base al nivel de clasificación.

- Para el despliegue del modelo es necesaria la ejecución del BIA (*Business Impact Analyst*) para obtener la clasificación actualizada para los activos.

- Este modelo se alienará a la Estructura de Gobierno Corporativa.

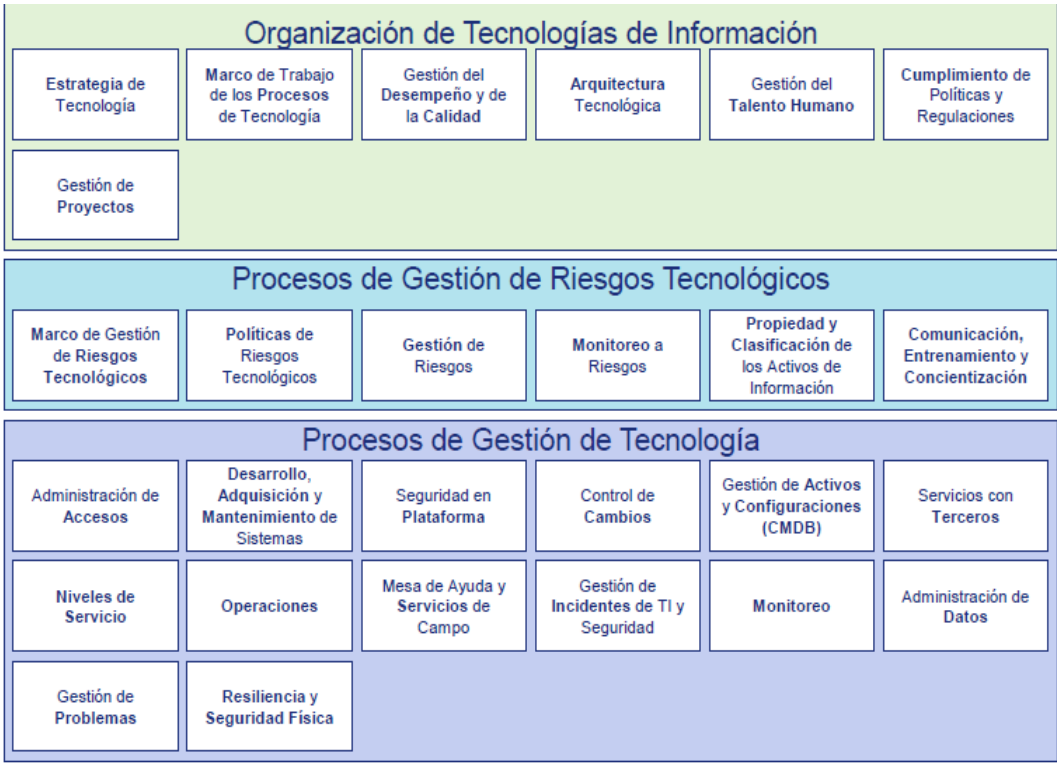


Fig. 11 Mapa de Procesos
Fuente: Elaboración propia

Procesos de Gestión de Tecnología.

Enfocado a la parte operativa del área, donde se busca atender el día a día pero utilizando procesos claramente definidos, por ejemplo tenemos las parte de control de cambios en la cual ante un requerimiento de cambio de un activo de información es el dueño de dicho activo quién autoriza que el custodio proceda con el cambio, también podemos hablar del monitoreo de seguridad de acuerdo a las reglas de negocio pre establecidas.

De esta manera orquestamos todos los procesos operativos para alinearse a la estrategia del área y esta a su vez al negocio.

4.1.1 Alineamiento de Estrategias

El alineamiento de la estrategia del negocio con TI se muestra en el siguiente cuadro:

Tabla 2 Alineamiento de Estrategias

		Objetivos Estratégicos del Negocio				Cobit	
	Giro del Negocio	Objetivo Estratégico 1	Objetivo Estratégico 2	Objetivo Estratégico 3	Objetivo Estratégico 4	Objetivos para el Gobierno Empresarial de TI	
Objetivos Estratégicos de TI	El giro único del negocio de AFP es la administración de Fondos de Pensiones individuales	La diversifica-ción del negocio a nivel de latinoameri-ca,conside-rando y respetando los propios "core" del negocio en cada país.	El desarrollo de sinergias comerciales , lo cual implica que los clientes participen más de un servicio o producto brindado.	Eliminación de los costos redundan-tes	La adquisición de nueva infraestruc-tura tecnológica que le permita satisfacer estas nuevas estrategias	Asegurar que se obtiene el óptimo de las iniciativas, servicios y activos de TI, brindando soluciones confiables para alcanzar las necesidades del negocio. Garantizar que los riesgos para el negocio, relacionado con TI, se gestionen y no exceden el nivel aceptable establecido por la dirección. Garantizar que las necesidades de recursos de TI se cubren en forma eficiente, con costos optimizados.	Estratégias de TI
	Integrar los procesos de TI de AFP adquirida a los actuales logrando un estandar más adecuado.		X	X	X	Implementación de Sistemas de Calidad y Seguridad de la Información en TI.	
	Gestionar los procesos de negocio a través de TI de manera confiable y medible con orientación al	X	X	X	X	Enfoque intensivo en el Outsourcing	
	Usar las mejores prácticas logrando mejoras sostenibles en el tiempo	X	X	X	X	Adopción de soluciones tecnológicas de AFP adquirida para optimizar y diversificar los servicios al cliente	
	Definir información simple, completa, oportuna y transparente	X	X	X	X	Adquisición de un Sistema Integral único, el ERP SAP para empresa del Grupo.	
	Aplicar la tecnología en beneficio del crecimiento del negocio.	X	X		X	Ir hacia una unidad integrada de TI a nivel del grupo	
	Conseguir una plataforma de TI que soporte esta integración.	X	X		X	Uso de infraestructura que se encuentre alineada al negocio.	

Fuente: Elaboración propia.

4.1.2 Procedimiento de Elaboración del Plan Estratégico

Objetivo

Brindar los lineamientos básicos para la elaboración del Plan Estratégico de Tecnología de Información aplicable dentro del alcance establecido y en base a las buenas prácticas recomendadas por COBIT.

Alcance

La metodología de elaboración del Plan Estratégico de Tecnología de Información (PETI), abarca a toda la Organización de TI alineada a las estrategias de negocio que hayan sido plenamente planificadas y establecidas en la compañía.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO1 Definir un Plan Estratégico" con un avance del 57.14% de acuerdo a la tabla 1, identificando las siguientes carencias:

- El Plan estratégico de Tecnología de Información (PETI) debe estar alineado a las estrategias de negocio.
- El plan de capacidad de infraestructura debe servir como entrada para la elaboración del PETI, con la finalidad de soportar las nuevas necesidades de la organización.
- Los proyectos de desarrollo, modificación y/o adquisición de nuevo software se deben contemplar dentro de los proyectos enfocados en los servicios de TI.

Información adicional referente a dicho procedimiento consultar el Anexo S.

Solución Propuesta

La metodología de Elaboración del Plan Estratégico de Tecnologías de Información tiene los siguientes resultados relevantes:

- Análisis de la situación actual de las TI en la compañía.
- Estrategias de TI alineadas a las estrategias de negocio.
- Plan operativo de TI para la implantación de las estrategias de TI.

4.2 Mejoramiento de Procedimientos.

4.2.1 Administración de Accesos

Objetivo

El objetivo principal del procedimiento es tener un escenario controlado para la administración de las cuentas de usuarios de cualquier activo de información.

Alcance

Aplica a toda la administración de cuentas de usuarios, sea personal interno o externo de la compañía, en los diferentes activos tanto a nivel aplicativo como de infraestructura. Asimismo cubre aspectos relacionados a los procesos de revisión y monitoreo de cuentas, lineamientos para el uso de contraseñas, entre otros.

Situación Actual

El nivel de madurez requerido para el presente proceso es 4 y se relaciona al dominio" "Delivery and Support" "DS5 Garantiza la seguridad de los sistemas" y de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 16.67% de avance, identificando las siguientes carencias:

- Falta de un rol que cumpla la función de Administrador de Accesos.
- Falta de definición de los dueños de activos de información y custodios.
- Concientización de los dueños respecto a la seguridad de información.
- Proceso formal de revisión de accesos.

Solución Propuesta

Para poder cubrir la brecha presentada es necesario implementar los siguientes puntos:

- Procedimiento de Creación de Cuentas de Usuario.
- Procedimiento de Revisión de Accesos.
- Procedimiento de Acceso a Ambientes de Producción para Personal de Desarrollo.

Información adicional referente a dichos procedimientos consultar el Anexo B.

Beneficios

- Mejora en el control del acceso a los recursos informáticos de la compañía.
- Optimización del control de los perfiles con la revisión de la debida correspondencia con las funciones laborales de los usuarios.
- Asegurar la información de los ambientes de producción mediante la debida autorización de los accesos con privilegios y el control de cuentas temporales.
- Control constante de los privilegios de acceso y de los estados de los usuarios en los diferentes activos de información.

4.2.2 Administración de Datos

La administración de datos está compuesta de tres componentes:

- Lineamiento de Intercambio de Información.
- Eliminación Segura de Información.
- Respaldo y Restauración.

Lineamiento de Intercambio de Información

Objetivo

El objetivo principal es proteger la información confidencial de la compañía en el intercambio interno y externo, y el uso de medios de información, ante amenazas que afecten la confidencialidad, integridad y disponibilidad de la información.

Alcance

Tiene un alcance para los intercambios de información sensible definido como C3 y C4 (Ver Criterios para la definición de los niveles de criticidad de los activos de TI Fig. 8) tanto si el intercambio es interno/externo, para los medios de información que sean sensibles y que es necesario implementar controles.

Situación Actual

De acuerdo al nivel de madurez requerido para el presente control se identificó en el dominio "Delivery and Support" "DS11 Administración de Datos" y de acuerdo a lo descrito en el capítulo anterior Tabla 1 vemos que sólo tenemos un 25% de avance, identificando las siguientes carencias:

- No se identificó lineamientos formales para el intercambio de información.
- No existe la concientización de seguridad de información por parte de la organización.

Solución Propuesta

- Elaboración de Lineamiento de Intercambio de Información.

Beneficios

- Cumplir con los requerimientos legales y contractuales del intercambio de la información de nivel C3 y C4.
- Niveles de seguridad con terceros, para el intercambio de información de nivel C3 y C4.
- Relación de técnicas de seguridad de la información en los medios de información.
- Relación de controles de seguridad implementados en los medios de almacenamiento.

Información adicional referente a dichos procedimientos consultar el Anexo C.

Eliminación Segura de Información

Objetivo

El objetivo principal del proceso es proteger la información en diferentes medios la cual no es eliminada en forma segura, y por lo tanto está expuesta por personas no autorizadas.

Alcance

El proceso de eliminación segura de la información, tiene como alcance todo activo de información que almacene información de la organización y se inicia mediante la definición de los tipos de eliminación segura y el registro de actas de los equipos y medios eliminados en forma segura.

Situación Actual

De acuerdo al nivel de madurez requerido para el presente control se identificó en el dominio "Delivery and Support" "DS11 Administración de Datos" y de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 25% de avance, identificando las siguientes brechas:

- No se identifica un procedimiento de eliminación segura de medios.
- Todo personal de TI debe identificar los medios donde se tenga información confidencial.
- Los propietarios de la información y del medio donde se almacena son responsables de eliminar la información con los mecanismos establecidos, cuando se re-usa o elimina el medio.
- El analista de seguridad debe definir los mecanismos oficiales para eliminar la información lógica o física.
- Cada vez que se elimine la información se debe elaborar un Acta de eliminación segura donde firmen los propietarios y/o el usuario y/o el custodio y/o el ejecutivo de Seguridad / DRP, según sea el caso.

Situación Propuesta

- Procedimiento de Eliminación Segura de Medios. (Información adicional referente a dichos procedimientos consultar el Anexo C)

Beneficios

- Relación de técnicas de eliminación segura para diferentes medios.
- Actas de eliminación segura de la información.
- Niveles de seguridad con terceros, para la eliminación segura de la información.

Respaldo y Restauración

Objetivo

El objetivo principal es realizar el respaldo y la restauración de los activos de TI, para poder disponer los datos en caso de un incidente.

Alcance

Procedimiento de respaldo y restauración inicia desde el registro de la tarea de respaldo en el Schedule de gestión de tareas, hasta que realice la restauración de la información sea por necesidad de prueba o para atender un evento.

Situación Actual

De acuerdo al nivel de madurez requerido para el presente control se identificó en el dominio "Delivery and Support" "DS11 Administración de Datos" y de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 25% de avance, identificando las siguientes brechas:

- No se identifica la realización de pruebas de recuperación de información calendarizadas.

Situación Propuesta

- Procedimientos de Respaldo y Restauración

Beneficios

- Contar con una copia de respaldo probada que puede ser usada para restaurar el sistema de información de producción.

4.2.3 Gestión de Control de Cambios

Objetivo

El objetivo principal del proceso es gestionar adecuadamente los cambios de infraestructura y aplicaciones con la finalidad de que se lleven eficientemente y minimizar los impactos en la continuidad operativa y de seguridad.

Alcance

El proceso de gestión de cambios, empieza desde el requerimiento del cambio RFC (Request for Change), la revisión y aprobación del cambio, las pruebas y el pase a producción del requerimiento de cambio.

Todos los cambios de IT que impactan en la funcionalidad del ambiente de producción de los diferentes activos de la compañía (Aplicaciones e Infraestructura).

Situación Actual

De acuerdo al nivel de madurez requerido para el presente control se identificó en el dominio "Adquirir e Implementar" "AI6 Administrar los Cambios" y "AI7 Instalar y Acreditar Soluciones y Cambios" de acuerdo a lo descrito en el capítulo anterior Tabla 1

vemos que sólo tenemos un 5.56% de avance para AI6 y un 0% para AI7, identificando las siguientes brechas:

- Asegurar que se otorguen las autorizaciones adecuadas durante todo el ciclo del cambio.
- Minimizar los impactos de continuidad operativa y de seguridad.
- Solucionar errores conocidos.
- Desarrollo de nuevos servicios.
- Mejora a los servicios existentes.
- Cumplimientos legales requeridos.

Situación Propuesta

- Procedimiento de Cambio Normal.
- Procedimiento de Cambio de Emergencia.
- Procedimiento de Adquisición de la Solución.
- Procedimiento de Desarrollo de la Solución.
- Procedimiento de Pruebas de la Solución.
- Procedimiento de Pase a Producción.
- Procedimiento de Monitoreo del Cambio.

Información adicional referente a dichos procedimientos consultar el Anexo D.

4.2.4 Desarrollo, Adquisición y Mantenimiento de Sistemas

Plan de Aseguramiento de Software

Objetivo

El objetivo principal es contar con un patrón planificado y sistemático que permita las acciones necesarias para proporcionar la confianza adecuada que el software cumpla con los requisitos para la cual fue creado.

Alcance

Plan de Aseguramiento de Calidad de Software, aplica a todos los tipos de desarrollos internos, externos y adquisiciones. Se aplica durante el ciclo de vida del desarrollo de sistemas.

Situación Actual

De acuerdo al nivel de madurez requerido 2 para el presente control se identificó en el dominio Planear y Organizar "PO8 Administrar la Calidad" de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que cumple al 100%.

Con una periodicidad mensual, siempre al final de cada mes, los responsables de la ejecución de las pruebas de calidad y de la fábrica del software proporcionarán al responsable de aseguramiento de calidad la siguiente información:

- Resultados de las revisiones de los artefactos.
- Acciones realizadas.
- Excepciones de calidad.

- Se obtuvo una clasificación formal de los desarrollos de acuerdo a la tabla 3

Tabla 3 Clasificación Formal de los Desarrollos.

Tamaño y Esfuerzo del trabajo	Duración máxima	Costo Estimado
Correctivos Urgentes	1 semana	Bajo
Pequeños y correctivos	1 mes	Bajo
Medianos	4 meses	Medio
Grandes y Proyectos	Más de tiempo	Alto

Fuente: Elaboración propia.

- Descripción de los artefactos, los artefactos que se producen como parte del desarrollo son evaluados para asegurarse que se está cumpliendo con la calidad.
- Tipos de casos de prueba.
- Cumplimiento de los artefactos.
- Verificación de los artefactos.
- Revisión de la calidad de acuerdo a los indicadores.

Información adicional de los procedimientos consultar el Anexo E.

Solución Propuesta

De acuerdo al nivel de madurez requerido no se encontró carencia.

Beneficios

Los hallazgos identificados permiten a la organización tener como fortaleza el proceso de calidad de desarrollo de software., motivo por el cual se le recomienda que el nivel de madurez que puede alcanzar pueda llegar a un nivel 3 con facilidad.

4.2.5 Gestión de Incidentes de Seguridad

Objetivo

Asegurar que los eventos y debilidades de seguridad de información que se presentan en la organización y su entorno, sean comunicados de una manera oportuna para realizar acciones correctivas a tiempo y prevenir su repetición de la misma.

Alcance

Es iniciado cuando el Ejecutivo de Seguridad Informática y DRP recibe la notificación de un evento o de un Incidente de Seguridad de la Información y toma acción para resolverlo en conjunto con el equipo de contención, mediante acciones orientadas a la solución del incidente. Debiendo informar al Oficial de Seguridad de la Información cuando la criticidad lo amerite.

Situación Actual

De acuerdo al nivel de madurez 4 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS5 Garantizar la Seguridad de los Sistemas" y de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 16.67% de avance, identificando las siguientes carencias:

- El responsable de seguridad de la información debe tener entre sus funciones la contención de incidentes de seguridad de la información.
- No existe reportes de incumplimiento de normas de seguridad de la información.
- Como parte la inducción al personal todo colaborador debe ser capacitado para detectar y reportar los incidentes de seguridad.
- No existe clasificación de tipos de incidentes ni su registro.
- Todo incidente categorizado como crítico debe ser reportado al Oficial de Seguridad de la Información.

Solución Propuesta

- Elaboración de un procedimiento de Gestión de Incidentes de Seguridad de la información.

Información adicional referente a dicho procedimiento consultar el Anexo F.

Beneficios

- Capacidad de respuesta ante incidente.
- Gestión de los incidentes de seguridad de información.
- La capacidad para reducir el riesgo y los costos para la organización.
- Capacidad para detectar, informar, evaluar los incidentes, reduce en un menor tiempo inactividad los servicios de la organización.
- Capacidad para identificar las posibles mejoras en los servicios.

4.2.6 Gestión de Incidentes de TI

Objetivo

El objetivo principal del proceso de la Gestión de Incidentes es restaurar la normalidad del servicio lo más pronto posible minimizando el impacto adverso en las operaciones del negocio, garantizando que los mejores niveles posibles de calidad y disponibilidad del servicio se mantenga.

Alcance

El proceso de la Gestión de Incidentes se inicia a través de una llamada telefónica del usuario, un correo electrónico del personal de TI o mediante una alerta de alguna herramienta de monitoreo y termina cuando después de recuperar el servicio TI se consigue la conformidad del usuario.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS8 Administrar la Mesa de Servicio y los Incidentes" y de acuerdo a lo descrito en el capítulo anterior vemos que sólo tenemos un 35.71% de avance, identificando las siguientes carencias:

- Todo incidente y su estado deben ser comunicados oportuna y efectivamente.
- Los incidentes se deben resolver en plazos aceptables para el negocio.
- Se debe mantener la satisfacción del cliente en lo posible.
- Se debe mantener la satisfacción del cliente en lo posible.
- La gestión de los incidentes debe estar alineada con los niveles de servicio y objetivos generales de la empresa.
- Todos los incidentes deben ser registrados y administrados por un único sistema de gestión.
- Todos los incidentes deben supeditarse a un esquema de clasificación y priorización estándar que sea común en toda la empresa.
- Los registros de incidentes deben ser auditados de forma regular para asegurarse de que se han introducido y categorizados correctamente.

Solución Propuesta

- Procedimiento de Gestión de Incidentes.
- Procedimiento de Generación y Validación del Reporte Mensual de la Mesa de Ayuda

Información adicional referente a dichos procedimientos consultar el Anexo G.

Beneficios

- Mejora la productividad de los usuarios al eliminar rápidamente los incidentes TI.
- Cumplimiento de los niveles de servicio acordados en el SLA.
- Mayor control de los procesos y monitoreo del servicio.
- Optimización de los recursos disponibles.

La gestión de incidentes es decisiva en toda empresa, porque evidencia su valor en relación a otros procesos de la operación del servicio. A menudo es el primer proceso en ser implementado.

- Todo incidente y su estado deben ser comunicados oportuna y efectivamente.
- Los incidentes se deben resolver en plazos aceptables para el negocio.

4.2.7 Gestión de Problemas

Objetivo

El objetivo principal de la gestión de problemas es la administración de su ciclo de vida, comprendiendo su identificación, la investigación, la elaboración de la documentación respectiva y la solución definitiva o temporal del problema.

La gestión de problemas trata de minimizar el impacto negativo en el negocio, tanto de los incidentes como de los mismos problemas, causados por errores subyacentes en la infraestructura de TI, y trata de prevenir en forma proactiva la recurrencia de los incidentes relacionados con estos errores.

Para lograrlo, la gestión de problemas pretende determinar la causa raíz de los incidentes, documentarla y comunicar los errores conocidos y tomar acciones para mejorar o corregir la situación.

En resumen la gestión de problemas tiene como objetivos:

- Prevenir los problemas e incidentes resultantes de un evento.
- Eliminar los incidentes recurrentes.
- Minimizar el impacto de los incidentes que no puedan ser prevenidos.

Alcance

El proceso de la Gestión de Problemas comienza mediante una comunicación de la mesa de ayuda, a través una alerta de una herramienta de monitoreo, por medio de información de la gestión de incidentes, debido a un informe de la Gestión Proactiva de Problemas o por un correo electrónico de uno o más proveedores externos.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS10 Administración de Problemas" y de acuerdo a lo descrito en el capítulo anterior Tabla 1 vemos que sólo tenemos un 25% de avance, identificando las siguientes carencias:

- No se identificó un procedimiento formal para la gestión de problemas.
- El proveedor del servicio debe analizar los datos y tendencias sobre los incidentes y problemas para identificar la causa raíz y su potencial acción preventiva.
- Cuando la causa raíz del problema ha sido identificada, pero el problema no ha sido resuelto de manera permanente, el proveedor del servicio debe identificar las acciones para reducir o eliminar el impacto del problema en los servicios.
- Los errores conocidos deben ser registrados, generando de esta manera una base de conocimiento.
- La eficacia de la resolución de los problemas debe ser monitoreada, revisada y se debe informar sobre la misma.
- Las tecnologías de soporte deben integrarse con el propósito que el negocio obtenga beneficios y fácilmente pueda interconectarse con las tecnologías propias de la

gestión de servicios que usan o proporcionan información relacionada de uno o más problemas.

Solución Propuesta

- Procedimiento formal de Gestión de Problemas.

Información adicional referente a dicho procedimiento consultar el Anexo H.

Beneficios

- Una mayor disponibilidad de los servicios TI gracias a la reducción del número y la duración de los incidentes que en esos servicios pueden causar. Para eso la gestión de problemas trabaja conjuntamente con la gestión de incidentes y la gestión del cambio para asegurar que la disponibilidad y calidad de servicio se incrementan.
  Cuando se resuelve los problemas e incidentes, la información de la resolución es registrada en la base de conocimiento. En el mediano plazo, esta información es utilizada para acelerar el tiempo de resolución y encontrar soluciones permanentes, reduciendo el número y el tiempo de resolución de los incidentes.
- Reducción de los gastos en soluciones temporales o parches que no funcionan.
- Disminución de los costos de resolución de los incidentes repetidos.

4.2.8 Gestión de Talento Humano

La gestión del talento humano, se basa en tres pilares claramente identificados:

- Elaboración del Plan de Capacitación de TI.
- Elaboración del Pan de Concientización de Riesgos Operativos y TI
- Cambio de Puestos y Funciones

Elaboración del Plan de Capacitación de TI

Objetivo del Proceso

El objetivo principal del proceso es contar con el personal calificado y capacitado en el Área de Tecnología de Información (TI) para la ejecución y función de los roles, con la finalidad de minimizar los riesgos que puedan existir al no estar preparado.

Alcance

El proceso del Plan de Capacitación de Tecnología de Información, se inicia a través del análisis situacional del área de Tecnología con la finalidad de detectar las necesidades de aprendizaje hasta la ejecución, monitoreo y mejora de los programas de capacitación de TI.

Situación Actual

De acuerdo al nivel de madurez 2 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO7 Administrar los Recursos Humanos de TI" y de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 25% de avance, identificando las siguientes carencias:

- Plan de Capacitación de TI de acuerdo a los requerimientos de la organización.

Solución Propuesta

- Procedimiento de Elaboración del Plan de Capacitación de TI.

Información adicional referente a dicho procedimiento consultar el Anexo I.

Beneficios

- Plan de Capacitación del personal de TI
- Reporte de cobertura en capacitación para el personal de TI

Elaboración del Plan de Concientización de Riesgos Operativos y Tecnología de Información

Objetivo

El objetivo principal de este proceso es el mejorar la capacidad de percibir, sentir y que sea consciente el personal de AFP la importancia de gestionar los riesgos y el cumplimiento de los controles y procedimientos de TI.

Alcance

El proceso del plan de concientización de seguridad de la información (SI) y tecnología de información (TI), se inicia a través del análisis situacional de las áreas de la organización, con la finalidad de detectar las necesidades de ejecutar un plan hasta la ejecución, monitoreo y mejora de los programas de concientización.

Situación Actual

De acuerdo al nivel de madurez 2 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO7 Administrar los Recursos Humanos de TI" y de acuerdo a lo descrito en el capítulo anterior vemos que sólo tenemos un 25% de avance, identificando las siguientes carencias:

- Todo personal de TI debe ser consciente de la importancia de cumplir con los procedimientos y controles de los procesos de TI.
- Todo personal de TI debe participar en la ejecución del plan de concientización.
- Es responsabilidad de Riesgos Operativos y la Subgerencia de Servicios de Sistemas elaborar planes de concientización.

Solución Propuesta

- Procedimiento de Elaboración del Plan de Concientización de Riesgos Operativos y Tecnología de Información.

Información adicional referente a dicho procedimiento consultar el Anexo I.

Beneficios

- Plan de concientización del personal de Riesgos Operativos (ROP) y Tecnología de Información (TI).
- Reporte de cobertura en concientización del personal de ROP y TI.
- Nivel de concientización del personal de ROP y TI.

Cambio de Puesto y Funciones

Objetivo

El objetivo del presente documento es asegurar que el cambio de funciones dentro de la Subgerencia de Sistemas se realice en forma ordenada, garantizando la reasignación oportuna de responsabilidades y accesos y previniendo cualquier posible conflicto de segregación de funciones.

Alcance

El procedimiento inicia con la solicitud del Cambio de Puesto y/o Funciones de determinado colaborador por parte del Responsable del Área al cual pertenece el colaborador. El procedimiento termina con la modificación de los accesos, la asignación de nuevas funciones al colaborador y las actualizaciones del Manual de Organización y Funciones, del documento de Descripción de Puestos y del documento de Roles y Funciones de la Subgerencia de Servicios de Sistemas.

Situación Actual

De acuerdo al nivel de madurez 2 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO7 Administrar los Recursos Humanos de TI" y "PO4 Definir los Procesos, Organización y Relaciones de TI" de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 25% de avance, identificando las siguientes carencias:

- Segregación de funciones en personal de TI.
- No existe un procedimiento formal de cambio de puestos y funciones.

Solución Propuesta

- Procedimiento de Cambio de Puestos y Funciones.

Información adicional referente a dicho procedimiento consultar el Anexo I.

Beneficios

- Definición y asignación clara de las responsabilidades para el cambio de puesto del colaborador.
- La redefinición de los derechos de acceso del colaborador a la información y medios de procesamiento de la información.

4.2.9 Gestión de Desempeño y de la Calidad

Objetivo

El presente procedimiento tiene por objetivo garantizar una efectiva administración del desempeño de los servicios de tecnologías de la información brindados por la Subgerencia de Servicios de Sistemas a las demás áreas de la empresa, a través de un proceso de monitoreo eficaz. Dicho monitoreo se requiere para asegurar que las actividades que se realicen dentro de la subgerencia se hagan de manera correcta y que estén alineadas con el conjunto de direcciones y políticas de la organización.

Alcance

El procedimiento inicia con la definición de los indicadores de desempeño que serán utilizados por la Subgerencia de Servicios de Sistemas para medir el rendimiento de sus servicios de tecnologías de la información prestados a las demás áreas de la compañía y termina con la aprobación del resultado de la evaluación del desempeño real contra los indicadores de desempeño inicialmente establecidos por la Subgerencia de Servicios de Sistemas.

Situación Actual

De acuerdo al nivel de madurez 2 requerido para el presente control se identificó en el dominio "Monitor and Evaluate" "ME1 Monitorear y Evaluar el Desempeño de TI" de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 12.5% de avance, identificando las siguientes carencias:

- Los servicios de tecnología no cuenta con algún tipo de medición que haga cuantificable su labor.

Información adicional referente a dicho procedimiento consultar el Anexo J.

Solución Propuesta

- Procedimiento de Monitoreo de Desempeño de los Servicios de TI.

Beneficios

El procedimiento tiene los siguientes resultados relevantes:

- La comunicación e institucionalización de un proceso estándar de monitoreo de los servicios brindados por la Subgerencia de Servicios de Sistemas a las demás áreas de la compañía.

- El desarrollo de una base de conocimiento del desempeño histórico de los indicadores definidos por la Subgerencia de Servicios de Sistemas.
- La definición, usando criterios financieros y operativos tradicionales, de la función de la Subgerencia de Sistemas con respecto al desempeño global de la organización.

4.2.10 Marco de Trabajo de los Procesos de Tecnología

Se identificó como parte del marco de trabajo:

- Procesos de Tecnología.
- Validación de Roles y Responsabilidades.

Procesos de Tecnología.

Objetivo

El presente procedimiento tiene por objetivo establecer los lineamientos para administrar y organizar los procesos realizados en la Subgerencia de Sistemas, perteneciente a la Gerencia Central de Operaciones y Sistemas de AFP.

Alcance

El procedimiento inicia con la solicitud de la revisión de la documentación relacionada con el mapa de los procesos de TI y el documento del Sistema de Gestión. El procedimiento termina con la comunicación a la Subgerencia de Sistemas y al Gerente Central de Operaciones y Sistemas de la revisión del Sistema de Gestión de TI.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO4 Definir los Procesos, Organización y Relaciones de TI" de acuerdo a lo descrito en el capítulo anterior vemos que sólo tenemos un 44.44 % de avance, identificando las siguientes carencias:

- No se identificaron procesos claramente definidos que se encuentren alineados a los objetivos de la organización.

Información adicional referente a dicho procedimiento consultar el Anexo K.

Solución Propuesta

Establecer formalmente los siguientes procesos:

- Gestión del Desempeño y de la Calidad.
- Arquitectura Tecnológica.
- Gestión del Talento Humano
- Cumplimiento de Políticas y Regulaciones.
- Gestión de Proyectos

- Marco de Gestión de Riesgos Tecnológicos
- Políticas de Riesgos Tecnológicos
- Gestión del Riesgo
- Monitoreo a Riesgos
- Propiedad y Clasificación de los Activos de Información
- Comunicación, Entrenamiento y Concientización
- Administración de Accesos
- Desarrollo, Adquisición y Mantenimiento de Sistemas
- Seguridad en Plataforma
- Control de Cambios
- Gestión de Activos y Configuraciones
- Servicios con Terceros
- Niveles de Servicio
- Operaciones
- Mesa de Ayuda y Servicios de Campo
- Gestión de Incidentes de TI y Seguridad
- Monitoreo
- Administración de Datos.
- Gestión de Problemas
- Resiliencia y Seguridad Física.
- Recuperación a Desastres (DRP).
- Sistema de Gestión
- Propiedad y Clasificación de los Activos de Información

Beneficios

- Sistema de Gestión de TI actualizado.
- Contar con una estructura de procesos claramente definida que soporte y se encuentre alineado a los intereses de la organización.
- Personal de TI informado.

Validación de Roles y Responsabilidades TI

Objetivo

El objetivo del presente procedimiento es verificar si todos los roles existentes actualmente en la Gerencia de Sistemas están correctamente distribuidos entre los distintos puestos existentes en dicha gerencia.

Alcance

El procedimiento inicia con la revisión de las funciones de cada puesto que forma parte de la Gerencia de Sistemas y termina con la consolidación de las modificaciones y/o confirmación de la no actualización del Manual de Organización y Funciones y del Documento de “Roles en la Subgerencia de Servicios de Sistemas”.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO4 Definir los Procesos, Organización y Relaciones de TI" de acuerdo a lo descrito en el capítulo anterior Tabla 1, vemos que sólo tenemos un 44.44 % de avance, identificando las siguientes carencias:

- En el levantamiento de información inicial se detectaron conflictos de intereses por no tener una segregación de funciones adecuado.

Información adicional referente a dicho procedimiento consultar el Anexo K.

Solución Propuesta

- Definición formal de "Roles de Tecnología"

Beneficios

El procedimiento concluye con la consolidación de las modificaciones y/o confirmación de la no actualización del Manual de Organización y Funciones y del Documento de "Roles en la Subgerencia de Sistemas".

4.2.11 Monitoreo

Monitoreo de Seguridad e Infraestructura

Objetivo

El principal objetivo de este procedimiento es el monitoreo de la seguridad y la infraestructura de la red en base a los recursos que la soportan; el monitoreo de seguridad previene, generando alertas o generando reportes de las actividades realizadas en los diversos componentes de la red y en especial a los activos sensibles y críticos, de tal manera que se pueda identificar oportunamente cualquier falla, ataque u otro tipo de actividad que comprometa la estabilidad y la confiabilidad de los activos de información, sea que estén ubicados en el perímetro o en la red interna, de tal forma que se gestionen adecuadamente los incidentes, y se tomen acciones correctivas, y en el caso que se materialicen medir el impacto y tener un control estadístico del historial; en el monitoreo de infraestructura se realiza en base en umbrales definidos y tipos de alertas que se activan cuando el comportamiento no es el deseado, a fin de asegurar las operaciones de la red.

Alcance

El proceso de Monitoreo de Seguridad e Infraestructura se inicia a través de el establecimiento de las herramientas que se utilizan y el envío de las alertas por el SOC (Security Operational Center), análisis de vulnerabilidades, código seguro, hardening (customización de buenas prácticas) para la infraestructura y análisis de código seguro para los sistemas las cuales activan la gestión de incidentes y generación de acciones preventivas y correctivas.

Situación Actual

De acuerdo al nivel de madurez 4 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS5 Garantizar la Seguridad de los Sistema" con un avance de 16.67% y el nivel de madurez 3 "DS13, Organización y Relaciones de TI", con un avance 12.5 % de avance, descrito en la tabla 1 identificando las siguientes carencias:

- El monitoreo de Seguridad e Infraestructura no se encuentra acorde a las normas vigentes referidas a la gestión de la Seguridad de la Información.
- No se identificó las alertas y su estado se comuniquen en forma oportuna.
- Las alertas notificadas se deben resolver en plazos aceptables para el negocio.
- Se debe mantener la disponibilidad de los activos críticos en lo posible.
- La gestión del monitoreo de seguridad e infraestructura debe estar alineada con los niveles de servicio y objetivos generales de la empresa.
- No se auditan los registros de las alertas del monitoreo de forma regular para asegurarse de que se han introducido y categorizados correctamente.

Información adicional referente a dicho procedimiento consultar el Anexo L.

Solución Propuesta

- Proceso de Monitoreo de Seguridad e Infraestructura
- Hardening de todos los dispositivos.
- Monitoreo de Código Seguro
- Análisis de Vulnerabilidades
- Ethical Hacking

Beneficios

- Mantiene la seguridad de la infraestructura la cual soporta la gran parte de los sistemas y servicios de la organización.
- Mejora la productividad de los activos al eliminar rápidamente las alertas de seguridad e infraestructura (rendimiento y performance).
- Mayor control de los procesos y monitoreo de seguridad e infraestructura.
- Optimización de los recursos disponibles.
- Aseguramiento de los activos y gestión de la mejora contínua.

4.2.12 Operaciones

La gestión de operaciones se basa en los siguientes pilares:

- Ambiente Controlado para Pruebas.
- Gestión de Tareas.
- Propiedad y Clasificación de los activos de Información

Ambiente Controlados para Pruebas

Objetivo

El objetivo principal es establecer un ambiente para soportar la efectividad y eficiencia de las pruebas e integración de aplicaciones e infraestructura en un entorno controlado.

Alcance

El procedimiento de la definición de ambientes controlados para pruebas se inicia con el requerimiento solicitado por el custodio del activo hasta la evaluación y finalización del ambiente preparado.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Acquire and Implement" "AI3 Adquirir y Mantener Infraestructura Tecnológica" sin avance 0% de avance de acuerdo a la tabla 1, identificando las siguientes carencias:

- Contar con un entorno para realizar pruebas controladas antes de pasar a producción.
- No todos los ambientes identificados son homologados a los ambientes actuales de producción.

Solución Propuesta

- Establecer un procedimiento para la definición de ambientes controlados para pruebas.

Información adicional referente a dicho procedimiento consultar el Anexo M.

Beneficios

- Al contar con ambientes controlados para pruebas se reducen los incidentes que pueden ser reportados en los ambientes de producción.

Gestión de Tareas

Objetivo

El objetivo principal es ejecutar una serie de tareas autorizadas en un momento específico sobre un equipo o un grupo de equipos informáticos de forma confiable, consistente, repetible y por lo general de forma automatizada con un mínimo grado de atención operativa.

Alcance

Procedimiento de gestión de tareas inicia con la planificación de la ejecución de los Jobs en intervalos ya programados (minuto, día, semana mes) hasta finalizar con los resultados de la ejecución del cronograma.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Acquire and Implement" "AI4 Facilitar la Operación y el Uso" sin avance 0% y en el dominio "Delivery and Support" "DS13 Administración de Operaciones" con un nivel de madurez 3 sin avance 0% de acuerdo a la tabla 1, identificando las siguientes carencias:

- Monitoreo de trabajos
- Falta de un cronograma de trabajos diario, semanal y mensual.
- Comunicación mediante alertas a los interesados de la ejecución satisfactoria de la tarea o de algún incidente presentado.

Solución Propuesta

- Procedimiento de gestión de tareas.
- Procedimiento de ejecución del cronograma.

Información adicional referente a dicho procedimiento consultar el Anexo M.

Beneficio

- Asegurar que las tareas programas inicialmente se hayan ejecutado correctamente en el plazo y tiempo determinado.

Propiedad y Clasificación de los activos de Información

Objetivo

El objetivo principal del proceso es la generación del inventario de activos de tecnologías de información que permita clasificarlos e identificar el nivel de criticidad que tienen para el negocio desde el enfoque de seguridad de la información.

Alcance

El proceso de elaboración, actualización y/o mantenimiento de activos de TI, se inicia a través de la recopilación general de los inventarios de activos de TI que están a cargo de los administradores de los diferentes tipos de activos de TI y finaliza con la obtención del listado de activos de TI y su nivel de criticidad para el negocio; así mismo, la actualización

y mantenimiento del inventario, se realiza cada vez que se incorpore y/o se retire funcionalmente cualquier tipo de Activo de TI.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Plan and Organize" "PO4 Definir los Procesos, Organización y Relaciones de TI" con un avance de 44.44% de acuerdo a la tabla 1, identificando las siguientes carencias:

- Todos los activos de TI deben ser claramente identificados y registrados en la matriz de activos de información.
- La actualización del inventario de activos debe ser proactivo y a demanda cada vez que se identifiquen cambios en los activos de TI, estos cambios deben ser reportados por los Custodios de Activos de TI.
- El mantenimiento del inventario de activos de TI debe ser realizado con una periodicidad anual, siendo responsable de su coordinación el Gestor de Activos de TI.
- Todo activo informático debe tener asignado un nivel de clasificación con relación a la confidencialidad, integridad y disponibilidad según lo detallado
- El inventario de activos de TI, es el único que contiene la información oficial desde el enfoque de seguridad de información y en esta se centraliza la información pertinente de los inventarios de activos tecnológicos.
- La matriz de inventario de activos de TI debe registrar claramente quienes son los propietarios que los tienen a su cargo.
- Los Custodios de Activos de TI deben velar por la seguridad de los activos que tienen a su cargo de tal manera que garantice el mantenimiento de la confidencialidad, integridad y disponibilidad de la información.
- Los custodios pueden delegar a los usuarios tareas de rutina que se realicen con los activos. Sin embargo, el custodio comparte, con el usuario, la responsabilidad sobre la seguridad del activo.
- Se debe mantener el registro físico o lógico de la formalización de la clasificación asignada a los activos, así como de la responsabilidad de los propietarios y los custodios.

Solución Propuesta

- Procedimiento de elaboración del inventario de activos de TI.
- Procedimiento de actualización y mantenimiento de inventario de activos de TI.
- Implementación de criterios para la definición de los niveles de criticidad de los activos de TI.

Información adicional referente a dicho procedimiento consultar el Anexo M.

Beneficios

- Obtención de la matriz de inventario de activos de TI clasificados.
- Cumplimiento con la asignación de propietarios y custodios de activos de TI.
- Identificación de la criticidad de los activos de TI existentes en la empresa.
- Optimización del control de los activos de TI desde el enfoque de seguridad de la información.
- Input necesario para el análisis y evaluación de riesgos de seguridad de información.

El inventario de activos de información es base de todo el proceso de análisis y evaluación de riesgos, el cual permite la identificación de riesgos de información que asedian al negocio y se puedan tomar las decisiones de acción pertinentes.

4.2.13 Resiliencia y Seguridad Física.

Objetivo

El objetivo principal es definir e implementar protocolos para otorgar, limitar y revocar el acceso al Centro de Cómputo y diseñar e implementar medidas de protección contra factores ambientales.

Alcance

- Controlar el acceso al Centro de Cómputo.
- Minimizar interrupciones del servicio como consecuencia del monitoreo de los controles ambientales del Centro de Cómputo.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS12 Administración de Ambiente Físico" sin avance (0%) de acuerdo a la tabla 1, identificando las siguientes carencias:

- El centro de cómputo no lleva controles de accesos físicos adecuados.
- Las autorizaciones no se encuentran claramente definidas.

Solución Propuesta

- Procedimiento de monitoreo de controles ambientales y físicos del Centro de Cómputo.

- Lineamientos de uso del Centro de Cómputo.

Información adicional referente a dicho procedimiento consultar el Anexo N.

Beneficios

- Monitoreo y control adecuado en el Centro de Cómputo.
- Aprobación formal de ingresos.

4.2.14 Gestión de Seguridad en Plataforma

La presente gestión identifica tres campos a cubrir:

- Actualización de Antivirus.
- Seguridad Perimetral.
- Actualización de Parches de Seguridad.

Objetivo

Proteger la integridad de la información, mediante controles preventivos como la actualización de parches y la detección sobre el uso de software de procedencia dudosa, virus y otros similares. A nivel perímetro de red se debe proteger a todos los activos de información que se encuentren expuestos a redes externas.

Alcance

Es todo activo de información definido en la organización, como laptops, servidores y equipos de seguridad y comunicaciones.

Situación Actual

De acuerdo al nivel de madurez 4 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS5 Garantizar la Seguridad de los Sistemas" con un avance del 16.67% de acuerdo a la tabla 1, identificando las siguientes carencias:

- Los equipos deben contar con el antivirus actualizado, teniendo especial consideración sobre los equipos que almacenan o procesan información crítica y sensible.
- Se debe aplicar las políticas y enfrentar de manera sencilla las complejidades del despliegue del software y de los parches de seguridad.
- El usuario es el responsable de respetar y cumplir los lineamientos de seguridad de información establecidos en la organización.

- Se debe mantener actualizado el sistema operativo y todas sus aplicaciones con los últimos parches de seguridad.
- Se deben definir los mecanismos de protección (antivirus, parches etc.) requeridos por la organización.
- Todo software debe ser actualizado constantemente para mitigar algún tipo de incidente de seguridad.
- Todo software deben ser instalados de forma autorizada para evitar infección de códigos maliciosos.
- Todo tráfico externo a la red debe ser mediado adicionalmente de los firewalls, con IPS que mitiguen algún tipo de incidente., estos dispositivos deben estar constantemente monitoreados mediante un dispositivo de correlación de eventos.

Solución Propuesta

- Procedimiento de antivirus.
- Procedimiento de seguridad perimetral.
- Procedimiento de actualización de parches.

Información adicional referente a dicho procedimiento consultar el Anexo Ñ.

Beneficios

- Contar con controles internos como externos que minimicen el impacto ante incidente de seguridad.
- Minimiza vulnerabilidades en el software.
- Evita ataques de códigos maliciosos
- Mantiene un registro de parches.
- Firma de aceptación de riesgos.
- Permite disponer de aplicaciones seguras y resistentes a las intrusiones.

4.2.15 Gestión de Niveles de Servicio

Objetivo

Es asegurar que todos los servicios TI actuales y previstos se entreguen conforme a los objetivos de servicios fijados y alcanzables. Esto se consigue mediante un ciclo constante de negociación, acuerdos, supervisión, presentación de informes, revisión de los objetivos de los servicios TI y sus respectivos logros, por medio de acciones que intentan corregir o mejorar el nivel de servicio entregado.

Alcance

El proceso empieza con la determinación de los requerimientos del negocio, pasando por la elaboración y/o revisión de acuerdos escritos tales como SLAs, OLAs y UCs, monitoreo de los cumplimientos de los acuerdos y finaliza cuando se efectúa la revisión para fijar las y mejoras de los acuerdos para lograr mayores niveles de servicio.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS1 Definir y Administrar los Niveles de Servicio" con un avance del 50% de acuerdo a la tabla 1, identificando las siguientes carencias:

- Falta una administración formal de los niveles de servicio.
- No se actualiza con los nuevos servicios.
- No se realiza revisiones periódicas de los servicios.
- Falta de un monitoreo que permita ser proactivo.
- Identificación de los nuevos servicios TI o los modificados satisfacen realmente los SLRs del cliente.
- La Gestión del Nivel de Servicio también es responsable de asegurar que todos los objetivos de los SLAs están respaldados por los respectivos OLAs "Operational Level Agreement" y UCs "Underpinning Contracts".

Información adicional referente a dicho procedimiento consultar el Anexo O.

Solución Propuesta

- Procedimiento de Gestión de Niveles de Servicio.
- Procedimiento de Definición y Actualización de los Servicios.
- Procedimiento de la implementación del Servicio.
- Procedimiento de Servicio de Administración de Portafolio – Revisión Anual
- Procedimiento de Monitoreo de los Niveles de Servicio.

Beneficios

- Provee los servicios TI que cumplen lo establecido en los SLAs.
- Los nuevos servicios TI o los modificados satisfacen realmente los SLRs del cliente.
- El catálogo de servicios TI del negocio recibe un soporte acreditado tanto por los servicios TI técnicos garantizados por los OLAs definidos entre el personal TI como por los UCs firmados con los proveedores externos.
- Mayor control de los procesos y monitoreo del servicio.
- Optimización de los recursos disponibles.

4.2.16 Gestión de Mesa de Ayuda

Objetivo

El objetivo principal de la mesa de ayuda es brindar un único punto de contacto entre el proveedor de los servicios TI y los usuarios.

El personal de la mesa de ayuda se encarga de la atención de las solicitudes de servicio y de los cambios del tipo estándar, con el propósito de restaurar la normalidad del servicio que permita a los usuarios volver a trabajar satisfactoriamente. En este contexto la restauración del servicio se entiende en el sentido más amplio posible.

Alcance

El proceso empieza con la determinación de las necesidades del negocio, pasando por la elaboración de acuerdos escritos, seguimiento y verificación de los cumplimientos de los acuerdos y finaliza con la revisión y mejoras de los acuerdos para lograr mayores niveles de servicio.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS8 Administrar la Mesa de Servicio y los Incidentes" con un avance del 35.71% de acuerdo a la tabla 1, identificando las siguientes carencias:

- Mejorar la calidad y la más rápida respuesta a las solicitudes de los usuarios.
- Mejorar de la comunicación y el trabajo en equipo.
- Mayor atención y un enfoque proactivo en la prestación de servicios.
- Falta una reducción del impacto negativo en el negocio.
- Mayor control y gestión de la infraestructura.
- Mejor uso de los recursos de soporte TI y aumento de la productividad del personal administrativo.

Información adicional referente a dicho procedimiento consultar el Anexo P.

Solución Propuesta

Procedimiento de Mesa de Ayuda que contemple:

- Percepción y satisfacción mejorada respecto a la prestación del servicio.
- Aumento de la accesibilidad, de la comunicación y de la información a través de un único punto de contacto.
- Gestión de la información más significativa en el soporte de las decisiones.

4.2.17 Gestión de Catalogo de Servicio

Objetivo

Mantener controlado y actualizado el catálogo de servicios del área de TI que es uno de los elementos más importantes en el enfoque integral de la prestación de los servicios de TI.

Alcance

La gestión del catálogo de servicios empieza cuando el canal de entrada de servicios le transfiere un nuevo servicio versionado y queda a decisión del Gestor del Catálogo ponerlo en operación y finaliza cuando el servicio es dado de baja.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio "Delivery and Support" "DS1 Definir y Administrar los Niveles de Servicio" con un avance del 50 % de acuerdo a la tabla 1, identificando las siguientes carencias:

- Todo nuevo servicio será incorporado en el Catálogo de Servicios cuando haya realizado la prueba de disponibilidad del servicio y los aprobadores involucrados manifiesten por escrito su aceptación.
- Todo servicio será dado de baja del Catálogo de Servicios cuando haya vencido la prueba de disponibilidad del servicio que lo sustituirá y los aprobadores manifiesten por escrito la aceptación y la baja del servicio respectiva.
- Toda propuesta para un nuevo servicio deberá ser iniciada a través del proceso de Gestión del Cambio y luego incorporada en el Portafolio de Servicios.
- El proceso debe producir y mantener el catálogo de servicios, garantizando que se proporciona una fuente central, precisa y coherente de datos, que lleva un registro de todos los servicios operativos o servicios que están en vías de ingresar al entorno de producción, junto con los datos correspondientes de cada servicio.

Información adicional referente a dicho procedimiento consultar el Anexo Q.

Solución Propuesta

Procedimiento de Gestión del Catálogo de Servicio, el catálogo de servicios es la fuente central de información de los servicios TI prestados por un proveedor de servicios. Esto asegura que cada área de la empresa puede ver una y solo una, imagen precisa y consistente de los servicios TI con sus detalles y su estado. Incluye una vista de cara al cliente de los servicios TI también denominada Catálogo de Servicios TI del Negocio, tales servicios que serán utilizados por los procesos de negocio de acuerdo a los niveles de servicio fijados.

Beneficios

- El catálogo de servicios es único para toda la empresa.
- Es actualizado una vez al año, excepto que la autoridad TI decida lo contrario.

4.2.18 Gestión de Proveedores de TI

El objetivo principal de la gestión de proveedores externos TI es obtener valor por el dinero que se les paga y brindar servicios TI de calidad al negocio, asegurando que tanto los contratos como los acuerdos con proveedores apoyan los requerimientos de la empresa y que cada uno de los proveedores cumple con sus compromisos contractuales.

Los objetivos específicos del proceso de la gestión de proveedores son:

- Obtener la mejor relación calidad-precio de los proveedores y de los contratos.
- Asegurar que los contratos con los proveedores, están alineados con las necesidades del negocio y que apoyan y están alineados con los objetivos acordados en los SLAs en conjunto con la Gestión de los Niveles de Servicio.
- Gestionar las relaciones con los proveedores considerando la gestión de desempeño del proveedor.
- Negociar y acordar los contratos con los proveedores y gestionarlos durante su vigencia o ciclo de vida.
- Mantener una política de proveedores, un soporte del proveedor y un sistema de información de gestión de contratos.

Alcance

El proceso de la gestión de proveedores TI externos se inicia desde que se convoca a los interesados en participar en la selección de proveedores, durante un periodo específico, para así poder participar tanto en invitaciones, concursos y licitaciones que la empresa efectúe y finaliza cuando se realiza el contrato/ejecución de servicio.

Resultados Relevantes

- Garantiza que todos los objetivos en que se basan los contratos y acuerdos con los proveedores están alineados con las necesidades del negocio y los objetivos fijados en los SLAs.
- Asegura la entrega de servicios TI de calidad que están alineados con las expectativas del negocio.
- Se alinea con todos los requerimientos corporativos y con las condiciones de los demás procesos de la gestión servicios TI, en particular con la Gestión de la Seguridad de la Información y la Gestión de la Continuidad de los Servicios TI.

Esto asegura que los resultados que el negocio obtiene dependen del valor generado por cada uno de los servicios prestados por los proveedores, que definitivamente están alineados con las necesidades del negocio.

La gestión de los principales proveedores de TI se define de acuerdo a la siguiente matriz:

Tabla 4 Gestión de Proveedores de TI.

Empresa / SLA - atributos	Contrato Vigente	Especificaciones del SLA: Formuló un SLA específico	Alcance	Horario de atención	Disponibilidad	Confiabilidad	Atención al cliente/usuario	Punto de contacto	Informe de Rendimiento	Informe de Funcionalidad	Gestión del cambio	Continuidad del servicio	Seguridad	Responsabilidad	Informes	Resolución de Contrato a favor
IBM **Servicio de Mantenimiento de Hardware**	Si	No	Si	Si	No	Si	Si	Si	No	No	Si	Si	Si	Si	No	No
Lightech **Monitoreo de dispositivos y determinanción de problemas**	Si	No	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
COSAPI SOFT S.A. **Mantenimiento de Software**	D	No	Si	Si	No	No	Si	Si	No	No	No	No	No	Si	No	No
COSAPI DATA **Centro de Servicios TI**	Si	No	Si	Si	Si	No	Si	Si	Si	No	Si	Si	Si	No	No	No

D: Desconocido

Fuente: Elaboración propia.

4.2.19 Gestión de Configuración de Servidores Críticos

Objetivo

El objetivo específico es definir y controlar los componentes de los servicios y la infraestructura TI y mantener la información precisa de la configuración de los servicios y de la infraestructura TI, incluyendo la situación histórica, desde la planificada hasta la actual.

Este procedimiento incluye la recolección de la información de la configuración inicial, el establecimiento de las normas, la verificación y la auditoría de la información de la configuración y la actualización del repositorio de configuración de acuerdo a lo que se necesite.

Una efectiva gestión de la configuración facilita una mayor disponibilidad, minimiza los problemas de los servicios y activos en producción y resuelve los problemas más rápido.

En resumen la gestión de los elementos configurables se orienta a:

- Proporcionar un apoyo eficiente y eficaz a los procedimientos de la gestión de servicios, generando información precisa de la configuración para que el personal pueda decidir en el momento adecuado.
- Minimizar el número de problemas de calidad y de cumplimiento causados por la configuración inadecuada de los servicios y activos.
- Optimizar los activos de servicios TI, configuraciones, competencias y recursos.

Alcance

El procedimiento de la Identificación y mantenimiento de elementos configurables comienza con una solicitud de cambio, para incorporar un nuevo elemento de configuración o modificarlo en la CMDB, pasando por una revisión del Propietario del Activo, cuando sea necesario los riesgos serán evaluados por el Oficial de Seguridad de la Información que emitirá un Informe de Riesgos, para que Propietario del Activo decida si el Custodio actualiza la CMDB, hecho que tendrá que ser comprobado por el Administrador del Cambio.

El alcance no considera la gestión de los activos financieros.

Situación Actual

De acuerdo al nivel de madurez 3 requerido para el presente control se identificó en el dominio “Delivery and Support” “DS9 Administrar la configuración” con un avance del 60 % de acuerdo a la tabla 1, identificando las siguientes carencias:

- Una mejor previsión y planificación de los cambios.
- Los cambios y las versiones pueden ser evaluados y planificados para ser realizados con éxito.
- La capacidad para determinar los costos de un servicio.

Información adicional referente a dicho procedimiento consultar el Anexo R.

Solución Propuesta

Elaboración del Procedimiento de Gestión de Configuración de Servidores Críticos que contemple:

- Los incidentes y los problemas son resueltos conforme a los objetivos de nivel de servicio.
- Los niveles de servicio y garantías son objetivamente entregados.
- Se determina la trazabilidad de los cambios basándose en los requisitos.

4.3 Relevamiento e Identificación de Controles Claves de TI

4.3.1 Relación de Controles por Aplicativo

Antecedentes

Se elaboró un "Checklist de Controles por aplicativo" alineado al objetivo de control Cobit "AI2.3 Control y Posibilidad de Auditar las Aplicaciones", por lo que se han identificado un conjunto de aspectos que rigen el funcionamiento de la aplicación.
Para el presente trabajo no se utilizó el formato que posee AFP llamado "CheckList Seguridad Información – APP".

Análisis

Se han evaluado 10 aplicaciones por ser consideras críticas y encontrarse dentro del alcance de SOX.

Tabla 5 Aplicaciones a Evaluar.

APLICACIÓN	DETALLE	PLATAFORMA
Acreditación	Acreditación	AS/400
Beneficios y Pensiones AFP	Beneficios y Pensiones AFP	AS/400
Módulo Comercial	Módulo Comercial	AS/400
Módulo de Traspasos	Módulo de Traspasos	AS/400
Recaudo	Recaudo	AS/400
Rezagos	Rezagos	AS/400
Contabilidad Multifondos	Caja Bancos	Cliente/servidor
Contabilidad Multifondos	Contabilidad	Cliente/servidor
Sistema de Inversiones	Inversiones	Cliente/servidor
Gestión de RRHH	RRHH	Cliente/servidor

Fuente: Elaboración propia.

Criterios del Checklist

A continuación se detalla los criterios de las verificaciones utilizadas y los escenarios de riesgos que buscan identificar:

Tabla 6 Criterios del Checklist.

Criterio	Detalle	Escenarios de riesgo que mitiga
Controles Manuales	Acciones de verificación que se realizan fuera de la aplicación	Cubre los riesgos que requieren juicio de una persona
Controles en la implementación del negocio	Requerimientos del negocio específicos sobre su proceso, que rigen como debería funcionar el aplicativo	Cubre límites de operación, aplicación de normas y acciones de cumplimiento
Controles automatizados en la aplicación		
Autorización y Escalamiento	Acciones de escalamiento y autorización, bien sea de pares o de un superior	Cubre los riesgos relacionados con segregación de funciones y fraude
Ingreso	Validaciones que se realizan al momento del registro de la información sean manuales o automáticas	Cubre los errores operativos al momento de ingreso
Procesamiento de datos	Lógica automática que se realiza para generar información a partir de la información ingresada	Cubre riesgos relacionados a manipulación de la información
Salida de datos	Validaciones que se realizan a las salidas de la aplicación, sean manuales o automáticas	Cubre errores que pudieron realizarse en el aplicativo
Pistas de auditoria	El registro de quien, cuando y como se modificó un registro importante	Permite mantener trazabilidad de la operación
Integridad de datos	Validaciones internas del aplicativo para asegurar que los datos son del tipo y rango válidos, así mismo que sean consistentes con otros datos relacionados.	Cubre riesgos relacionados a manipulación de la información
Matriz de roles de usuarios	Como se encuentran definido los accesos	Cubre riesgos relacionados a la eficacia de cómo se brindan los accesos
Controles de Integridad de la BD	Validaciones propias a nivel de la base de datos para asegurar la consistencia de la información	Cubre riesgos relacionados a manipulación de la información
Controles de actualización de la documentación		
Manuales y documentación del aplicativo	La existencia de los manuales para operar y brindar soporte	Cubre riesgos relacionados a la imposibilidad de dar soporte al aplicativo
Manuales y documentación de condiciones especiales únicas y personalización	La existencia de los manuales elaborados por modificaciones	Cubre riesgos relacionados a la imposibilidad de dar soporte al aplicativo
Hardening de plataforma		
Pistas de auditoría del Sistema Operativo	Si se cuenta con información para poder identificar cambios no autorizados en la plataforma	Permite mantener trazabilidad de la operación
Control de Accesos		
Revisión de la Matriz de roles de usuarios	Frecuencia de revisión de los accesos	Cubre los riesgos de usuarios con accesos no vigentes/autorizados

Fuente: Elaboración propia.

Resumen de la Evaluación

Se recolecto la información sobre las 10 aplicaciones, quedando de la siguiente forma:

Tabla 7 Resumen de la Evaluación.

Control	App con el control	No aplica	No cuenta
Controles Manuales (1)	5	-	-
Controles en la implementación del negocio (1)	7	-	-
Autorización y Escalamiento	3	3	4
Ingreso	10	-	-
Procesamiento de datos	9	-	1
Salida de datos	10	-	-
Pistas de auditoria	7	2	1
Integridad de datos	9	-	1
Matriz de roles de usuarios	7	3	-
Controles de Integridad de la BD	8	-	2
Manuales y documentación del aplicativo	10	-	-
Manuales y documentación de condiciones especiales únicas y personalización	10	-	-
Pistas de auditoría del Sistema Operativo	10	-	-
Revisión de la Matriz de roles de usuarios	7	3	

Fuente: Elaboración propia.

4.3.2 Checklist de Seguridad de Proveedores Críticos

Debido a que las organizaciones buscan proveedores confiables que les permita dar soporte a la cadena de valor de la organización es necesario una evaluación rigurosa como se puede apreciar en las siguientes tablas:

Vista general de matriz de evaluación de Infraestructura TI

Tabla 8 Checklist de Proveedores Críticos.

	Descripción de evaluaciones		Pesos
1	Evaluación Empresa		20%
		Tiempo Compañía	3%
		Tamaño	3%
		Clientes	3%
		Experiencia	4%
		Respaldo Financiero	4%
		Conocimiento de nuestra infraestructura	3%
		Cuenta con personal certificado en el servicio propuesto	
2	Evaluación Técnica		40%

	2.1	<A.1: Hardware >		30%
			Equipos marca reconocida por Gartner	
			Configuración solicitada	
	2.2	<A.2: Sofware de Sistemas>		
			Casa de software reconocida	
			Configuración solicitada	
			Soporte y licenciamiento	
	2.3	<A.3: Red>		
			Equipos marca reconocida	
			Configuración solicitada	
	2.4	A.4: Servicios		10%
			Alcance solicitado	5%
			Soporte y niveles de servicio	5%
3	Evaluación de Propuesta			20%
		Plazos de entrega		5%
		Garantia de equipos		5%
		Valor agregado		5%
		Soporte y Matenimiento		5%
		Horario de atención		
4	Evaluación Económica			20%
		Precio		10%
		Condiciones de pago		10%
		Resolución de contrato favorable a la empresa		
			Total	100%

Fuente: Elaboración propia.

Tabla 9 Zonas de dominio Técnico para evaluación de Adquisiciones TI

<A.1: Hardware>: A.1.1 : Equipos de cómputo A.1.2 : Equipos de Almacenamiento A.1.3 : Equipos Telefonía A.1.4 : Partes de Hardware A.1.5: Equipos de Respaldo A.1.6: Dispositivos de Seguridad	**<A.2: Software de Sistemas>:** A.2.1: Software de Base de Datos A.2.2: Software de Virtualización A.2.3: Software de Replicación A.2.4: Software Middleware A.2.5: Software para Servicio Web A.2.6: Software para Archiving A.2.7: Software para Contenido A.2.8: Software de Monitoreo
<A.3: Red>: A.3.1: Dispositivos de Red	**<A.4: Servicios>:** A.4.1: Servicio de Mesa de Ayuda

A.3.2: Dispositivos de control de redes A.3.3: Medios de transmisión de red	A.4.2: Servicio de Consultoría TI A.4.3: Servicios de Datacenter A.4.4: Servicios de Conectividad A.4.5: Servicios de Cloud Computing A.4.6: Servicios de Implementación A.4.7: Servicios de Configuración

Fuente: Elaboración propia.

Tabla 10 Resumen Dominio Técnico.

	Pesos	DELL	HP	IBM
Evaluación de Empresa	20%	0	0	0
Evaluación Técnica	40%	0	0	0
Evaluación de Propuesta	20%	0	0	0
Evaluación Económica	20%	0	0	0
		0	**0**	**0**

Fuente: Elaboración propia.

Tabla de Valores

Tabla 11 Parámetros de Evaluación Empresa

Parámetros de Evaluación Empresa		
Tiempo	0	< 3 años
	1	entre 3 y 6 años
	3	> 6 años
Tamaño	0	< 50 empleados
	1	entre 50 y 150 empleados
	3	> 150 empleados
Clientes	0	No tiene clientes del rubro
	1	Tiene pocos clientes del rubro
	3	Tiene clientes del rubro
Experiencia	0	< 3 años
	2	entre 3 y 6 años
	4	> 6 años
Respaldo Financiero	0	No tiene respaldo financiero
	2	Tiene poco respaldo

	4	Tiene respaldo
Conocimiento	0	No tiene conocimiento de nuestra infraestructura
	1	Tiene poco conocimiento de nuestra infraestructura
	3	Tiene conocimiento de nuestra infraestructura

Fuente: Elaboración propia.

Tabla 12 Parámetros de Evaluación de Propuestas.

Parámetros de Evaluación Propuesta		
Plazos de entrega	0	Mayor plazo de entrega
	3	Plazo de entrega intermedio
	5	Menor plazo de entrega
Garantía de equipos	0	No tiene garantía
	3	Tiene poca garantía
	5	Tiene garantía
Valor agregado	0	No tiene valor agregado
	3	Tiene valor agregado
	5	Tiene mucho valor agregado
Soporte y Mantenimiento	0	No tiene mantenimiento
	3	Precio relativamente mayor al presupuestado
	5	Precio dentro de lo presupuestado o menos

Fuente: Elaboración propia.

Tabla 13 Parámetro de Evaluación Técnica.

Parámetro Selección de Evaluación Técnica		
Selección	No	No incluir en evaluación
	Si	Incluir en evaluación

Fuente: Elaboración propia.

Tabla 14 Parámetros de Evaluación Técnica Grupal.

Parámetros Evaluación Técnica HW, SW y Net						
Grupo1	Grupo2	Grupo3	Grupo4	Grupo5	Grupo6	Grupo7
10%	15%	30%				15%
5%	8%	15%				8%
5%	7%	15%				7%
10%	15%		15%		30%	
4%	6%		6%		10%	
4%	6%		6%		10%	
2%	3%		3%		10%	
10%			15%	30%		15%
5%			8%	15%		8%
5%			7%	15%		7%

Fuente: Elaboración propia.

Grupo1: Hw=S, Sw=S, Net=S
Grupo2: Hw=S, Sw=S, Net=N
Grupo3: Hw=S, Sw=N, Net=N
Grupo4: Hw=N, Sw=S, Net=S
Grupo5: Hw=N, Sw=N, Net=S
Grupo6: Hw=N, Sw=S, Net=N
Grupo7: Hw=S, Sw=N, Net=S

Tabla 15 Parámetros de Evaluación Técnica Grupal

Parámetros de Evaluación Técnica				
Grupo1	Hw11	Equipos marca reconocida	0	Marca no conocida
			3	Marca poco conocida
			5	Marca conocida
Grupo2	Hw12	Equipos marca reconocida	0	Marca no conocida
			5	Marca poco conocida
			8	Marca conocida
Grupo3	Hw13	Equipos marca reconocida	0	Marca no conocida
			7	Marca poco conocida
			15	Marca conocida
Grupo7	Hw14	Equipos marca reconocida	0	Marca no conocida
			5	Marca poco conocida
			8	Marca conocida

4.3.3 Checklist de Seguridad del Centro de Cómputo Principal y Alterno.

Tabla 16 Verificación del Centro de Cómputo Principal y Alterno.

Verificación	**Si**	**No**	**Descripción**	**Anual**	**Mensual**	**Perma-nente**	**Monito-reo**
El Área Segura es un ambiente completamente cerrado y restringido su acceso sólo al personal autorizado	X		El área de monitoreo cuenta con un control biométrico, para acceder se sigue el procedimiento de monitoreo de controles ambientales y físicos del Centro de Cómputo			X	
Cuenta con Cámaras de Video	X		Se cuenta con área de monitoreo				X
Solo personal autorizado ingresa al centro de cómputo y se hace uso de la bitácora del centro de computo	X		Según el procedimiento de monitoreo de controles ambientales y físicos del Centro de Cómputo			X	

Verificación	Si	No	Descripción	Anual	Mensual	Perma-nente	Monito-reo
Está dotadas de señalética de seguridad (Zonas seguras, riesgo eléctrico, etc.) y de ingreso solo personal autorizado		X	No se encuentra presente	X			
El personal no ingresa con comida o bebida al centro de cómputo	X		Según el procedimiento de monitoreo de controles ambientales y físicos del Centro de Cómputo			X	
No se permite el uso equipos de fotografía, video u otras formas de registro a realizarse por terceros	X		Según el procedimiento de monitoreo de controles ambientales y físicos del Centro de Cómputo			X	
Las labores de realizadas por terceros son supervisadas	X		Supervisado por el personal previamente autorizado, según el procedimiento de monitoreo de controles ambientales y físicos del Centro de Cómputo			X	
Los terceros que realicen trabajos de riesgo cuentan con el Seguro complementario de trabajo de riesgo		X	No es solicitado			X	
Es suficientemente amplia	X		El ambiente es amplio para ingresar y maniobrar un servidor	X			
No existen elementos combustibles en el interior (pila de papeles, cartón, etc.)	X		Se identificó cajas de cartón en el área de monitoreo				X
Áreas de carga y descarga de insumos y suministros de cómputo se encuentren en ambientes separados	X			X			
Están lejos de instalaciones de agua y desagüe	X		No hay baño o kitchen próximo	X			
Equipos protegidos del polvo	X		Los equipos se encuentran en gabinetes		X		
Cuenta con detectores de humo/fuego	X		Ubicados en el techo	X			
Cuenta con detectores de temperatura y temperatura acorde de funcionamiento	X		Cuentan con 3 termómetros distribuidos en el centro de cómputo				X
Detectores de agua/humedad y humedad acorde de funcionamiento	X		Debajo del piso falso				X
Cuenta con equipos de aire acondicionado de precisión	X		Cuenta con uno de precisión y como respaldo uno de confort	X			

Verificación	Si	No	Descripción	Anual	Mensual	Perma-nente	Monito-reo
Cuenta con extintores adecuados para el control de incendios de origen eléctrico	X		Cuenta con extintores basados en Halotron	X			
Los Gabinetes están anclados al piso y techo		X	Los gabinetes solo están con frenos, en sismos fuertes se podrían desplazar	X			
Los equipos están instalados como mínimo a 20 centímetros sobre el nivel del piso para hacer frente a inundaciones		X	El piso falso está a 15cm, por lo que algunos equipos que se encuentran en la parte inferior del gabinete están expuestos, en especial el UPS	X			
Cuenta con circuitos eléctricos y tableros de distribución independientes a cualquier otra conexión	X		Si	X			
En el tablero eléctrico está el directorio de circuitos	X		Si	X			
Los equipos están conectados a dos líneas de corriente, una para la principal y otra para contingencia	X		Es una sola línea la que sale del tablero eléctrico	X			
Cuenta con equipos UPS (Suministro de Energía Ininterrumpida), conectados a los equipos informáticos	X			X			
Cuenta con corriente estabilizada	X		El tablero eléctrico controla los picos y el UPS estabiliza		X		
Se cuenta con Grupo Electrógeno conectado a los equipos, verificando periódicamente su operatividad	X		Hacen uso del equipo electrógeno independiente del edificio	X			
La edificación cuenta con Luces de Emergencia	X		El edificio cuenta con luces de emergencia	X			
Cuenta con línea de puesta a Tierra y pozo de tierra	X		Hacen uso de pozo a tierra del edificio	X			
No hay sobrecarga del cableado eléctrico, ni tampoco carga adicional en los tableros eléctricos.	X				X		
El cableado de datos y telefonía se encuentra empotrado o en canaletas		X	El cableado en los gabinetes de comunicaciones están enredados	X			

Verificación	Si	No	Descripción	Anual	Mensual	Perma-nente	Monito-reo
Los cables de la red eléctrica y de comunicaciones están separados para evitar interferencias.	X			X			

Fuente: Elaboración propia.

4.3.4 Documento de Roles y Responsabilidades

Matriz de Segregación de funciones

Objetivo
Servir como referencia para la identificación de conflictos entre los roles existentes a la fecha en las áreas de TI de la organización.

Consideraciones
Esta matriz se ha realizado en base criterios de alto nivel. Se usa como referencia el marco de trabajo de COBIT 4.1.

No se sustenta en un análisis de riesgos previamente realizado.

Tabla 17 Consideraciones de Roles y Responsabilidades.

Pregunta "LLAVE"	¿El Rol A pueden ser asumido sin conflicto de seguridad por el Rol B o viceversa? (Donde "A" son las columnas y "B" son las filas.)
Leyenda	Definiciones
C= Sí hay Conflicto	Cuando si guardan alguna relación pero no es conveniente por temas de seguridad de la información que un Rol realice actividades de otro Rol.
NC= No hay Conflicto	Cuando si guardan alguna relación y es indistinto que por temas de seguridad de la información que un Rol realice actividades de otro Rol.
NA= No Aplica	Cuando no guardan una relación. Por ejemplo un rol de un área "A" comparado contra un área "B".

Fuente: Elaboración propia.

Tabla 18 Descripción de los Niveles.

Descripción de los Niveles	
Nivel	**Descripción**
5	Rol de nivel gerencial con capacidad de toma de decisiones estratégicas.
4	Roles de nivel sub-gerencial.
3	Rol de nivel jefatural. Capacidad de tomas de decisiones tácticas. Con personal a cargo.
2	Rol de nivel ejecutivo. Responsabilidades administrativas y con capacidad de tomas de decisiones operativas.
1	Rol de carácter operativo. Ejecuta tareas de rutina e instrucciones.
Cross	Son roles colectivos. Pueden estar dentro de este grupo varios niveles jerárquicos.
Externo	Se refiere a personas o entidades que no pertenecen a la organización.
Área	Tipo de rol que abarca todas las personas de un unidad organizacional denominada "área"
Grupo de trabajo	Rol colectivo que puede estar conformado por diferentes niveles jerárquicos según se requiera. Y esta funciona cuando este está constituido y activo. Un Rol de Persona si bien puede formar parte de un Grupo de Trabajo, no puede ejercer de manera individual una actividad que a éste le corresponde.

Fuente: Elaboración propia.

Criterios	Tema	Definición
1	Cruce de roles	Un Rol de ÁREA no se pude comparar contra el Rol de una Persona
2	Cruce de roles	Un Rol de GRUPO DE TRABAJO no se pude comparar contra el Rol de una Persona
3	Cruce de roles	Si bien un Rol de Persona puede tener conflicto con un Rol de Grupo de Trabajo no evita que éste forme parte del dicho Grupo de Trabajo. Por ejemplo: Un Proveedor si puede pertenecer al "Grupo de resolución N° 3" pero no puede asumir sus actividades como tal
4	Cruce de roles	La actividad de un Rol Colectivo no cruzará con la actividad de un Rol de Persona y viceversa.
5	Dueño del aplicativo	Se refiere sólo a los aplicativos del área usuaria
6	Propietario de la información	Se refiere sólo a la información del área usuaria
7	Nivel del Rol	El Rol de una persona solo puede ejecutar un nivel de rol superior o inferior al nivel de su Rol por encargatura
8	Responsabilidad	Un Rol de área no puede aceptar una responsabilidad
9	Responsabilidad	Un Rol de Grupo de Trabajo puede aceptar una responsabilidad, Ej. Comité de Seguridad

Fuente: Elaboración propia.

Tabla 19 Criterios

Tabla 20 Segregación de Funciones.

	N°	1	2	3	4	5	6	7
	Nivel	1	1	3	3	4	2	2
N°	**Nivel**	Roles	Analista de sistemas	Operador de Infraestructura tecnológica	Gestor de proyectos de infraestructura	Gestor de infraestructura tecnológica	Sub gerente de servicios de sistemas	Ejecutivo senior de infraestructura - servidores	Ejecutivo senior - BD
1	1	Analista de sistemas	-	C	NA	NA	NA	C	C
2	1	Operador de Infraestructura tecnológica	C	-	NA	NA	NA	NC	NC
3	3	Gestor de proyectos de infraestructura	NA	NA	-	NC	NC	NC	NC
4	3	Gestor de infraestructura tecnológica	NA	NA	NC	-	NC	NC	NC
5	4	Sub gerente de servicios de sistemas	NA	NA	NC	NC	-	NA	NA
6	2	Ejecutivo senior de infraestructura - servidores	C	NC	NC	NC	NA	-	NC

Fuente: Elaboración propia.

4.3.5 Plan de Mitigación de Riesgos

Tabla 21 Organización de TI

Proceso COBIT 4.1	Checklist de Evaluación del Nivel de Madurez del Proceso COBIT 4.1					
PO1 Definir un Plan Estratégico de TI	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.	¿Existe una política que defina cómo y cuándo realizar la planeación estratégica de TI?	Implementar el procedimiento del Plan de mitigación de riesgos	A mediano plazo	1	1	Existen lineamientos a nivel de empresa pero no se sabe acerca de la existencia de un documento.
	¿La planeación estratégica de TI sigue un enfoque estructurado que se documenta y se da a conocer a todo el equipo?	Plan de comunicación de la elaboración y resultados del Plan de Estrategias de TI.	A mediano plazo	1	1	No existe documentación, pero si se dan a conocer los lineamientos de la planeación estratégica.
	¿Es razonablemente sólido el proceso de planeación de TI y garantiza que es factible realizar una planeación adecuada?	Plan de auto-evaluación del proceso Estratégico	A mediano plazo	1	1	Esta basado en reuniones y necesidades de las áreas de negocio.
	¿Se otorga discrecionalidad a gerentes individuales específicos con respecto a la implantación del proceso de planeación estratégica de TI? ¿Existen procedimientos para analizar el proceso?	Elaborar el procedimiento de análisis del proceso de planeación estratégica de TI	A mediano plazo	0	2	
	¿La estrategia general de TI incluye una definición consistente de los riesgos que	Incluir en el proceso de elaboración del Plan Estratégico de TI los	A corto plazo	0	2	No se ha realizado el análisis respecto al cuadrante que define

	la organización está dispuesta a tomar como innovador o como seguidor?	resultados de análisis de riesgos de TI y de Negocio				si se somos innovadores o seguidores.
	¿Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías?	Elaborar un procedimiento para desarrollar los Casos de Negocio, donde se evidencien los riesgos de la no adquisición, a pesar de que hubo una aprobación.	A corto plazo	1	1	Si bien la adquisición de nuevos productos y tecnología, está orientado a la necesidad del negocio, existen ciertas influencias de los recursos humanos, técnicos y financiero para adquirirlas. Por ejemplo casos donde se presupuestó y luego no hubo el dinero suficiente.
	¿Se discute la planeación estratégica de TI en reuniones de la dirección del negocio?	Implementación del procedimiento de analisis del proceso de planeación estratégica de TI	A mediano plazo	2	0	
	TOTAL			6	57.14%	
PO4 Definir los Procesos, Organización y Relaciones de TI	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, y	¿Existen roles y responsabilidades definidos para la organización de TI y para terceros?	Elaborar un plan de revisión de los roles y responsabilidades de TI	A corto plazo	2	0	
	¿La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI?			2	0	
	¿Se define el ambiente de control interno?	Elaborar las políticas de control interno, donde se fijen los periodos de esos controles	A corto plazo	1	1	Parcialmente, se tienen reuniones mensuales de

uno o más comités de dirección, en los cuales participen tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.						seguimiento y se contemplan acciones de auditoría.
	¿Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores?	Elaborar políticas de relación de Terceros o aplicar si se tiene	A corto plazo	0	2	Se contempla cada vez que el caso lo amerite.
	¿La organización de TI está funcionalmente completa?	Elaborar un plan de implementación de los procedimientos que se han elaborado	A corto plazo	1	1	Existe documentos pero falta implantarlo
	¿Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios?	Revisar el MOF y verificar las funciones del personal de TI y la de los usuarios	A mediano plazo	1	1	Se aplicarán mejoras en el 2014
	¿Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos?	Implementar el Plan de Capacitación, en base al procedimiento establecido	A mediano plazo	1	1	El personal requiere ampliar sus conocimientos y competencias certificadas, se ha realizado un análisis del perfil de personal con respecto a sus capacidades con el fin de determinar planes de acción para cubrir las brechas existentes.
	¿Existe una definición formal de las relaciones con los usuarios y con terceros?	Elaborar los SLAs respectivos para cada Área de Negocio, para garantizar la calidad de servicio que los usuarios requieren. Revisar los contratos con la finalidad de lograr mejoras	A corto plazo	1	1	Existe una tendencia de mejora tanto en la formalización de las relaciones con los usuarios (SLAs) como con los terceros (contratos o Ucs), Se tiene formalizado

						mediante los contratos y reglamentos internos.
	¿La división de roles y responsabilidades está definida e implantada?	Plan de revisión de roles y responsabilidades, bajo la matriz RACI, y Matriz de Segregación	A corto plazo	1	1	Se tiene un documento de roles y responsabilidades implementado y se está mejorando.
	TOTAL			10	44.44%	
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
La dirección debe elaborar un marco de trabajo de control empresarial para TI y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.	¿La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares?	Elaboración de Políticas de TI y otras que estén relacionadas con TI e implantarlos, como por ejemplo Políticas de Seguridad de la Información	A mediano plazo	1	1	Existe documentos pero falta implantarlo
	¿El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal? ¿Las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas claves?			2	0	
	¿La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación?			2	0	Se realizan capacitaciones
	¿El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplique de forma rigurosa?			2	0	Se han brindado capacitaciones en SOX a toda la institución

	¿Existe un marco general de desarrollo para las políticas y estándares de control? ¿El monitoreo del cumplimiento de estas políticas y estándares es inconsistente?	Implementar el proceso de monitoreo de políticas y cumplimiento de los estándares de controles de TI.	A corto plazo	1	1	Hay lineamientos para documentar, pero su ejecución no es gestionada de manera centralizada y se encuentra en proceso el monitoreo de controles.
	¿Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas?			2	0	Se encuentran definidos
	TOTAL			10	16.67%	
PO7 Administrar los Recursos Humanos de TI	**Nivel de Madurez Esperado 2 - Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.	¿Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar de hacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado?	Elaborar una política de contratación de personal de TI	A corto plazo	1	1	Los procesos de incorporación de nuevos recursos se realiza en base a una planificación anual, sin embargo si fuese necesario se incorpora el recurso usando otros mecanismos
	¿Se imparte entrenamiento informal al personal nuevo, quiénes después reciben entrenamiento según sea necesario?			2	0	
	TOTAL			3	25.00%	
PO9 Evaluar y Administrar los Riesgos de TI	**Nivel de Madurez Esperado 3 - Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**		**Comentario**
Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El	¿Existe una política de administración de riesgos para			2	0	Cuenta con la politica de la casa

marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.	toda la organización que defina cuándo y cómo realizar las evaluaciones de riesgos?					matriz
	¿La administración de riesgos sigue un proceso definido, el cual está documentado?			2	0	
	¿El entrenamiento sobre administración de riesgos está disponible para todo el personal?			2	0	Se cuenta con videos de riesgo operativo disponibles para el personal de la empresa
	¿La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo? (1)			2	0	Es obligatorio y se generan una constancia de la capacitación
	¿La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados?			2	0	La gestión de riesgos corporativo debe ser única, y lo que debe existir diversos análisis según la naturaleza del riesgo.
	¿Por lo general, un proceso para mitigar los riesgos claves se institucionaliza una vez que los riesgos se identifican?			2	0	Si bien es cierto que existen controles, pero no hay una identificación de los riesgos para que puedan ser institucionalizados
	¿Las descripciones de puestos consideran las responsabilidades de administración de riesgos?	Definir las responsabilidades de al administración de riesgos, como por ejemplo el propietario de riesgos	A mediano plazo	1	1	Difundir bien las responsabilidades de los riesgos a todo nivel de la empresa.
	TOTAL			13	7.14%	

AI6 Administrar los cambios	Nivel de Madurez Esperado 4 - Preguntas	Plan de mitigación de riesgos	Tiempo de implementación	Calificación	Brecha	Comentario
Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.	¿El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas?			2	0	Está en plena mejora
	¿El proceso es eficiente y eficaz, pero se basa en considerables procedimientos manuales y controles para asegurar que la calidad se logra?			2	0	
	¿Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción?			2	0	Existen ordenes de cambio donde se consideran los criterios
	¿Se da un proceso de aprobación para cambios?			2	0	Validado por el administrador de cambios
	¿La documentación de administración de cambios está vigente y es correcta, con seguimiento formal a los cambios?			2	0	Validado por el administrador de cambios
	¿La documentación de configuración es generalmente exacta?			2	0	Validado por el administrador de cambios
	¿La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad			2	0	Validado por el administrador de cambios

	del negocio?					
	¿Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio?	Incluir en el plan de sensibilización la integración de TI con el Área de Negocio	A mediano plazo	1	1	Cada vez es más comprendida los beneficios de trabajar en conjunto.
	¿Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios?			2	0	Se realizan reuniones mensuales de los servicios en los cuales presentan sus informes
	TOTAL			17	5.56%	
ME1 Monitorear y Evaluar el Desempeño de TI	**Nivel de Madurez Esperado 2 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.	¿Se han identificado algunas mediciones básicas a ser monitoreadas?			2	0	Si se han identificado en la matriz SUAM
	¿Los métodos y las técnicas de recolección y evaluación existen? ¿Los procesos no se han adoptado en toda la organización?			2	0	Existen los métodos y las técnicas de recolección, no obstante la mayoría son manuales
	¿La interpretación de los resultados del monitoreo se basa en la experiencia de individuos clave?	Elaborar un procedimiento de supervisión, análisis y mejora de los proceso de TI	A corto plazo	1	1	En la mayoría de los casos
	¿Se seleccionan y se implantan herramientas limitadas para recolectar información, pero esta recolección no se basa en un enfoque planeado?			2	0	Se apoyan en el servicio del SOC y el correlacionador que les proporciona
	TOTAL			7	12.50%	
ME2 Monitorear y Evaluar el Control Interno	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Establecer un programa de control interno efectivo para TI requiere un proceso bien	¿La gerencia apoya y ha institucionalizado el monitoreo			2	0	Apoyado por la alta

definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las autoevaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.	del control interno?					gerencia
	¿Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo de control interno?			2	0	Solo se ha elaborado lineamientos y procedimientos y relacionados a la matriz corporativa.
	¿Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno?	Elaborar el plan de control interno	A corto plazo	0	2	Se encuentra en etapa de planificación
	¿Se ha definido un proceso para autoevaluaciones y revisiones de control interno, con roles definidos para los responsables del negocio y de TI?	Implementar el plan de auto-evaluaciones	A corto plazo	0	2	El documento se encuentra en elaboración
	¿Se usan herramientas, aunque no necesariamente están integradas en todos los procesos?	Implementar el proceso de gestión de evidencias, y automatizar en forma gradual la generación de evidencias	A mediano plazo	0	2	No se cuenta con una herramienta estandarizada que permita la integración del cumplimiento de los controles
	¿Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI?			2	0	
	¿Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos?			2	0	De la casa Matriz
	TOTAL			8	42.86%	
ME3 Garantizar el Cumplimiento con Requerimientos Externos	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Una supervisión efectiva del cumplimiento regulatorio requiere del establecimiento de	¿Se han desarrollado, documentado y comunicado			2	0	Se trata de cumplir con lo normado por

un proceso independiente de revisión para garantizar el cumplimiento de las leyes y regulaciones. Este proceso incluye la definición de una declaración de auditoría, independencia de los auditores, ética y estándares profesionales, planeación, desempeño del trabajo de auditoría y reportes y seguimiento a las actividades de auditoría. El propósito de este proceso es proporcionar un aseguramiento positivo relativo al cumplimiento de TI de las leyes y regulaciones.	políticas, procedimientos y procesos para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizás no se sigan y algunas quizás estén desactualizadas o sean poco prácticas de implementar?					la SBS y con proveedores
	¿Se realiza poco monitoreo y existen requisitos de cumplimiento que no han sido resueltos?			2	0	
	¿Se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y se instruye respecto a los procesos de cumplimiento definidos?			2	0	
	¿Existen contratos pro forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales?			2	0	Si cuentan con los formatos en su política de socios de negocio
	TOTAL			8	0	
ME4 Proporcionar Gobierno de TI	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de	¿La importancia y la necesidad de un gobierno de TI se reconocen por parte de la gerencia y se comunican a la organización?	Elaborar las Políticas Corporativas y comunicarlas	A corto plazo	1	1	Se tiene una iniciativa regional de desarrollo de una política de gobernabilidad de TI
acuerdo con las estrategias y objetivos empresariales.	¿Un conjunto de indicadores base de gobierno de TI se elaboran donde se definen y documentan los vínculos entre las mediciones de resultados y los impulsores del desempeño?	Elaborar un procedimiento de elaboración y seguimiento de los indicadores de Gobierno de TI	A mediano plazo	1	1	Se encuentra definidos y formalizados

	¿Los procedimientos se han estandarizado y documentado?			2	0	
	¿La gerencia ha comunicado los procedimientos estandarizados y el entrenamiento está establecido?	Elaborar el plan de comunicación de los procedimientos estandarizados	A corto plazo	1	1	Esta planeado para el 2014
	¿Se han identificado herramientas para apoyar a la supervisión del gobierno de TI?	Identificar e implementar herramientas para apoyar la supervisión del gobierno de TI	A mediano plazo	0	2	No se cuenta con herramientas
	¿Se han definido tableros de control como parte de los Balanced Scorecard de TI?	Elaborar tableros de control del gobierno de TI	A mediano plazo	0	2	
	¿Se delega al individuo su entrenamiento, el seguimiento de los estándares y su aplicación?	Incluir dentro del programa de capacitación, el conocimiento de estándares	A corto plazo	0	2	Esta planeado para el 2014
	¿Puede ser que se monitoreen los procesos, sin embargo, la mayoría de desviaciones se resuelven con iniciativa individual y es poco probable que se detecten por parte de la gerencia?			2	0	
	TOTAL			7	56.25%	

Fuente: Elaboración propia.

Tabla 22 Ciclo de Vida del Software

Proceso COBIT 4.1	**Checklist de Evaluación del Nivel de Madurez del Proceso COBIT 4.1**					
PO8 Administrar la Calidad	**Nivel de Madurez Esperado 2 - Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.	¿Se establece un programa para definir y monitorear las actividades del Sistema de Administración de la Calidad dentro de TI?	Implementar y monitorear las actividades del Sistema de Gestión de Calidad dentro de TI.	A mediano plazo	0	2	No se cuenta con un sistema para la administración de la calidad, se obtienen resultados relacionados vía otros procesos
	¿Las actividades del Sistema de Administración de la Calidad están enfocadas en iniciativas orientadas a procesos y proyectos, no a procesos de toda la organización?	Implementar y monitorear las actividades del Sistema de Gestión de Calidad dentro de TI.	A mediano plazo	0	2	No se cuenta con un sistema de administración de calidad
	TOTAL			0	100.00%	

Fuente: Elaboración propia.

Tabla 23 Infraestructura Tecnológica

Proceso COBIT 4.1	**Checklist de Evaluación del Nivel de Madurez del Proceso COBIT 4.1**					
AI3 Adquirir y Mantener Infraestructura Tecnológica	**Nivel de Madurez Esperado 3 - Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.	¿Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura de TI?			2	0	Si tienen planes de mantenimiento
	¿El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente?			2	0	
	¿Se planea, programa y coordina el mantenimiento?			2	0	Utilizan ordenes de cambio
	¿Existen ambientes separados para prueba y producción?			2	0	Utilizan ordenes de cambio
	TOTAL			8	0.00%	
AI4 Facilitar la Operación y el Uso	**Nivel de Madurez Esperado 2 - Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la	¿Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo?			2	0	Los documentos son elaborados siguiendo el mismo patrón
	¿No hay un enfoque uniforme para el desarrollo de procedimientos de usuario			2	0	Existe documentación de

infraestructura.	y de operación?					operación que se elabora de acuerdo a necesidad y estilo del especialista
	¿Los individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran?			2	0	Existe documentación de proyectos que se elabora de acuerdo a necesidad y estilo del especialista
	¿Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización?			2	0	Cuentan con procedimientos y base de conocimientos para el soporte al usuario
	¿Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento?			2	0	
	TOTAL			10	00%	
AI7 Instalar y Acreditar Soluciones y Cambios	**Nivel de Madurez Esperado 3 - Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los	¿Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación?			2	0	Cubierto por el procedimiento de gestión de cambios (antiguo y nuevo)
	¿Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto?			2	0	Cubierto por el procedimiento de gestión de cambios (antiguo y nuevo)

sistemas operativos estén en línea con las expectativas convenidas y con los resultados.	¿El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales?			2	0	Se utiliza un instructivo para el pase a producción
	¿La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación? (1)			2	0	No se han presentado los casos
	TOTAL			8	0.00%	
DS1 Definir y Administrar los Niveles de Servicio	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.	¿Las responsabilidades están bien definidas pero con autoridad discrecional?	Plan de implementación de los procedimientos SOX	A mediano plazo	1	1	En el 2014 se aplicará los roles incluidos en los procedimientos de SOX
	¿El proceso de desarrollo del acuerdo de nivel de servicio está en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción del cliente?	Plan de evaluación de los niveles de servicio	A corto plazo	1	1	Existen niveles de servicio estándar, no se evalúan de forma individual
	¿Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar?			2	0	Se encuentran definidos
	¿Las deficiencias en los niveles de servicio están identificadas pero los procedimientos para resolver las deficiencias son informales?	Implementar los procedimientos de niveles de servicio	A corto plazo	0	2	Son de reciente aplicación, aun no se tiene resultados

	¿Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado?	Incluir en el procedimiento de niveles de servicio (cuadro de servicio esperado vs presupuesto)	A corto plazo	1	1	Existe un vínculo del presupuesto, pero los niveles de servicios de los contratos deben ser mejorados
	¿Los niveles de servicio están acordados pero pueden no responder a las necesidades del negocio?	Plan de evaluación de los niveles de servicio	A corto plazo	1	1	Son de reciente aplicación, aun no se tiene resultados
	TOTAL			6	50.00%	
DS2 Administrar los servicios de terceros	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.	¿Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores?	Elaborar Políticas de Terceros que incluyan niveles de servicios, mejorar o incluir procedimientos bien establecidos	A corto plazo	1	1	Cubierto parcialmente por la política de socio de negocio
	Cuando se hace un acuerdo de prestación de servicios, ¿La relación con el tercero es meramente contractual?			2	0	Se tiene contrato
	¿La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operativos y de control?			2	0	Cubierto parcialmente por la política de socio de negocio
	¿Se asigna la responsabilidad de supervisar los servicios de terceros?			2	0	
	¿Los términos contractuales se basan en formatos estandarizados?			2	0	Cubierto parcialmente por la política de socio de negocio

	¿El riesgo del negocio asociado con los servicios del tercero está valorado y reportado?			2	0	Existe una evaluación de riesgo de proveedores
	TOTAL			11	8.33%	
DS5 Garantizar la Seguridad de los Sistemas	**Nivel de Madurez Esperado 4 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
La necesidad de mantener la integridad de la información y de proteger los activos de TI requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.	¿Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas en forma clara?	Definir la organización de Seguridad de la Información, en base a las nuevos estándares como ISO 27001:2013	A mediano plazo	1	1	Cuentan con personal de seguridad, no obstante falta involucrar otros roles y falta difundir los roles de seguridad a otras gerencias.
	¿Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad?			2	0	Análisis de riesgo del año 2013, se realizan análisis de riesgos por eventos y cambios importantes.
	¿Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas?			2	0	La casa matriz utiliza fuentes internacionales y es proporcionada a AFP
	¿El contacto con métodos para promover la conciencia de la seguridad es obligatorio?			2	0	La participación en la concientización en seguridad es obligatoria
	¿La identificación, autenticación y autorización de los usuarios está estandarizada?			2	0	Cuentan con usuario y contraseña

	¿La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad?	Elaborar un programa de capacitación en base a la organización de seguridad de la información que contemple la seguridad informática	A corto plazo	1	1	Se cuenta con parte del personal certificado en seguridad informática. Se recomienda en adición al rol de los responsables de seguridad la certificación a los administradores de TI que son responsables de cumplimiento
	¿Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad?	Elaborar términos de referencia de los proveedores de seguridad de acuerdo a los estándares internacionales	A corto plazo	1	1	Las pruebas de seguridad las realiza externos y esta afecto a su forma de trabajar.
	¿Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización?			2	0	Existe un oficial de seguridad de la información.
	¿Los reportes de seguridad están ligados con los objetivos del negocio?			2	0	Los reportes forman parte de los informes de riesgo operacional
	¿La habilitación sobre seguridad se imparte tanto para TI como para el negocio?			2	0	Es aplicable a toda la organización.
	¿La habilitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad?			2	0	Se cuenta con plan de seguridad de TI, se encuentra en proceso de implementación.
	¿Los KGIs y KPIs ya están definidos pero no se miden aún?	Implementar los KGI y KPI establecidos y monitorearlos	A corto plazo	1	1	Ya están definidos pero aún no se encuentran generando

						información.
	TOTAL			20	16.67%	
DS8 Administrar la Mesa de Servicio y los Incidentes	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.	¿Se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes?			2	0	
	¿Los procedimientos se estandarizan y documentan, pero se lleva a cabo entrenamiento informal?	Elaborar Términos de referencia de los proveedores de Mesa de Ayuda, incluyendo la exigencia de estándares en sus procedimientos.	A corto plazo	1	1	Manejado internamente por el servicio de tercero
	¿Se deja la responsabilidad al individuo de conseguir entrenamiento y de seguir los estándares?			2	0	
	¿Se desarrollan guías de usuario y preguntas frecuentes, pero los individuos deben encontrarlas y puede ser que no las sigan?	Elaborar Términos de referencia de los proveedores de Mesa de Ayuda, incluyen guías, preguntes frecuentas	A corto plazo	0	2	El proveedor afirmó que las tendrá para el 2014
	¿Las consultas y los incidentes se rastrean de forma manual y se monitorean de forma individual, pero no existe un sistema formal de reporte?			2	0	Se gestiona usando el CA services Desk
	¿No se mide la respuesta oportuna a las consultas e incidentes y los incidentes pueden quedar sin resolución?	Elaborar Términos de referencia de los proveedores de Mesa	A corto plazo	1	1	Si bien es cierto que los tiempos de respuesta son

		de Ayuda, incluyen respuesta oportuna a los incidentes y que estos sean constantemente monitoreados				pactados con el Tercero, se requiere un proceso de medición para los niveles de atención.
	¿Los usuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes?			1	1	Parcialmente, se requiere una implantación de los procedimientos existente.
	TOTAL			9	35.71%	
DS9 Administrar la Configuración	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.	¿Los procedimientos y las prácticas de trabajo se han documentado, estandarizado y comunicado, pero la habilitación y la aplicación de estándares dependen del individuo?			2	0	
	¿Se han implementado herramientas similares de administración de configuración entre plataformas?	Definir e implementar herramientas de administración de la configuración	A mediano plazo	0	2	Se realiza manualmente
	¿Es poco probable detectar las desviaciones de los procedimientos? ¿Las verificaciones físicas se realizan de manera inconsistente? (1)			2	0	No cuentan con mecanismos para detectar errores operativos
	¿Se lleva a cabo algún tipo de automatización para ayudar a rastrear cambios en el software o en el hardware?	Definir e implementar herramientas para detectar cambios en el software o en el	A mediano plazo	0	2	No cuentan con herramientas o mecanismos

		hardware.				
	¿La información de la configuración es utilizada por los procesos interrelacionados?	Plan de implementación de la configuración.	A mediano plazo	0	2	No se cuenta con una gestión de la configuración.
	TOTAL			4	60.00%	
DS10 Administración de Problemas	**Nivel de Madurez Esperado 3 – Preguntas**			**Calificación**	**Brecha**	**Comentario**
Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y la satisfacción del usuario.	¿Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y habilitación?			2	0	Si está en proceso de formalización 2014
	¿Se estandarizan los procesos de escalamiento y resolución de problemas?			2	0	Si está en proceso de formalización 2014
	¿El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar?			2	0	
	¿Es poco probable detectar las desviaciones de los estándares y de las normas establecidas?	Implementar el proceso de gestión de incidentes y problemas	A mediano plazo	1	1	Si está en proceso de formalización 2014
	¿La información se comparte entre el personal de manera formal y proactiva?	Implementar el proceso de gestión de incidentes y problemas	A mediano plazo	1	1	Esta en progreso
	¿La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales?	Implementar el proceso de gestión de incidentes y problemas	A mediano plazo	1	1	Si está en proceso de formalización 2014
	TOTAL			9	25.00%	

DS11 Administración de Datos	Nivel de Madurez Esperado 3 – Preguntas	Plan de mitigación de riesgos	Tiempo de implementación	Calificación	Brecha	Comentario
Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.	¿Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización?			2	0	Existen responsables en la administración de datos (propietarios, custodios, usuarios)
	¿Se establece la responsabilidad sobre la administración de los datos?			2	0	Existe un documentos de aceptación de responsabilidades
	¿Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad?			2	0	
	¿Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos/recuperación y desecho de equipo?	Implementar los lineamientos y procedimientos de eliminación segura	A corto plazo	1	1	No cubren desecho de equipo
	¿Se lleva a cabo algún tipo de monitoreo sobre la administración de datos?	Implementar el proceso.	A mediano plazo	1	1	Cubren la parte de respaldo, restauración y replicación
	¿Se definen métricas básicas de desempeño?	Implementar el proceso de administración de datos	A mediano plazo	1	1	En progreso de la parte de respaldo, restauración y replicación
	¿Aparece el entrenamiento sobre administración de información?	Implementar el proceso de administración de datos	A mediano plazo	1	1	
	TOTAL			10	28.57%	

DS12 Administración del Ambiente Físico	Nivel de Madurez Esperado 3 – Preguntas	Plan de mitigación de riesgos	Tiempo de implementación	Calificación	Brecha	Comentario
La protección del equipo de cómputo y del personal requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.	¿Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado?			2	0	
	¿Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia?			2	0	
	¿Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado?			2	0	Cuentan con controles de acceso físico
	¿Los visitantes se registran y acompañan dependiendo del individuo?			2	0	cuentan con libro de visita
	¿Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil?			2	0	Desde la recepción del piso no se puede identificar
	¿Las autoridades civiles monitorean el cumplimiento con los reglamentos de salud y seguridad?			2	0	Existe normativa relacionada
	¿Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro?			2	0	No se cuenta con un Plan de mitigación de riesgos
	TOTAL			14	0.00%	
DS13 Administración de Operaciones	**Nivel de Madurez Esperado 3 – Preguntas**	**Plan de mitigación de riesgos**	**Tiempo de implementación**	**Calificación**	**Brecha**	**Comentario**
Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este	¿Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo?			2	0	Las tareas se trabajan de forma flexible y colaboran las áreas

proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.						usuarias
	¿Se han asignado recursos y se lleva a cabo alguna habilitación durante el trabajo?			2	0	
	¿Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal?			2	0	Se elaboran instructivos para las operaciones
	¿Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia?			2	0	Los eventos escalan hasta el sub gerente de servicios de sistemas
	¿Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervención del operador?	Realizar análisis de riesgos frecuentes en las operaciones de TI que no están automatizadas	A corto plazo	1	1	Las tareas están automatizadas, mas no el cronograma de ejecución
	¿Se introducen controles para colocar nuevos trabajos en operación?			2	0	
	¿Se desarrolla una política formal para reducir el número de eventos no programados?	Mejorar las políticas de administración de operaciones incluyendo eventos no programados	A corto plazo	1	1	Si tienen una política no formal
	¿Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal? (1)			2	0	
	TOTAL			14	12.50%	

Nota (1) Siguiendo a COBIT las preguntas cuentan con una parte negativa que confirman el nivel, el puntaje 2 en este caso no representa el cumplimiento de la parte negativa, pero es usado para evitar una falsa percepción de brecha. Considerar 0= No, 1 = Parcialmente (es obligatorio llenar el comentario) – 2 Sí.

Fuente: Elaboración propia.

4.3.6 Relación de Controles Internos para Proveedores

Análisis
Se identificó los riesgos asociados a los procedimientos, de los procesos SOX, que pueden ser o ya están siendo mitigados (mesa de ayuda por ejemplo) a través de la intervención de terceros que prestan servicios TI.

Tabla 24 Riesgos TI cuyos controles necesitan revisión de terceros

Proceso	Procedimiento	Rol	Revisión del Tercero	Riesgos asociados
Gestión de Incidentes de TI y SI	**Gestión de Incidentes SI**	**Mesa de Ayuda**	• Registra, clasifica y analiza • El incidente de Seguridad de la Información que le fue escalado.	• Falla de los equipos tecnológicos. • Interrupción inesperada del servicio. • Reducción de la calidad del servicio. • Potencial interrupción del servicio.
Seguridad en Plataforma	**Procedimiento Antivirus**	**Responsable de la Consola**	• El fabricante actualiza las firmas del código malicioso y actualiza aquellos que no hayan sido investigados.	• Bajo rendimiento de las aplicaciones de negocio. • Acceso no autorizado a la información.
Seguridad en Plataforma	**Actualización de parches de seguridad**	**Ejecutivo de Seguridad y DRP**	• El fabricante comprueba la vigencia de los controles, genera una actualización y despliega las actualizaciones para su implementación.	• Filtración de la información corporativa. • Ataques de denegación de servicios.
Seguridad en Plataforma	**Actualización de parches de seguridad**	**Ejecutivo de Seguridad y DRP**	• El fabricante comprueba la vigencia de los controles, genera una actualización y despliega las actualizaciones para su implementación.	• Filtración de la información corporativa. • Ataques de denegación de servicios.
Gestión de Incidentes de TI y SI	**Gestión de Incidentes TI**	**Mesa de Ayuda**	• Registra, clasifica y analiza el incidente TI que fue escalado.	• Excesiva complejidad y volumen de incidentes, solicitudes de servicio, que por primera vez aparecen y que no pueden atenderse conforme a los plazos fijados. • No tener fuentes de información convenientes. • Hay un desequilibrio entre los objetivos y las acciones

Proceso	Procedimiento	Rol	Revisión del Tercero	Riesgos asociados
				en la resolución de los incidentes.
Gestión d Problemas	**Gestión de Problemas**	**Mesa de Ayuda**	• Gestiona el problema, solo ante un escalamiento.	• Paralizaciones en las operaciones del negocio. • Desproporcionado número de problemas con alta complejidad que impide cumplir con los acuerdos de nivel de servicio. • Falta de herramientas y recursos especializados en la determinación de la causa raíz de un problema y en la adopción de medidas apropiadas para eliminar los incidentes. • No existen fuentes de información apropiadas.
Niveles de Servicio	**Catálogo de Servicios**	**Dueño del Catálogo**	• Una consultoría externa para revisar el catalogo y proponer mejoras.	• Inexactitud de los datos en el catálogo de servicios. • Limitada aceptación del catálogo de servicios respecto a los procesos operativos. • No se dispone de una herramienta para actualizar la información del catálogo. • No utilizar formalmente el portafolio de servicios y el catálogo de servicios. • La información del catálogo es muy detallada para mantenerla.
Niveles de Servicio	**Monitoreo de Niveles de Servicio**	**Proveedor Externo**	Auditoría, para validar el cumplimiento de los SLAs, "Service Level Agreement" OLAs "Operational Level Agreement" y UCs "underpinning Contracts".	• No cumplir con los SLA que el negocio demanda. • Falta de compromiso entre el área TI y sus clientes. • Carencia de herramientas y recursos para acordar, documentar, monitorear, informar y revisar los

Proceso	Procedimiento	Rol	Revisión del Tercero	Riesgos asociados
				SLAs. • Las altas expectativas y la baja percepción de los clientes. • Que se convierta sólo en un proceso burocrático.
Monitoreo	**Monitoreo de Seguridad e Infraestructura**	**SOC/Otras herramientas de Monitoreo Interno**	• Registra las alertas que llegan del servicio de SOC u otras herramientas de monitoreo, hace seguimiento de todas las alertas de monitoreo de Seguridad e Infraestructura registradas. • Efectúa el seguimiento del estado y del avance hacia la resolución de las alertas críticas asignadas. • Mantiene informado al Ejecutivo de Seguridad y DRP de los avances de la gestión del incidente.	• Acceso no autorizado a los recursos tecnológicos de la red. • Ataques externos como denegación de servicios. • No detectar errores en los elementos de configuración. • No validar los controles.
Monitoreo	**Hardening**	**Ejecutivo de Seguridad y DRP**	• Certifica que los nuevos recursos críticos tengan los "parches" actualizados y que sean capaces de defenderse contra las vulnerabilidades conocidas. • Facilita el despliegue rápido de una configuración inicial que sea segura y fácil de auditar para un nuevo servidor frente a cambios inesperados. • Potencia la seguridad de los nuevos componentes de la infraestructura TI frente a las amenazas internas y externas. • Reducción del fraude y error	• No contar con un nuevo servidor asegurado. • Fraude. • Error humano.

Proceso	Procedimiento	Rol	Revisión del Tercero	Riesgos asociados
			humano.	
Monitoreo	**Código Seguro**	**Consultor de Sistemas / Ejecutivo de Seguridad y DRP**	• Proteger la revelación de los datos de infraestructura. • Protección de la conexión a la BD. • Proteger los de datos de entrada	• Robo de información por un tercero. • Modificación no autorizada de los datos privados por un tercero.
Monitoreo	**Análisis de Vulnerabilidad**	**Proveedor**	• Monitoreo y Control de la Seguridad de la Infraestructura.	• No tener servidores seguros. • Perder conectividad en la red. • Falla en los medios de almacenamiento. • Defectos de diseño de programas. • Errores comunes de programación. • Defectos de instalación o programación. • Pérdida de la integridad de los datos. • Retiro del personal TI.
Monitoreo	**Ethical Hacking**	**Proveedor**	• Test de intrusión externa e interna.	• Ataques comunes tanto internos como externos. • Vulnerabilidades en los activos y controles. • Ingeniería Social.

Fuente: Elaboración propia.

Recomendaciones

Se sugiere determinar la tasa de disponibilidad de cada uno de los servicios TI en los horarios de atención, según sea el caso, durante un tiempo significativo que no exceda los

12 meses, para reconocer cuáles controles requieren la revisión de terceros debido al alto volumen de la demanda de los clientes o por el apremio del ente regulador.

Es tan importante el valor de la reputación, como intangible, que un experto en economía "Jonathan Kendrick" afirmó "que ya en el 2008, el valor de los activos intangibles de una empresa representaba el 85% de su valor, valor no muy lejano de la realidad hoy".

4.3.7 Seguridad en Plataforma – Monitoreo

Antecedentes

- Se utilizó el formato de AFP llamado "CheckList OSG Servidores".

Análisis Servidores

Se han evaluado 02 servidores por ser considerados críticos y encontrarse dentro del alcance de SOX.

Tabla 25 Servidores Evaluados

Servidor	Nivel Evaluado	Aplicativo relacionado
SPPEDBS00006	Sistema Operativo Windows 2008	Sistema de Contabilidad
Huari	Sistema Operativo Windows 2003	Sistema de Inversiones

Fuente: Elaboración propia.

Resultados de la evaluación

Con respecto al servidor SPPEDBS00006:

Tabla 26 Criterios Cumplimiento.

Criterios	Cumple
Controles que cumplen	136
Controles que no cumplen	28
Controles que no aplican	198
Estados de los controles que se han re-categorizados	19
Controles que no cumplen con justificación	-
Controles que no cumplen y requieren trabajos especiales (ordenes de cambio)	28

Fuente: Elaboración propia.

En el caso del servidor SPPEDBS00006 se realizó una revisión exhaustiva de los controles, tomando alrededor de 6h de trabajo, por lo que se podría estimar 12h para la realización del hardening si fuese realizado de forma manual sobre una instalación nueva.

Sugerencias

- El OSG que utiliza AFP es extenso y profundo, incluyendo criterios más profundos a los considerados por ejemplo por las "Baselines Server Hardening" de Microsoft.
- Realizar actividades de seguimiento a los incumplimientos de las OSG, desde la fecha de elaboración en junio del 2011 no existe evidencia de seguimiento, en caso de una auditoria la presentación de las OSG desactualizadas jugarían en contra de la empresa.
- Definir un plan de tratamiento para los no cumplimientos, las OSG solo están indicando el riesgo, no existe actividad correctiva ni responsable, por lo que no existe un cambio en el estado del no cumplimiento a pesar de su identificación.
- Los controles evaluados para órdenes de cambio fueron preliminarmente verificados conseguimiento de que se realicen las pruebas y ejecución durante una ventana de trabajo.
- Se hace notar que la realización de hardening sobre servidores en producción es riesgoso ya que probablemente deje de funcionar correctamente algunas aplicaciones.
- Se sugiere para el caso de las nuevas versiones de los sistemas operativos utilizar estándares de hardening; como el proporcionado por Microsoft y su herramienta Microsoft Security Compliance Manager, o cualquier herramienta que les permita ese apoyo o basarse en las guías proporcionadas por Nist "National Institute of Standard and Tecnology"
- Debido a la complejidad de las tareas de hardening que son diferentes a las actividades normales administración de los servidores se sugiere brindar capacitaciones especializadas al personal responsable.
- Preparar la migración de los servidores Windows Server 2003 a una versión más reciente, debido a que la fecha de fin de soporte extendido es el 14 de Julio de 2015, el soporte técnico principal venció el 13 de Julio del 2010[5], por lo que se está exponiendo la entidad a un riesgo por software no soportado
- Se sugiere integrando los puntos anteriores, preparar la plantilla del Windows Server 2012 usando un estándar de hardening con soporte en el tiempo, la plantilla será utilizada para los servidores virtuales nuevos que recibirán las aplicaciones de los Windows Server 2003, por los cambios mayores que se estarían realizando se deberán probar extensamente en el ambiente de pruebas antes de reemplazar a los servidores de producción.
- Se hace notar que la premisa de hardening es deshabilitar lo que no se usa, restringir accesos y auditar todo lo posible, no obstante se está cometiendo un error al considerar el hardening como una actividad estática que es realizado una única vez, mientras que el equipo durante su uso degrada su seguridad el atacante

[5] http://support.microsoft.com/lifecycle/default.aspx?LN=es-pe&x=23&y=6&p1=10394

evoluciona sus vectores de ataque dando lugar a ataques más sofisticados que sin importar sus medidas tomadas ya no serán efectivas (Ej. Tienes una defensa con huecos del 2007 cuando el ataque usa técnicas del 2013) por lo que se sugiere nuevamente:

- Actualicen sus OSG de hardening.
- Ejecuten anualmente la revisión completa del cumplimiento del hardening.

Contraten servicios especializados en el mercado que intenten penetrar sus medidas tomadas.

4.4 Implementación de Flujos y Controles.

En esta última etapa definimos los flujos de acuerdo a los procesos definidos en la etapa I, identificando en dichos flujos claramente los actores que participan en los controles.

Cabe mencionar que los actores son los responsables de la ejecución del control generando las evidencias respectivas para su auditoria posterior.

A continuación se presenta la tabla de relaciones de procesos versus controles.

Tabla 27 Relación de Procesos vs Controles.

	Proceso	Control	Anexo
1	Gestión de Accesos –Altas de Usuarios	Creación de cuentas de usuario por el Administrador de Cuentas de Accesos	B
2	Gestión de Accesos –Altas de Usuarios	Autorización de Accesos por parte del Propietario	B
3	Gestión de Accesos – Revisión de Acceso Anual - Trimestral	Verificación de seguridad a nivel de acceso Anual.	B
4	Gestión de Accesos – Revisión de Acceso Anual - Trimestral	Verificación de seguridad a nivel de acceso Trimestral.	B
5	Gestión de Accesos – Revisión de Acceso Mensual.	Verificación de seguridad a nivel de acceso Mensual.	B
6	Gestión de Accesos – Baja de Cuenta de Usuarios.	Se basa en la revisión de acceso Mensual.	B
7	Gestión de Accesos – Accesos a Producción para Personal de Desarrollo	Autorización de acceso a producción por parte de los dueños de activos de información al personal de TI.	B
8	Administración de Datos	Acta de autorización de usuarios que usan medios de almacenamiento, comunicación externa y equipos y medios móviles	C
9	Administración de Datos –	Propietario de la	C

	Proceso	Control	Anexo
	Eliminación Segura de Medios	información, autoriza la eliminación de dicho contenido en el medio que lo almacena	
10	Administración de Datos – Eliminación Segura de Medios	Acta de eliminación segura de la información	C
11	Administración de Datos – Procedimiento de Respaldo y Restauración.	Validación de almacenamiento de cintas de backup en el proveedor de custodia de medios.	C
12	Administración de Datos – Procedimiento de Respaldo	Verificación de Respaldo	C
	Administración de Datos – Procedimiento de Restauración	Validación de la restauración en base al plan de pruebas.	C
13	Administración de Datos – Procedimiento de Restauración	Validación del reporte de respaldo de información.	C
14	Gestión de Control de Cambios – Cambio Normal	Validación de impacto y priorización del requerimiento del cambio, por parte del CAB Change Advisory Board.	D
15	Gestión de Control de Cambios – Cambio Normal	Validación del registro del requerimiento de cambio y su prioridad por parte del propietario del activo.	D
16	Gestión de Control de Cambios – Cambio Normal	Reivisión del cumplimiento de los puntos de control a nivel de estándares de desarrollo y calidad, realizado por el Custodio.	D
17	Gestión de Control de Cambios – Cambio Normal	Aprobación de diseño detallado / técnico del requerimiento por parte del custodio	D
18	Gestión de Control de Cambios – Cambio Normal	Validación del desarrollo de la aplicación realizado por el custodio.	D
19	Gestión de Control de Cambios – Cambio Normal	Validación de los controles a nivel de la aplicación, realizado por el custodio	D
20	Gestión de Control de Cambios – Cambio Normal	Aprobación del formato de pase a producción, realizado por el propietario del activo.	D
21	Gestión de Control de Cambios – Cambio Normal	Plan de pruebas en ambiente controlado realizado por el ejecutor de pase a producción.	D
22	Gestión de Control de Cambios – Cambio Normal	Validación del cambio realizado realizado por el jefe del área.	D

	Proceso	Control	Anexo
23	Gestión de Control de Cambios – Cambios de Emergencia	Validación del registro del requerimiento de cambio y la prioridad,	D
24	Gestión de Control de Cambios – Cambios de Emergencia	Validación de documentación que sustenta el cambio.	D
25	Gestión de Control de Cambios – Cambios de Emergencia	Aprobación del formato de pase a producción	D
26	Gestión de Control de Cambios – Cambios de Emergencia	Validación del requerimiento de cambio.	D
27	Gestión de Control de Cambios – Adquisición de la Solución.	Basado en el proceso de cambios normales.	D
28	Gestión de Control de Cambios – Desarrollo de la Solución.	Revisión del cumplimiento de los puntos de control a nivel de estándares de desarrollo y calidad	D
29	Gestión de Control de Cambios – Desarrollo de la Solución.	Validación del desarrollo de la aplicación (Documentación de desarrollo, pruebas)	D
30	Gestión de Control de Cambios – Realizar pruebas a la solución.	Basado en el proceso de cambios normales o de emergencia	D
31	Gestión de Control de Cambios – Pase a Producción	Aprobación del formato de pase a producción	D
32	Gestión de Control de Cambios – Procedimiento de monitoreo del cambio	Validación del seguimiento y reporte al negocio de los requerimientos internos	D
33	Gestión de Control de Cambios – Procedimiento de monitoreo del cambio	Validación del seguimiento y reporte al negocio de los requerimientos atendidos por la fábrica de sw	D
34	Gestión de Incidentes de Seguridad de la Información	Registro, clasificación en la bitácora de incidentes.	F
35	Gestión de Incidentes de TI.	Registro/Clasificación de incidentes por la Mesa de Ayuda	G
36	Gestión de Incidentes de TI.	Registro/Clasificación de incidentes por la Mesa de Ayuda	G
37	Gestión de Incidentes de TI.	Valida la encuesta	G
38	Gestión de Incidentes de TI.	Tracking de Atención	G
39	Gestión de Problemas	Escalamiento y clasificación de la solicitud del usuario por la Mesa de Ayuda	H
40	Gestión de Problemas	Verifica atención de la solicitud por el usuario	H
41	Gestión de Problemas	Monitoreo desempeño de la	H

	Proceso	Control	Anexo
		mesa de ayuda	
42	Gestión del Talento Humano – Plan de Concientización de Riesgos Operativos.	Revisión del plan de concientización de riesgos operativos.	I
43	Gestión del Talento Humano – Plan de Concientización de Riesgos de TI.	Revisión del plan de concientización de riesgos TI.	I
44	Gestión del Talento Humano – Cambio de Puesto y Funciones	Revisión y Validación de del puesto vs Matriz de Segregación de Funciones	I
45	Gestión de Desempeño y de la Calidad.	Revisión del desempeño del resultado de indicadores definidos	J
46	Gestión de Desempeño y de la Calidad.	Validación anual de definición de métricas nuevas o modificación de métricas de TI	J
47	Gestión de Desempeño y de la Calidad.	Revisión del informe de cumplimiento de indicadores de desempeño definidos	J
48	Marco de Trabajo de los Procesos de Tecnología	Validación/Revisión del Sistema de Gestión de TI	K
49	Marco de Trabajo de los Procesos de Tecnología	Registro de historial de versiones del documento	K
50	Marco de Trabajo de los Procesos de Tecnología – Roles de Tecnología.	Validación de actualización del MOF/Funciones/Roles	K
51	Marco de Trabajo de los Procesos de Tecnología – Roles de Tecnología.	Verifica/Actualiza la Matriz de Segregación de Funciones	K
52	Monitoreo de Seguridad e Infraestructura.	Monitoreo de alertas	L
53	Monitoreo de Seguridad e Infraestructura.	Validación de alertas	L
54	Monitoreo de Seguridad e Infraestructura.	Validación de seguridad interna y perimetral	L
55	Monitoreo de Seguridad e Infraestructura - Hardening	Revisión de Informe de Seguridad	L
56	Monitoreo de Seguridad – Flujo de Código Seguro	Revision de Informes de Seguridad	L
57	Monitoreo de Seguridad – Análisis de Vulnerabilidades.	Revisión del Informe de Seguridad	L
58	Monitoreo de Seguridad – Ethical Hacking	Revisión de Informes de Seguridad	L
59	Operaciones	Verificación de la aplicación del checklist de configuración de ambientes controlados	M
60	Operaciones – Gestión de	Validación de Programación	M

	Proceso	Control	Anexo
	Tareas.	de Tareas	
61	Operaciones – Actualizar Cronograma	Validación de Programación de tareas	M
62	Operaciones – Ejecutar del Cronograma.	Validación de Programación de tareas	M
63	Operaciones – Ejecutar del Cronograma.	Comunicación a los dueños de activos sobre ejecución de tareas.	M
64	Operaciones - Elaboración del Inventario de Activos de TI.	Validación de la responsabilidad de los dueños y custodios de información a través del documento de aceptación de responsabilidades.	M
65	Operaciones - Elaboración del Inventario de Activos de TI.	Validación de la responsabilidad de los dueños y custodios de información a través del documento de aceptación de responsabilidades	M
66	Operaciones - Elaboración del Inventario de Activos de TI.	Revisión de la actualización del Inventario de activos de TI por el Subgerente de Servicios de Sistemas	M
67	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz de Inventario de Activos de TI	M
68	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Servidores Físicos y Virtuales	M
69	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Aplicativos	M
70	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Equipos de Comunicación	M
71	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Equipos de Seguridad	M
72	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Servicios Genéricos	M
73	Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Conexiones Externas	M
74	Operaciones - Elaboración del Inventario de Activos de TI.	Guía de Clasificación de Activos de TI	M
75	Resilencia y Seguridad Física.	Verificación de controles ambientales y físicos	N
76	Resilencia y Seguridad Física – Control de Acceso al Centro de Cómputo	Bitacora de Control de Acceso al Centro de Cómputo.	N
77	Gestión de Seguridad en Plataforma - Antivirus	Verificación de firmas actualizadas	Ñ

	Proceso	Control	Anexo
78	Gestión de Seguridad en Plataforma – Seguridad Perimetral	Verificación de firmas actualizadas	Ñ
79	Actualización de Parches de Seguridad	Verificación de actualización de parches.	Ñ
80	Gestión de Niveles de Servicio	Monitoreo de Niveles de Servicio	P
81	Gestión de Niveles de Servicio – Definición y/o actualización de servicios.	Factibilidad de Implementación	O
82	Gestión de Niveles de Servicio – Implementación de Servicio.	Revisión y Válida los SLA'a y UC's requeridos.	O
83	Gestión de Niveles de Servicio del Portafolio – Revisión Anual	Validación del Catálogo de Servicios de TI	O
84	Gestión de Niveles de Servicio del Portafolio – Revisión Anual	Verificación de los Servicios y Métricas.	O
85	Gestión de Niveles de Servicio del Portafolio – Revisión Anual	Validación del Catálogo de Servicios de TI.	O
86	Gestión de Niveles de Servicio del Portafolio – Revisión Anual	Validación del inventario de proveedores de TI	O
87	Gestión de Niveles de Servicio del Portafolio – Revisión Anual	Validación del catálogo de Servicios de TI.	O
88	Gestión de Niveles de Servicio del Portafolio – Revisión Anual	Verificación de los servicios y métricas con terceros	O
89	Gestión de Niveles de Servicio del Portafolio – Monitoreo de Niveles de Servicio.	Monitoreo del reporte de cumplimiento de niveles de servicio de proveedores	O
90	Gestión de Niveles de Servicio del Portafolio – Monitoreo de Niveles de Servicio.	Monitoreo del reporte de Cumplimiento de SLA de TI.	O
91	Gestión de Mesa de Ayuda	Registro de solicitud emitida por el usuario(telefónico/correo) realizada por la Mesa de Ayuda	P
92	Gestión de Mesa de Ayuda	Escalamiento y Clasificación de ls solicitud del usuario.	P
93	Gestión de Mesa de Ayuda	Revisión de las atenciones de la mesa de ayuda.	P
94	Gestión de Mesa de Ayuda	Verificación de Atención de la Solicitud por el usuario.	P
95	Gestión de Mesa de Ayuda	Monitoreo de desempeño de la mesa de ayuda	P
96	Gestión del Catálogo de Servicios.	Evaluación de Factibilidad del Servicio.	Q
97	Gestión de Servidores Críticos	Actualización de la CMDB	R
98	Definición del Plan Estratégico	Validación del histórico de mediciones de monitoreo de infraestructura y servicios –	S

	Proceso	Control	Anexo
		Desarrollo del plan de capacidad.	
99	Definición del Plan Estratégico	Desarrollo del Plan de Seguridad de TI por el Ejecutivo de Seguridad	S
100	Definición del Plan Estratégico	Validación de las necesidades de la gerencia por el Gerente Central de Operaciones y Sistemas a través de Acta de Reunión	S
101	Definición del Plan Estratégico	Aprobación y comunicación del Plan Estratégico de TI (PETI) por el Gerente Central de Sistemas al Comité de Gerencia	S

Fuente: Elaboración propia.

Capítulo 5
Análisis de Resultados

5.1 Matriz de Resultados por Proceso y Control

La presente matriz muestra la relación entre procesos, control y valor obtenido antes de la mejora y el porcentaje esperado luego de la aplicación de los controles involucrados en cada proceso.

Tabla 28 Resultados por Procesos y Control.

Proceso	**Control**	**Flujo Anexo**	**Macro Proceso**	**Dominio Cobit**	**Objetivo de Control**	**Modelo de Madurez**	**Valor Previo**	**Valor Esperado Inicial ***
Gestión de Accesos – Altas de Usuarios	1.-Creación de cuentas de usuario por el Administrador de Cuentas de Accesos. 2.- Autorización de Accesos por parte del Propietario	2	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Gestión de Accesos – Revisión de Acceso Anual - Trimestral - Mensual	1.-Verificación de seguridad a nivel de acceso Anual/Trimestral/Mensual.	2	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Gestión de Accesos – Baja de Cuenta de Usuarios.	Se basa en la revisión de acceso Mensual.	2	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Accesos – Accesos a Producción para Personal de Desarrollo	Autorización de acceso a producción por parte de los dueños de activos de información al personal de TI.	2	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Administración de Datos	Acta de autorización de usuarios que usan medios de almacenamiento, comunicación externa y equipos y medios móviles	3	Gestión de Tecnología	Delivery and Support DS11	Manage Data	3	28.57%	80%
Administración de Datos – Eliminación Segura de Medios	1.-Propietario de la información, autoriza la eliminación de dicho contenido en el medio que lo almacena. 2.- Acta de eliminación segura de la información	3	Gestión de Tecnología	Delivery and Support DS11	Manage Data	3	28.57%	80%
Administración de Datos – Procedimiento de Respaldo y Restauración.	Validación de almacenamiento de cintas de backup en el proveedor de custodia de medios.	3	Gestión de Tecnología	Delivery and Support DS11	Manage Data	3	28.57%	80%
Administración de Datos – Procedimiento de Respaldo	1. Verificación de Respaldo. 2.- Validación de la restauración en base al plan de pruebas. 3.-Validación del reporte de respaldo de información.	3	Gestión de Tecnología	Delivery and Support DS11	Manage Data	3	28.57%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Control de Cambios – Cambio Normal	1.- Validación de impacto y priorización del requerimiento del cambio, por parte del CAB Change Advisory Board. 2.- Validación del registro del requerimiento de cambio y su prioridad por parte del propietario del activo 3.-Validación del registro del requerimiento de cambio y su prioridad por parte del propietario del activo. 4.Validación del desarrollo de la aplicación realizado por el custodio.	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Cambio Normal	Reivisión del cumplimiento de los puntos de control a nivel de estándares de desarrollo y calidad, realizado por el Custodio.	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Cambio Normal	Aprobación de diseño detallado / técnico del requerimiento por parte del custodio	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Control de Cambios – Cambio Normal	1.- Aprobación del formato de pase a producción, realizado por el propietario del activo. 2.- Plan de pruebas en ambiente controlado realizado por el ejecutor de pase a producción. 3.- Validación del cambio realizado realizado por el jefe del área.	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Cambios de Emergencia	1.- Validación del registro del requerimiento de cambio y la prioridad. 2.- Validación de documentación que sustenta el cambio. 3.-Aprobación del formato de pase a producción. 4.- Validación del requerimiento de cambio	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Adquisición de la Solución.	Basado en el proceso de cambios normales.	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Desarrollo de la Solución.	Revisión del cumplimiento de los puntos de control a nivel de estándares de desarrollo y calidad	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Control de Cambios – Desarrollo de la Solución.	Validación del desarrollo de la aplicación (Documentación de desarrollo, pruebas)	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Realizar pruebas a la solución.	Basado en el proceso de cambios normales o de emergencia	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Pase a Producción	Aprobación del formato de pase a producción	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Procedimiento de monitoreo del cambio	Validación del seguimiento y reporte al negocio de los requerimientos internos	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Control de Cambios – Procedimiento de monitoreo del cambio	Validación del seguimiento y reporte al negocio de los requerimientos atendidos por la fábrica de sw	4	Gestión de Tecnología	Acquisition and Implementation AI 6	Manage Changes	4	5.56%	80%
Gestión de Incidentes de Seguridad de la Información	Registro, clasificación en la bitácora de incidentes.	6	Gestión de Tecnología	Delivery and Support DS8	Manage Service Desk and Incidents	3	35.71%	80%
Gestión de Incidentes de TI.	1.-Registro /Clasificación de incidentes por la Mesa de Ayuda. 2.-Registro/Clasificación de incidentes por la Mesa de Ayuda 3.-Valida la encuesta	7	Gestión de Tecnología	Delivery and Support DS8	Manage Service Desk and Incidents	3	35.71%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Incidentes de TI.	Tracking de Atención	7	Gestión de Tecnología	Delivery and Support DS8	Manage Service Desk and Incidents	3	35.71%	80% 80%
Gestión de Problemas	1.-Escalamiento y clasificación de la solicitud del usuario por la Mesa de Ayuda. 2.- Verifica atención de la solicitud por el usuario 3.-Monitoreo desempeño de la mesa de ayuda	8	Gestión de Tecnología	Delivery and Support DS10	Manage Problems	3	25.00%	80%
Gestión del Talento Humano – Plan de Concientización de Riesgos Operativos.	Revisión del plan de concientización de riesgos operativos.	9	Organización de TI.	Planning and Organization PO7	Manage IT Human Resources	2	25.00%	80%
Gestión del Talento Humano – Plan de Concientización de Riesgos de TI.	Revisión del plan de concientización de riesgos TI.	9	Organización de TI.	Planning and Organization PO7	Manage IT Human Resources	2	25.00%	80%
Gestión del Talento Humano – Cambio de Puesto y Funciones	Revisión y Validación de del puesto vs Matriz de Segregación de Funciones	9	Organización de TI.	Planning and Organization PO7	Manage IT Human Resources	2	25.00%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Desempeño y de la Calidad.	1.-Revisión del desempeño del resultado de indicadores definidos. 2.- Validación anual de definición de métricas nuevas o modificación de métricas de TI 3.-Revisión del informe de cumplimiento de indicadores de desempeño definidos	10	Organización de TI.	Monitor and Evaluate ME1	Monitor and Evaluate IT Performance	2	12.50%	80%
Marco de Trabajo de los Procesos de Tecnología	1.- Validación/Revisión del Sistema de Gestión de TI. 2.- Registro de historial de versiones del documento 3.- Validación de actualización del MOF/Funciones/Roles. 4. Verifica/Actualiza la Matriz de Segregación de Funciones	11	Organización de TI.	Monitor and Evaluate ME4	Provide IT Governance	3	57.26%	80%
Monitoreo de Seguridad e Infraestructura.	1.-Monitoreo de alertas.	12	Gestión de Tecnología	Delivery and Support DS 13	Manage Operations	3	12.50%	80%
Monitoreo de Seguridad e Infraestructura.	Validación de alertas	12	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Monitoreo de Seguridad	Validación de seguridad interna y perimetral	12	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Monitoreo de Seguridad	Revisión de Informe de Seguridad	12	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Monitoreo de Seguridad – Flujo de Código Seguro	Revision de Informes de Seguridad	12	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Monitoreo de Seguridad – Análisis de Vulnerabilidades.	Revisión del Informe de Seguridad	12	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Monitoreo de Seguridad – Ethical Hacking	Revisión de Informes de Seguridad	12	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Operaciones	1.-Verificación de la aplicación del checklist de configuración de ambientes controlados. 2.- Validación de Programación de Tareas - Actualización Cronograma - Ejecución	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Operaciones – Ejecutar del Cronograma.	Comunicación a los dueños de activos sobre ejecución de tareas.	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Operaciones - Elaboración del Inventario de Activos de TI.	Validación de la responsabilidad de los dueños y custodios de información a través del documento de aceptación de responsabilidades.	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Operaciones - Elaboración del Inventario de Activos de TI.	Validación de la responsabilidad de los dueños y custodios de información a través del documento de aceptación de responsabilidades	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Operaciones - Elaboración del Inventario de Activos de TI.	Revisión de la actualización del Inventario de activos de TI por el Subgerente de Servicios de Sistemas	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Operaciones - Elaboración del Inventario de Activos de TI.	1.-Formato de Matriz de Inventario de Activos de TI. 2.-Formato de Matriz Inventario de Servidores Físicos y Virtuales 3.- Formato de Matriz Inventario de Aplicativos. 4.-Formato de Matriz Inventario de Equipos de Comunicación. 5.- Formato de Matriz Inventario de Equipos de Seguridad.	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Servicios Genéricos	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Operaciones - Elaboración del Inventario de Activos de TI.	Formato de Matriz Inventario de Conexiones Externas	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Operaciones - Elaboración del Inventario de Activos de TI.	Guía de Clasificación de Activos de TI	13	Gestión de Tecnología	Delivery and Support DS13	Manage Operations	3	12.50%	80%
Resilencia y Seguridad Física.	Verificación de controles ambientales y físicos	14	Gestión de Tecnología	Delivery and Support DS12	Ensure Continuous Service	3	0.00%	80%
Resilencia y Seguridad Física – Control de Acceso al Centro de Cómputo	Bitacora de Control de Acceso al Centro de Cómputo.	14	Gestión de Tecnología	Delivery and Support DS12	Ensure Continuous Service	3	0.00%	80%
Gestión de Seguridad en Plataforma - Antivirus	Verificación de firmas actualizadas	15	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Gestión de Seguridad en Plataforma – Seguridad Perimetral	Verificación de firmas actualizadas	15	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Gestión de Seguridad - Actualización de Parches de Seguridad	Verificación de actualización de parches.	15	Gestión de Tecnología	Delivery and Support DS5	Ensure Systems Security	4	16.67%	80%
Gestión de Niveles de Servicio	Monitoreo de Niveles de Servicio.	16	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Niveles de Servicio – Definición y/o actualización de servicios.	Factibilidad de Implementación	16	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%
Gestión de Niveles de Servicio – Implementación de Servicio.	Revisión y Válida los SLA'a y UC's requeridos.	16	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%
Gestión de Niveles de Servicio del Portafolio – Revisión Anual	1.-Validación del Catálogo de Servicios de TI. 2.- Verificación de los Servicios y Métricas. 3.- Validación del Catálogo de Servicios de TI. 4.- Validación del inventario de proveedores de TI. 5.- Validación del catálogo de Servicios de TI. 6.- Verificación de los servicios y métricas con terceros.	16	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%
Gestión de Niveles de Servicio del Portafolio – Monitoreo de Niveles de Servicio.	Monitoreo del reporte de cumplimiento de niveles de servicio de proveedores	16	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Gestión de Niveles de Servicio del Portafolio – Monitoreo de Niveles de Servicio.	Monitoreo del reporte de Cumplimiento de SLA de TI.	16	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%
Gestión de Mesa de Ayuda	1.-Registro de solicitud emitida por el usuario(telefónico/correo) realizada por la Mesa de Ayuda. 2.- Escalamiento y Clasificación de ls solicitud del usuario 3.- Revisión de las atenciones de la mesa de ayuda. 4.- Verificación de Atención de la Solicitud por el usuario. 5.- Monitoreo de desempeño de la mesa de ayuda	17	Gestión de Tecnología	Delivery and Support DS8	Manage Service Desk and Incidents	3	35.71%	80%
Gestión del Catálogo de Servicios.	Evaluación de Factibilidad del Servicio.	18	Gestión de Tecnología	Delivery and Support DS1	Define and Manage Service Levels	3	50.00%	80%
Gestión de Servidores Críticos	Actualización de la CMDB	19	Gestión de Tecnología	Delivery and Support DS9	Manage the Configuration	3	60.00%	80%

Proceso	Control	Flujo Anexo	Macro Proceso	Dominio Cobit	Objetivo de Control	Modelo de Madurez	Valor Previo	Valor Esperado Inicial *
Definición del Plan Estratégico	1.-Validación del histórico de mediciones de monitoreo de infraestructura y servicios – Desarrollo del plan de capacidad.. 2.- Desarrollo del Plan de Seguridad de TI por el Ejecutivo de Serguridad 3.-Validación de las necesidades de la gerencia por el Gerente Central de Operaciones y Sistemas a través de Acta de Reunión. 4.- Aprobación y comunicación del Plan Estratégico de TI (PETI) por el Gerente Central de Sistemas al Comité de Gerencia	20	Organización de TI.	Planning and Organization PO1	Define a Strategic IT Plan	3	57.14 %	80%

Fuente: Elaboración propia.

*Valor Esperado Inicial, considerando las primeras interacciones de los controles como evidencia, se proyecta alcanzar un 100% luego de las 3 primeras interacciones de los controles con sus respectivas evidencias sustentadoras.

5.2 Informe de Brechas Detectadas

Se convocó a los actores, gestores y responsables del proceso de seguridad de la plataforma, adquisición de infraestructura y se realizó las siguientes actividades:

1. Se mostró los procedimientos del proceso de seguridad de plataforma y se tomó como referencia el monitoreo de seguridad e infraestructura.
2. Detalle de las bases de datos y las aplicaciones.
3. Identificar los riesgos asociados a las operaciones de los controles.
4. Identificación de los roles y responsabilidades.

Durante el taller intervinieron los gestores, operadores y propietarios, también se identificaron problemas en las operaciones, como la estandarización de las adquisiciones de tecnología.

Luego de la tormenta de ideas, se procedió a las respuestas del cuestionario y hubo una confusión si la respuesta era por cada actor o por el proceso. Se aclara que las respuestas son en base a un consenso del proceso que se está autoevaluando.

También se solicitó la identificación de los riesgos, y hubo confusión en los conceptos de riesgos, amenazas, vulnerabilidades y consecuencias.

Las respuestas del cuestionario es la siguiente:

Tabla 29 Ejemplo de Brechas Detectadas..

	1. Nivel de comunicación de los riesgos y controles, sus objetivos, alcances.	2. Nivel de entendimiento de la asignación de roles y responsabilidades en el proceso de gestión de riesgos y la operación de los controles.	3. Nivel de cumplimiento de los roles y responsabilidades en el proceso de gestión de riesgos y la operación de los controles.	4. Niveles de monitoreo y revisión de los riesgos y controles, en base a los puntos de control y evidencias.	5. Validar los niveles de sensibilización y competencias en el proceso de gestión de riesgos y la operación de los controles.
¿Tienes conocimiento del proceso de Seguridad en Plataforma, y cuáles son sus procedimientos?	*3*				
¿Existe una comunicación adecuada entre el gestor de riesgos, propietarios del proceso y actores?	3				
¿Tienes conocimiento de los roles y responsabilidades en los procedimientos que pertenecen al proceso de Seguridad en Plataforma?		4			
¿Cumples con tus roles y responsabilidades consignados en los procedimientos que pertenecen al proceso de Seguridad en Plataforma?			4		
¿Tienes conocimientos de los riesgos y controles que operan en el proceso de Seguridad en Plataforma?				4	
¿Incrementas tus niveles de sensibilización y competencias en las operaciones del proceso de Seguridad en Plataforma?					4

Fuente: Elaboración propia.

Conclusiones del Taller:

- Es necesario difundir los procesos de tecnología de información y explicar los objetivos, alcances y las actividades de los procedimientos.
- Durante el taller los principios de identificación de riesgos no eran muy claros, por ejemplo identificar activos, amenazas, vulnerabilidades, consecuencias e impactos.
- Si bien cada actor del proceso conoce sus responsabilidades, no se tiene tan claro los propietarios, autorizadores, por ejemplo el propietario del proceso de monitoreo de infraestructura.
- No está claro las políticas de seguridad de la plataforma, por ejemplo las estandarizaciones en las adquisiciones.
- No se tiene identificado en su totalidad todas las partes interesadas en este proceso.
- Se identificaron las capacidades en la gestión de base de datos.

Plan de acción

- Estandarización en las adquisiciones de la infraestructura.
- Reforzar en las capacidades del manejo de la infraestructura estandarizada.
- Debe realizarse talleres de gestión de riesgos y comunicar las responsabilidades.
- Comunicar las operaciones de los procesos y sus relaciones con otras.

Conclusiones

Luego de estas iteraciones se han obtenido las siguientes conclusiones:

1. El proceso de autoevaluación nos ayuda a identificar oportunidades de mejoras.

2. No se debe confundir que el proceso de autoevaluación sirve para prepararse para las auditorias.

3. Se debe ejercer los principios de:
   Transparencia, con la finalidad de visualizar las actividades de las operaciones de los procesos de tecnologia, tal como se estan operando, sin ocultar algunos no-cumplimientos.
   Inclusión, que participen todos las partes interesadas e interesados, todos los niveles de la operación del proceso.
   Democratico, hacer participar a todos en el taller y tomar en cuenta todas las opiniones con la finalidad de identificar riesgos, controles, cumplimiento, estandarización y otros necesarios para la autoevaluación.

4. Tener claridad en el proceso y conocer los objetivos, alcances y actores que participan en las operaciones del proceso.

5. Las respuestas del cuestionario debe ser un consenso de todos los que operan el proceso y no la opinion de uno de ellos.

6. Las personas que participan en los talleres, deben conocer los principios de la gestión de riesgos.

7. Las personas deben identificar los indicadores de sus operaciones con la finalidade determinar la eficacia de los miemos en base a los objetivos del proceso.

8. Los talleres de autoevaluación deben ejecutarse periodicamente, de acuerdo a un plan establecido anualmente.

9. Es necesario que los participantes conozcan todos los procedimientos del proceso y si es posible explicarles, y hacerle notar cuales son los roles y responsabilidades.

10. Se cuenta con una matriz donde se detallan los cuestionarios para cada proceso y además se tienen los criterios para responder el cuestionario.

11. La persona que deben llevar el Taller es el dueño del proceso, y debe tener las habilidades de conducción del taller y las tecnicas aplicadas (Tormenta de ideas).

5.3 Checklist de Autoevaluación

El presente checklist nos permitirá mantener las evidencias de los controles por proceso y evitar la falta de la misma. Cabe recordar que la certificación SOX se renueva anualmente.

5.3.1 Criterio de Autoevaluación.

Con la finalidad de estandarizar los criterios de evaluación se implementó los siguientes criterios.

Tabla 30 Criterio de Autoevaluación.

	1. Nivel de comunicación de los riesgos y controles, sus objetivos, alcances.	2. Nivel de entendimiento de la asignación de roles y responsabilidades en el proceso de gestión de riesgos y la operación de los controles.	3. Nivel de cumplimiento de los roles y responsabilidades en el proceso de gestión de riesgos y la operación de los controles.	4. Niveles de monitoreo y revisión de los riesgos y controles, en base a los puntos de control y evidencias.	5. Validar los niveles de sensibilización y competencias en el proceso de gestión de riesgos y la operación de los controles.
	Posibles causas: No existen planes de comunicación, no están claros el entendimiento de los riesgos, no participo en los análisis	Posible causas: No se cuentan con procedimientos claros y entendibles, los procedimientos son complejos, mayor conocimiento de mis roles y	Posibles causas: No existe suficiente capacitación, no cuenta con herramientas que me faciliten el cumplimiento, demasiados controles en mis operaciones.	Posibles causas: No se generan las evidencias que ayuden a monitorear nuestras operaciones, no tenemos tiempo de monitorear nuestras operaciones.	Posibles causas: No hay un plan sobre la sensibilización, no hay un plan de competencias, no llevo cursos de sensibilizaci

	de riesgos.	responsabilidades			ón, no llevo cursos para mejorar mis capacidades.
Muy Alto	Existe un plan de comunicación de riesgos y controles a todos los niveles, con objetivos, documentado, e indicadores	Los procedimientos que participo están documentados y comunicados, y se entiende claramente mis roles y responsabilidades	Cumplo en su totalidad los roles y responsabilidades que se me han asignado	Realizo constantemente un monitoreo y revisión de los riesgos y controles de mis operaciones	Valido los niveles de sensibilización y competencia, y constantemente los incremento
Alto	Existe un plan de comunicación que llega a algunos niveles	Algunos procedimientos esta documentados y comunicados, y entiendo parcialmente mis roles y responsabilidades	Cumplo en su mayoría los roles y responsabilidades pero a veces lo hago con bastante dificultad	Realizo un monitoreo y revisión de los riesgos y controles de algunas operaciones	Valido los niveles de sensibilización y competencia, pero trato de incrementar mis niveles
Medio	Existe una comunicación de los riesgos y controles	Algunos procedimientos están documentos pero no comunicados pero conozco mis roles y procedimientos por intuición	Tengo dificultades para cumplir mis roles y responsabilidades	Realizo un monitoreo y revisión de los riesgos y controles en forma muy remota	Eventualmente valido los niveles de sensibilización y competencias
Bajo	Tienen conocimiento de los riesgos y controles a bajo nivel	No tengo conocimiento de todos mis procedimientos y mis roles y responsabilidades no están claras	Cumplo con algunos roles y responsabilidades, debido a que son dificultosos	Tengo la intención de realizar un monitoreo y revisión de los riesgos y controles de mis operaciones, pero no lo hago	Muy rara vez valido mi nivel de sensibilización y competencia
Muy Bajo	No tienen conocimiento de los riesgos y controles	No tengo entendimiento de mis roles y responsabilidades	Mayormente no cumplo mis roles y responsabilidades por diferentes causas (capacidad, dificultoso y otros)	No hago un monitoreo y revisión de los riesgos y controles porque no tengo tiempo	No valido mi nivel de sensibilización y competencia

Fuente: Elaboración propia.
Para cada proceso involucrado es necesario realizar el checklist de autoevaluación.

Tabla 31 Checklist Proceso – Riesgo Asociado.

Objetivo	Proceso	Procedimiento	Riesgos Asociados
Proteger la plataforma de infraestructura tecnológica ante amenazas internas y externas	Seguridad en Plataforma	Monitoreo de Seguridad e Infraestructura Actualización de antivirus Actualización de parches de seguridad Adquisición, implementación y mantenimiento de infraestructura	Ataques a la infraestructura tecnológica interna y externa. Errores en la configuración operativa y de seguridad de la infraestructura tecnológica. Códigos maliciosos en los equipos y la red. Paralizaciones de los equipos más críticos de la infraestructura tecnológica.
Controlar los cambios en los sistemas de información ante riesgos que pueden afectar a la organización.	Control de Cambios	Gestión de cambios. Definición de ambientes controlados para pruebas. Migración de datos. Respaldo y Restauración. Monitoreo de aplicativos en producción- pos implementación.	Paralizaciones o mal funcionamiento producidos por los cambios de los sistemas de información. Interrupción en los procesos del negocio. Una mala operación en el pase a producción. Mal monitoreo en las pruebas de los cambios en los sistemas de información.
Proporcionar información precisa sobre la configuración TI a todos los diferentes procesos de gestión.	Gestión de activos y configuraciones	Gestión de activos y configuraciones	Mal diseño de un sistema de información, al no tomar bien las configuraciones de los componentes de TI. Mala operación de los activos de tecnología de información. Paralizaciones en la infraestructura tecnológica en la gestión de incidentes. Mala gestión de problemas.

Obtener una mayor calidad de los servicios con Terceros en un precio adecuado.	Servicios con Terceros	Gestión de proveedores de TI Gestión de niveles de Servicio Monitoreo de niveles de servicio	Malos acuerdos de servicios con los proveedores. Paralizaciones en nuestras operaciones que dependen de Terceros. Fallas en la seguridad en las operaciones con Terceros. Malos niveles de servicios operados por Terceros.
Es poner la tecnología al servicio de los clientes y usuarios.	Niveles de Servicio	Gestión de niveles de Servicio Monitoreo de niveles de servicio	Insatisfacción de los clientes del uso de la tecnología. Mala calidad en los servicios de tecnología. Fallas en el monitoreo de los niveles de servicios. Reclamos y quejas de los clientes y usuarios que pueden llegar a tener impactos legales.
Definir, planificar, documentar y difundir las operaciones de tecnología	Operaciones	Adquisición, implementación y mantenimiento de infraestructura Para la definición de ambientes controlados para pruebas Elaboración y difusión de manuales Operativos Respaldo y Restauración Gestión de tareas	Errores en las operaciones de implementación y mantenimiento de la infraestructura tecnológica. Fallas en las operaciones de respaldo de la información de los sistemas. Falta de claridad en las operaciones tecnológicas. Desconocimiento de las nuevas asignaciones en las operaciones tecnológicas.
Brindar un servicio de punto de contacto entre los usuarios y la gestión de servicios de tecnología de información	Mesa de Ayuda y Servicios de Campo	Gestión de mesa de ayuda	Mala respuesta en la comunicación de incidentes de tecnología de información. Inadecuada atención de los requerimientos de los usuarios. Insatisfacción de los usuarios en el uso de la tecnología. Inadecuada gestión de problemas.

Para garantizar un enfoque coherente y eficaz para la gestión de incidentes de TI y de seguridad de la información	Gestión de Incidentes de TI y Seguridad	Gestión de incidentes de seguridad de la información Gestión de incidentes de TI Gestión de mesa de ayuda	Paralizaciones de los servicios de tecnología que pueden ocasionar impactos en los procesos de negocio Fraudes producto a debilidades en la seguridad de los procesos Inadecuada comunicación de los incidentes de TI y de seguridad. Inadecuada respuesta de los incidentes debido a una mala priorización.
Monitorizar todos los sucesos importantes, con la finalidad de detectar y escalar condiciones para contribuir a una operación normal del servicio	Monitoreo	Monitoreo de Seguridad e Infraestructura	Saturación de los recursos tecnológicos Fallas en las operaciones en la infraestructura tecnológica. Inadecuada detección de eventos que pueden llegar a ser incidentes. Ataques interno o externo de la infraestructura tecnológica.
Mantener disponible y confiables los datos de los sistemas informáticos.	Administración de Datos	Respaldo y Restauración Mantenimiento de base de datos	No disponibilidad de los datos que soportan los sistemas informáticos. Datos no confiables en los sistemas informáticos. Mala manipulación de los datos de los sistemas informáticos. Fallas en el procesamiento de los datos de los sistemas informáticos.
Investigar las causas y determinar posibles soluciones de los problemas de los servicios de TI	Gestión de Problemas	Gestión de mesa de ayuda	Paralizaciones de los servicios de TI más críticos. Ausencia o mal escalamiento de los problemas en los servicios de TI. Inadecuada activación de los planes de contingencia. Falta de capacidad de respuesta del personal de TI ante un problema en los servicios.

Mantener la seguridad física de las áreas restringidas	Resiliencia y Seguridad Física	Monitoreo de controles ambientales y físicos del Centro de Cómputo	Accesos no autorizados en las áreas restringidas. Inadecuado ambientación en las Áreas de procesamiento de datos. Falta de monitoreo de los controles ambientales y físicos de las Áreas de procesamiento de datos. Ausencia y/o inadecuadas políticas de la seguridad física.

Fuente: Elaboración propia.

Todos los procesos definidos en la Tabla 5.5 son evaluados mediante el cuestionario siguiente:

Tabla 32 Evaluación de Procesos
Proceso :_____

	1. Nivel de comunicación de los riesgos y controles, sus objetivos, alcances.	2. Nivel de entendimiento de la asignación de roles y responsabilidades en el proceso de gestión de riesgos y la operación de los controles.	3. Nivel de cumplimiento de los roles y responsabilidades en el proceso de gestión de riesgos y la operación de los controles.	4. Niveles de monitoreo y revisión de los riesgos y controles, en base a los puntos de control y evidencias.	5. Validar los niveles de sensibilización y competencias en el proceso de gestión de riesgos y la operación de los controles.
¿Tienes conocimiento del proceso de Seguridad en Plataforma, y cuáles son sus procedimientos?					
¿Existe una comunicación adecuada entre el gestor de riesgos, propietarios del proceso y actores?					
¿Tienes conocimiento de los roles y responsabilidades en los procedimientos del proceso de Seguridad en Plataforma?					

¿Cumples con tus roles y responsabilidades consignados en los procedimientos que pertenecen al proceso de Seguridad en Plataforma?					
¿Tienes conocimientos de los riesgos y controles que operan en el proceso de Seguridad en Plataforma?					
¿Incrementas tus niveles de sensibilización y competencias en las operaciones del proceso de Seguridad en Plataforma?					
TOTALES					

Firma del
Responsable de Área

Firma del
Responsable del Proceso

Fuente: Elaboración propia.

Tabla 33 Resumen

							2015	
	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5	Resultados Esperados	Semestre 1	Semestre 2
Organización de Tecnologías de Información								
Estrategia de Tecnología								
Marco de Trabajo de los Procesos de Tecnología								
Gestión del Desempeño y de la Calidad								
Arquitectura Tecnológica								
Gestión de Talento Humano								
Cumplimiento de Políticas y Regulaciones								
Gestión de Proyectos								
Procesos de Gestión de Riesgos								
Marco de Gestión de Riesgos Tecnológicos								
Políticas de Riesgo Tecnológico								
Gestión de Riesgos								
Monitoreo de Riesgos								
Propiedad Clasificación de los Activos de Información								
Comunicación, Entrenamiento y Concientización								
Procesos de Gestión de Tecnología								
Administración de Accesos								
Desarrollo, Adquisición y Mantenimiento de Sistemas								
Seguridad en Plataforma								
Control de Cambios								
Gestión de Activos y Configuraciones								

Servicios con Terceros								
Niveles de Servicio								
Operaciones								
Mesa de Ayuda y Servicios de Campo								
Gestión de Incidentes de TI y Seguridad								
Monitoreo								
Administración de Datos								
Gestión de Problemas								
Resiliencia y Seguridad Física								

2015							
Semestra 1							
Acciones correctivas							
Semestre 2							
Acciones correctivas							

Fuente: Elaboración propia.

Tabla 34 Cronograma de Revisión de Procedimientos.

	1	2	3	4	5	6	7	8	9	10	11	12
Organización de Tecnologías de Información												
Estrategia de Tecnología												
Marco de Trabajo de los Procesos de Tecnología												
Gestión del Desempeño y de la Calidad												
Arquitectura Tecnológica												
Gestión de Talento Humano												
Cumplimiento de Políticas y Regulaciones												
Gestión de Proyectos												
Procesos de Gestión de Riesgos												
Marco de Gestión de Riesgos Tecnológicos												
Políticas de Riesgo Tecnológico												
Gestión de Riesgos												
Monitoreo de Riesgos												
Propiedad Clasificación de los Activos de Información												
Comunicación, Entrenamiento y Concientización												
Procesos de Gestión de Tecnología												
Administración de Accesos												
Desarrollo, Adquisición y Mantenimiento de Sistemas												
Seguridad en Plataforma												
Control de Cambios												
Gestión de Activos y Configuraciones												
Servicios con Terceros												
Niveles de Servicio												
Operaciones												
Mesa de Ayuda y Servicios de Campo												
Gestión de Incidentes de TI y Seguridad												
Monitoreo												
Administración de Datos												
Gestión de Problemas												
Resiliencia y Seguridad Física												

Fuente: Elaboración propia.

Capítulo 6
Conclusiones

Principales Problemas Identificados

- La implementación de la nueva cultura organizacional, que implica la participación de todas las áreas dentro de la organización orientado al cumplimiento de SOX, involucro una serie de capacitaciones que motivaran al personal a cumplir este nuevo reto.
- Se consideró inicialmente que todos los controles deben ser automatizados, pero la realidad es que no siempre pueden ser automatizados debido a que la relación costo-beneficio no es justificable.
- Se necesitó documentar muchos procedimientos que si se realizaban pero de manera informal.
- La generación de evidencias se consideró como parte de los objetivos de los actores involucrados.
- Inicialmente se identificó una carga adicional de trabajo pero en el transcurso de la implementación y puesta en funcionamiento esta carga se asimilo como tareas rutinarias a desarrollar.
- Muchos procesos de la organización requirieron soporte para la gestión del cambio, debido a los nuevos controles implementados en estos procesos.
- No se tomó en cuenta la resistencia al cambio de algunos colaboradores debido a que estaban acostumbrados a tareas operativas repetitivas. Este punto se solucionó con capacitaciones focalizadas.
- Tener una visión de cómo el negocio se verá a futuro y lo que se implemente ahora permita ser flexible para su reutilización.
- Muchas áreas consideraron que el tema de SOX era netamente TI, sin embargo el enfoque es todo lo contrario, TI da soporte a los procesos del negocio de acuerdo a los apetitos de riesgo que se definan.
- La implementación de estos nuevos controles no deben ser visto de forma aislada si no debe ser vista de acuerdo al contexto que pertenece y las conexiones que puede tener con otros procesos. Implementaciones aisladas trae consigo una falta de consistencia en la evidencia presentada.

Conclusiones

- El proceso de certificación SOX es un proceso de re-acreditación anual, motivo por el cual los controles descritos en cada proceso deben alcanzar un nivel de madurez en el tiempo.

- No existe una metodología única para certificarse en SOX mediante la utilización de COBIT, cada organización tiene diferentes escenarios y diferentes apetitos de riesgos en las cuales hay que desarrollar diversos tipos de controles que no necesariamente los actuales aplican a otras organizaciones. Sin embargo el punto 4.3.5 Plan de Mitigación de Riesgos es un buen punto para iniciar el levantamiento de información en otras organizaciones.

- A pesar de ser un tema tecnológico, el factor humano es la pieza clave de aplicaciones de controles, motivo por el cual la capacitación constante en tema de seguridad y concientización son vitales para alcanzar los objetivos deseados.

- Al aplicar el presente modelo de controles, nos permite tener un alto nivel de gobierno corporativo para los temas de tecnología de información e incrementa el valor de la organización.

- En el proceso de Administración de Accesos se logra una identificación única para cada colaborador de la organización de esta manera la trazabilidad ante un incidente es fácil de evidenciar, adicionalmente mediante capacitaciones se logra formar conciencia que el identificador que utilizan es único y no se puede ceder a un tercero, es el único vínculo entre el colaborador y la organización.

  Se define una nueva sección dentro de TI, denominada Administración de Accesos, la cual en conjunto con el área de Seguridad realizan las revisiones periódicas de acceso.

- Se establece lineamientos para el intercambio de información de acuerdo a su clasificación, permitiendo de esta manera salvaguardar la información confidencial de la organización.

- La eliminación de información se realiza mediante procedimientos establecidos prestando especial interés en activos de información con clasificación de información confidencial o secreto.

- En la gestión de cambio se identifica claramente un cambio de emergencia de un cambio normal, inicialmente todos los cambios eran considerados de emergencia pero en realidad no eran emergencia sino urgencias que cae en la categoría de cambios normales, esta transformación se logra mediante una capacitación constante a todos los actores del proceso.

- En el tema de calidad de desarrollo de software no se encontró brecha sin embargo es el único proceso que está al 100% debido a la madurez solicitada que es 2, sin embargo se recomienda en la siguiente recertificación que el presente proceso suba a un nivel 3.

- Toda organización no está libre de un incidente de Seguridad y de TI, motivo por el cual la comunicación a los interesados debe ser clara y a tiempo, con la finalidad de mitigar el impacto de dicho incidente o tomar medidas alternas para no ver afectado el servicio involucrado, así mismo muchos incidentes se convierten en problemas los cuales deben ser elevados rápidamente a los especialistas internos o externos de la organización con el fin de evitar pérdidas económicas.

- Cuando hablamos de activos de información también se considera al ser humano, motivo por el cual se debe contar con un plan de capacitación que permita al colaborador enfrentar los nuevos retos que demanda la organización.

- La segregación de funciones debe estar claramente definida para evitar que el que ejecute no sea la misma persona que autoriza, con esto tipo de control minimizamos el riesgo de fraude.

- La implantación de indicadores de gestión en el área de tecnología hace visible las fortalezas y debilidades del área, así mismo su alineación a la estrategia del negocio.

- La definición de los procesos de TI permita tener una estructura que soporte los requerimientos del negocio e incrementa la agilidad para responder a auditorías internas, externa y entes reguladores como la SBS "Superintendencia de Banca y Seguros".

- El monitoreo de seguridad e infraestructura es fundamental como parte de las evidencias de la salud de gobierno de TI, contar con un ente externo que realice el monitoreo como un SOC "Security Operational Center" y un NOC "Network Operational Center" permitirá tener una línea base en cuanto a futuros incidentes.

- Contar con un ambiente controlado para pruebas permitirá medir el impacto que se pueda tener en un ambiente productivo. Cabe mencionar que tanto los ambientes de pruebas como los de producción deben estar homologados, esto quiere decir desde sistema operativo, memoria, procesador, parches, etc.

- Mantener actualizado un inventario de activos de información es necesario debido a permite realizar el análisis y evaluación de riesgos de seguridad de información, con lo cual la criticidad de un activo puede cambiar en las revisiones anuales.

- Se deben aplicar controles de accesos rigurosos en áreas restringidas como el Centro de Cómputo, las autorizaciones para su ingreso deben estar difundidas entre los interesados con la finalidad de evitar disrupciones en trabajos a realizar en dicha área. Así mismo deben haber lineamientos claros de que actividades son permitidas y cuales no se deben realizar en este tipo de instalación.

- La gestión de seguridad en plataforma va de la mano con el tema de monitoreo, pero adicionalmente se considera temas de seguridad perimetral en la cual se debe recalcar que toda conexión externa debe estar mediada con algún dispositivo de

seguridad, la utilización de software original implementado sus respectivos parches permite ser menos vulnerables en caso de un incidente.

- Se deben mantener acuerdos de niveles de servicios con las áreas del negocio estos contratos deben ser revisados en forma anual y el compendio de todos estos servicios prestados por TI deben encontrarse en un catálogo de servicios el cual debe ser de conocimiento de las áreas interesadas.

- Cualquier requerimiento hacia el área de TI, debe ser realizado mediante un único punto de contacto, en el presente caso lo realiza la mesa de ayuda, esto permitirá hacer un seguimiento a los requerimientos solicitados.

- Para el caso de proveedores se debe contar con una matriz que identifique los proveedores con sus respectivos SLA's esto con la finalidad de tener un mapeo directo de todos los proveedores que interactúan con el área de TI.

- Todo activo de información debe estar reflejado en la CMDB "Change Management Data Base" con la finalidad de realizar su gestión de cambio formal, la cual puede ser un cambio normal o de emergencia de esta manera reducimos incidentes presentados por cambios no planificados.

- El PETI "Plan Estratégico de Tecnologías de Información" debe ser actualizado en el último trimestre del año en conjunto con el plan de capacidad para servir como entrada al presupuesto anual del siguiente año.

- Tanto el Centro de Cómputo principal como el alterno deben cumplir tanto con controles físicos, ambientales y de seguridad que permitan ser parte del plan de continuidad de la organización.

- En toda actividad podemos identificar riesgos y las tecnologías de información no son ajenas a estos temas, las organizaciones tienen que ser flexibles en este mundo cambiante, muchos riesgos se podrán mitigar pero otros se tendrá que aceptar y vivir con ellos, estos últimos son considerados como riesgos residuales, lo que no se debe hacer es evitar los riesgos sino todo lo contrario se debe gestionar.

- Finalmente la autoevaluación[6], es recomendable realizarla anualmente antes de la re-certificación con la finalidad de monitorear algunas brechas o identificar procesos que por su naturaleza alcancen un grado de madurez mayor.

[6] Se puede encontrar información en punto 5.3 Checklist de Autoevaluación

Bibliografía.

1. Autor: Anand, Sanjay.
   Año: 2007.
   Título: Essentials of Sarbanes-Oxley.
   País: United States of America.
   Editorial: Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
   ISBN: 978-0-470-05668-4

2. Autor: IT Governance Institute.
   Año: 2013.
   Título: COBIT 5 A Business Framework for the Governance and Management of Enterprise IT.
   País: Printed in the United States of America.
   Editorial: IT Governance Institute .
   ISBN: 978-1-60420-237-3

3. Autor: INDECOPI
   Año: 2008.
   Título: Norma Técnica Peruana NTP-ISO/IEC 27001 2008.
   País: Perú.
   Editorial: INDECOPI.
   WEB: http://bvirtual.indecopi.gob.pe/normas/isoiec27001.pdf.
   Fecha: 03/01/2014

4. Autor: Colin Rudd.
   Año: 2005.
   Título: An Introductory Overview of ITIL.
   País: UK United Kingdom.
   Editorial: itSMF Ltd.
   ISBN: 0-9543521-9-X

5. Autor: ISO (International Organization for Standardization).
   Año: 2011.
   Título: ISO 27002.

País: España.
Web: http://www.iso27000.es/download/ControlesISO27002-2005.pdf.Fecha:10/01/2014.

6. Autores: Jan van Bon, Arjem de Long, Axel Kolthof, Mike Pieper, Ruby Tjassing, Annelies van der Veen, Tineke Verheijem.
   Año:2012
   Título: Gestión de Servicios de TI basado en ITIL V3.
   País: Holanda
   Editorial: Van Haren Publishing
   ISBN: 978 90 87531065

7. Autor: R&CSA - ISACA
   Año: 2014
   Título: IT Governance Institute COBIT 4.1.
   Web: http://www.isaca.org/Journal/Past-Issues/2001/Volume-1/Pages/Risk-and-Control-Self-Assessment-RCSA-.aspx.

8. Autor: Gonzalo Ulloa Villegas. Ph.D Decano de la Facultad de Ingeniería.
   Año:2014
   Título: Revista S&T, 9(17), 23-53.
   Editorial: Universidad Icesi – Cali - Colombia

Anexos

Anexo A Matriz por Dominios de COBIT

Tabla A1. Organización de TI

COBIT 4.1 Requerimiento de Control	Soporte Documental de los Controles Implementados	Control	Descripción del Control	Tipo de Control	Naturaleza del Control	Frecuencia	Evidencia	Medio de retención de la evidencia	Responsable	Área Responsable del Control	Riesgos Mitigados
Control de Referencia Cobit 4.1	*Proceso/Procedimientos/ Manuales/Guías/Políticas*	*Actividad de Control (Control Activity - Key Control)*	*Breve descripción del control*	*Preventivo/Correctivo/ Detectivo*	*Manual/Auto matizado*	*Tiempo Real/Tiempo Base/Diario/Semanal/ Mensual/Anual*	*Soporte de Evidencia del Control*	*Donde se almacena la evidencia y el soporte documental*	*Nombre de la Persona Responsable del Control*	*Área Responsable del Control*	*Riesgos que mitiga el control*
PO1 Define a Strategic IT Plan											
PO4 Define the IT Processes, Organization and Relationships											
PO6 Communicate Management Aims and Direction											

COBIT 4.1 Requerimiento de Control	Soporte Documental de los Controles Implementados	Control	Descripción del Control	Tipo de Control	Naturaleza del Control	Frecuencia	Evidencia	Medio de retención de la evidencia	Responsable	Área Responsable del Control	Riesgos Mitigados
PO7 Manage IT Human Resources											
PO9 Assess and Manage IT Risks											
AI6 Manage Changes											
ME1 Monitor and Evaluate IT Performance											
ME2 Monitor and Evaluate Internal Control											
ME3 Ensure Compliance With External Requirements											
ME4 Provide IT Governance											

Fuente: Elaboración propia.

Tabla A2. Ciclo de Vida de Software

COBIT 4.1 Requerimiento de Control	Soporte Documental de los Controles Implementados	Control	Descripción del Control	Tipo de Control	Naturaleza del Control	Frecuencia	Evidencia	Medio de retención de la evidencia	Responsable	Área Responsable del Control	Riesgos Mitigados
Control de Referencia Cobit 4.1	*Proceso/Procedimientos/ Manuales/Guías/Políticas*	*Actividad de Control (Control Activity - Key Control)*	*Breve descripción del control*	*Preventivo/Correctivo/Detectivo*	*Manual/Automatizado*	*Tiempo Real/Tiempo Base/Diario/Semanal/Mensual/Anual*	*Soporte de Evidencia del Control*	*Donde se almacena la evidencia y el soporte documental*	*Nombre de la Persona Responsable del Control*	*Área Responsable del Control*	*Riesgos que mitiga el control*
PO8 Manage Quality											

Fuente: Elaboración propia.

Tabla A3. Infraestructura Tecnológica

COBIT 4.1 Requerimiento de Control	Soporte Documental de los Controles Implementados	Control	Descripción del Control	Tipo de Control	Naturaleza del Control	Frecuencia	Evidencia	Medio de retención de la evidencia	Responsable	Área Responsable del Control	Riesgos Mitigados
Control de Referencia Cobit 4.1	*Proceso/Procedimientos/ Manuales/Guías/Políticas*	*Actividad de Control (Control Activity - Key Control)*	*Breve descripción del control*	*Preventivo/Correctivo /Detectivo*	*Manual/Auto matizado*	*Tiempo Real/Tiempo Base/Diario/Semanal /Mensual/Anual*	*Soporte de Evidencia del Control*	*Donde se almacena la evidencia y el soporte documental*	*Nombre de la Persona Responsable del Control*	*Área Responsable del Control*	*Riesgos que mitiga el control*
AI3 Acquire and Maintain Technology Infrastructure											
AI4 Enable Operation and Use											
AI7 Install and Accredit Solutions and Changes											
DS1 Define and Manage Service Levels											
DS2 Manage Third-party Services											

COBIT 4.1 Requerimiento de Control	Soporte Documental de los Controles Implementados	Control	Descripción del Control	Tipo de Control	Naturaleza del Control	Frecuencia	Evidencia	Medio de retención de la evidencia	Responsable	Área Responsable del Control	Riesgos Mitigados
DS5 Ensure Systems Security											
DS8 Manage Service Desk and Incidents											
DS9 Manage the Configuration											
DS10 Manage Problems											
DS11 Manage Data											
DS12 Manage the Physical Environment											
DS13 Manage Operations											

Fuente: Elaboración propia.

Anexo B Administración de Accesos

Anexo B1. Descripción del Procedimiento de Creación de Cuentas de Usuario

Este procedimiento está basado en el ciclo de vida de un usuario dentro de la empresa. Incluye usuarios internos y externos.

La creación de cuentas de usuario, comprende a todos los aplicativos de negocio, sistemas operativos y servicios de red de la compañía.

Para el proceso de creación de cuentas de usuario, se debe considerar lo siguiente:

- Perfiles:
  Los accesos se crean en base a un perfil definido y aprobado por el Propietario del Activo, los cuales son administrados a nivel del Administrador de Accesos.

- Autenticación de usuario:
  En las aplicaciones se cuenta con niveles de seguridad para la autenticación del colaborador con un usuario y contraseña basado en la política de seguridad.

- Repositorio centralizado:
  Se cuenta con el servicio de mesa un sistema de gestión de requerimientos (Service Desk) que administra las solicitudes de acceso y aprobaciones por las gerencias usuarias y los propietarios de activos.

- Identificación de Cuenta Única:
  Así mismo se otorga una cuenta de acceso única al usuario el cual permite su identificación en todos los sistemas de información.

- Usuarios Externos o Temporales:
  Se crean cuentas de servicios externos o temporales con la aprobación del Propietario del Activo, lo cual permite identificar su actividad en los sistemas de TI de la compañía.

  Las cuentas para externos son creadas a solicitud del Jefe del Área, responsable del servicio que brinda, quien enviará una solicitud a SOS indicando los datos personales del o los usuario, lista de aplicaciones y/o activos así como la fecha inicio y fin de la solicitud de acuerdo al tiempo de duración del servicio externo.

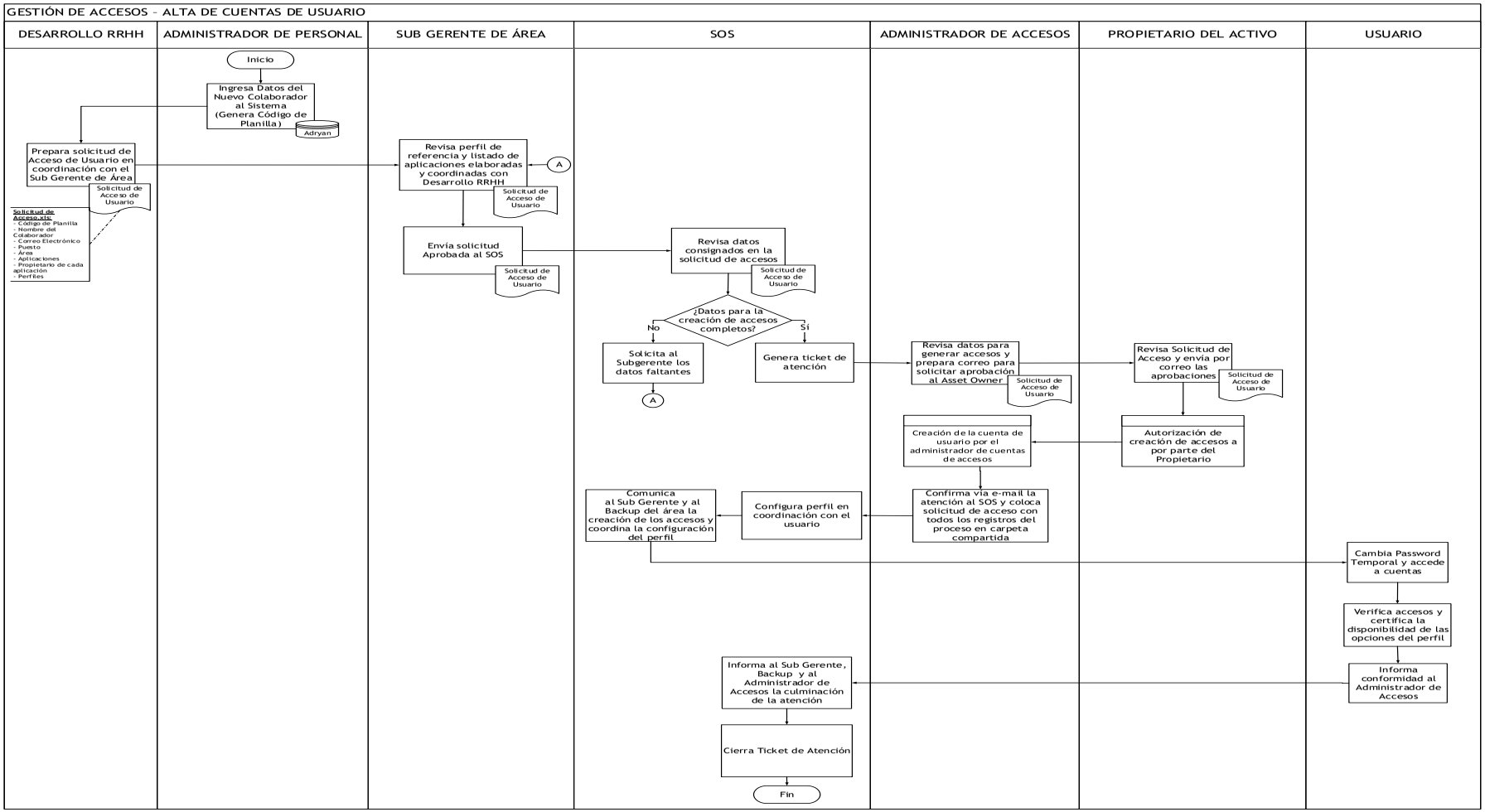


Figura B1. Gestión de Accesos – Alta de Cuentas de Usuario.

Descripción del Procedimiento Revisión de Accesos

Las revisiones periódicas de las cuentas de usuarios, genéricas, privilegiadas, de grupo y de servicio son realizadas para garantizar que los derechos de acceso se encuentran asignados de manera adecuada, que continúan alineados a las necesidades del negocio y las funciones que desempeñan los usuarios de acuerdo al puesto de trabajo.

Periodicidad de Revisión de Cuentas

La periodicidad de las revisiones es la siguiente:

- Revisión Mensual:
  - Bajas/Retiro de cuentas de acceso en tiempo (bloqueo y eliminación)
  - Revisión de lista de cambio de puestos (movimientos) obtenidos vía consulta al Sistema de Planillas.
  - Revisión de altas, modificaciones y bajas obtenido vía consulta al Sistema de Planillas.
  - Revisión de cuentas temporales.
- Revisión Trimestral:
  - Inexistencia de cuentas de acceso genéricas no autorizadas.
  - Usuarios privilegiados a nivel de plataforma.
  - Cuentas de servicio.
- Revisión Anual:
  - Usuarios privilegiados por aplicación.
  - Revisión de accesos concedidos y activos (Cuentas de accesos de Sistemas/Aplicaciones, Infraestructura, Cuentas Privilegiadas, Administradoras y de Servicio) con asignación de un usuario único por aplicación.
  - Depuraciones de cuentas de acceso (históricos).
  - Revisión de perfiles.

Adicionalmente el Propietario del Activos debe mantener en una matriz el control de accesos y privilegios que deberían estar configurados por cada cuenta de usuario de tal manera que sea un complemento para la revisión de cuentas.

El Administrador de Accesos debe mantener un inventario de las diferentes cuentas de acceso que hayan sido creadas.

El resultado de todas las revisiones realizadas, deben ser comunicadas al Oficial de Seguridad de la Información.

Desarrollo del Diagrama de Flujo de Revisión de Accesos (Anual/Trimestral)

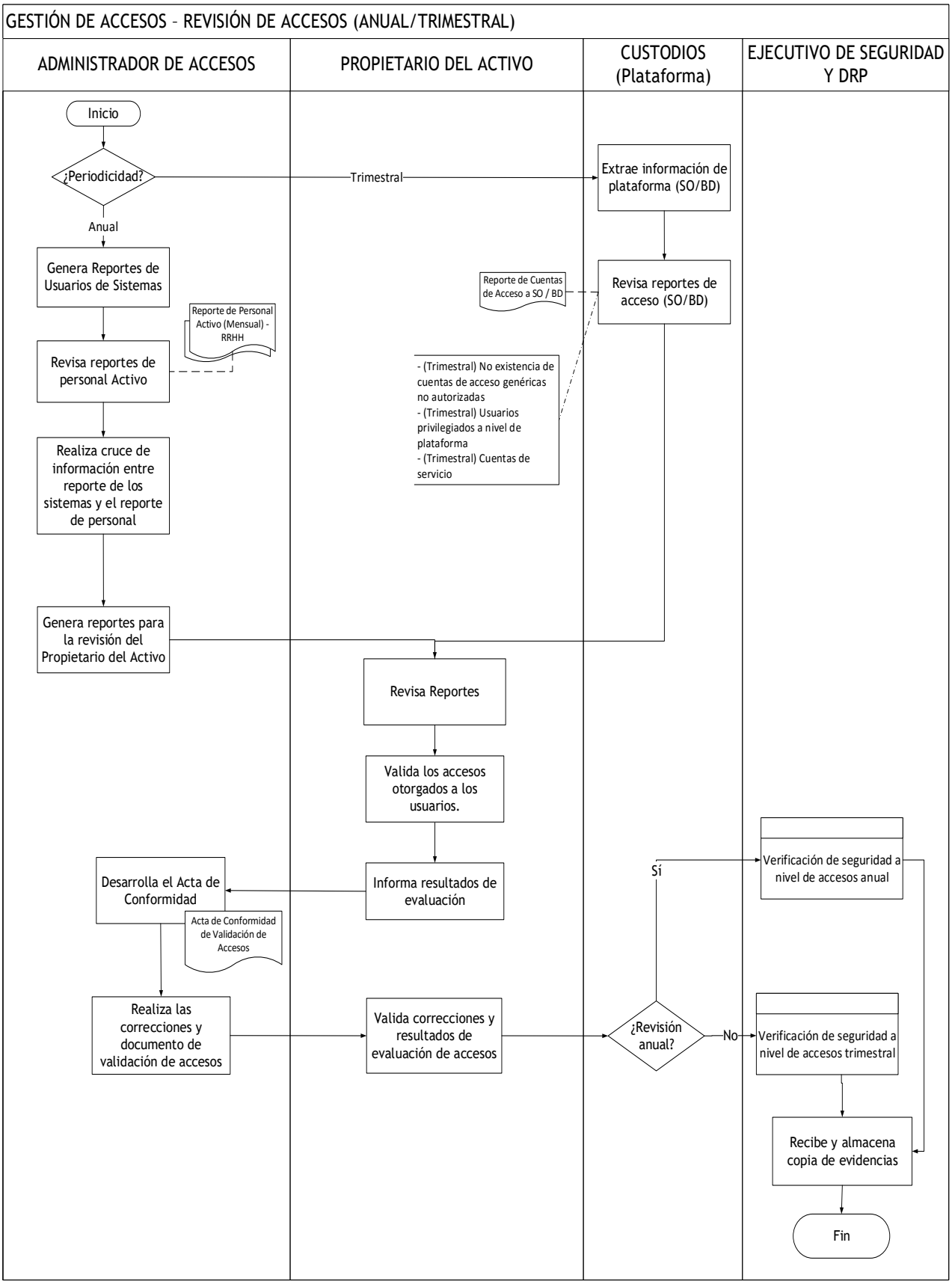


Figura B2. Gestión de Accesos – Revisión de Accesos (Anual/Trimestral)

Diagrama de Flujo Detallado del Proceso de Revisión de Accesos (Mensual)

Este procedimiento se aplica en forma mensual a las cuentas de usuarios activos, altas, modificaciones de perfil, cambios de puesto y ceses.

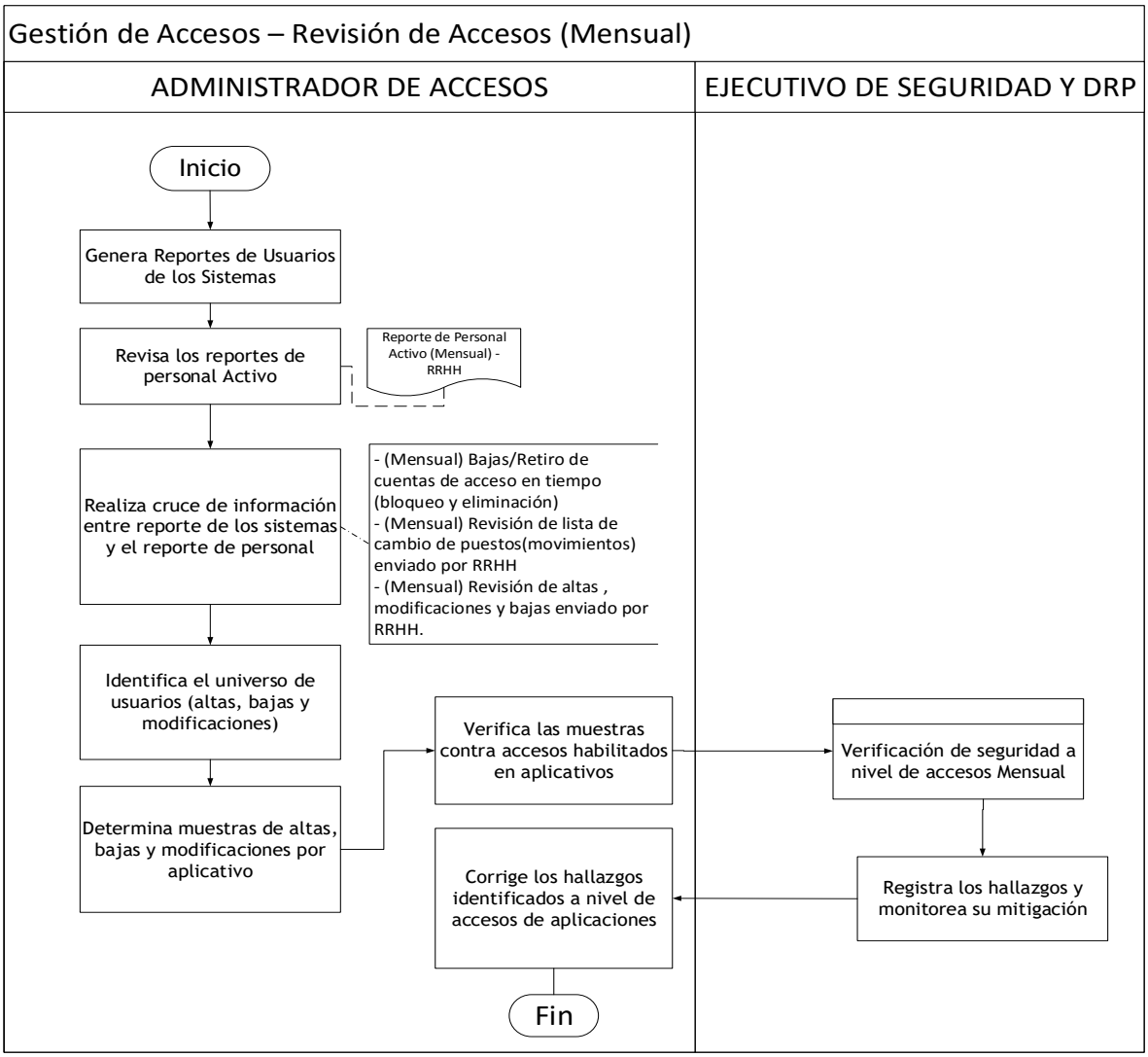


Fig. B3 Gestión de Accesos – Revisión de Accesos Mensual

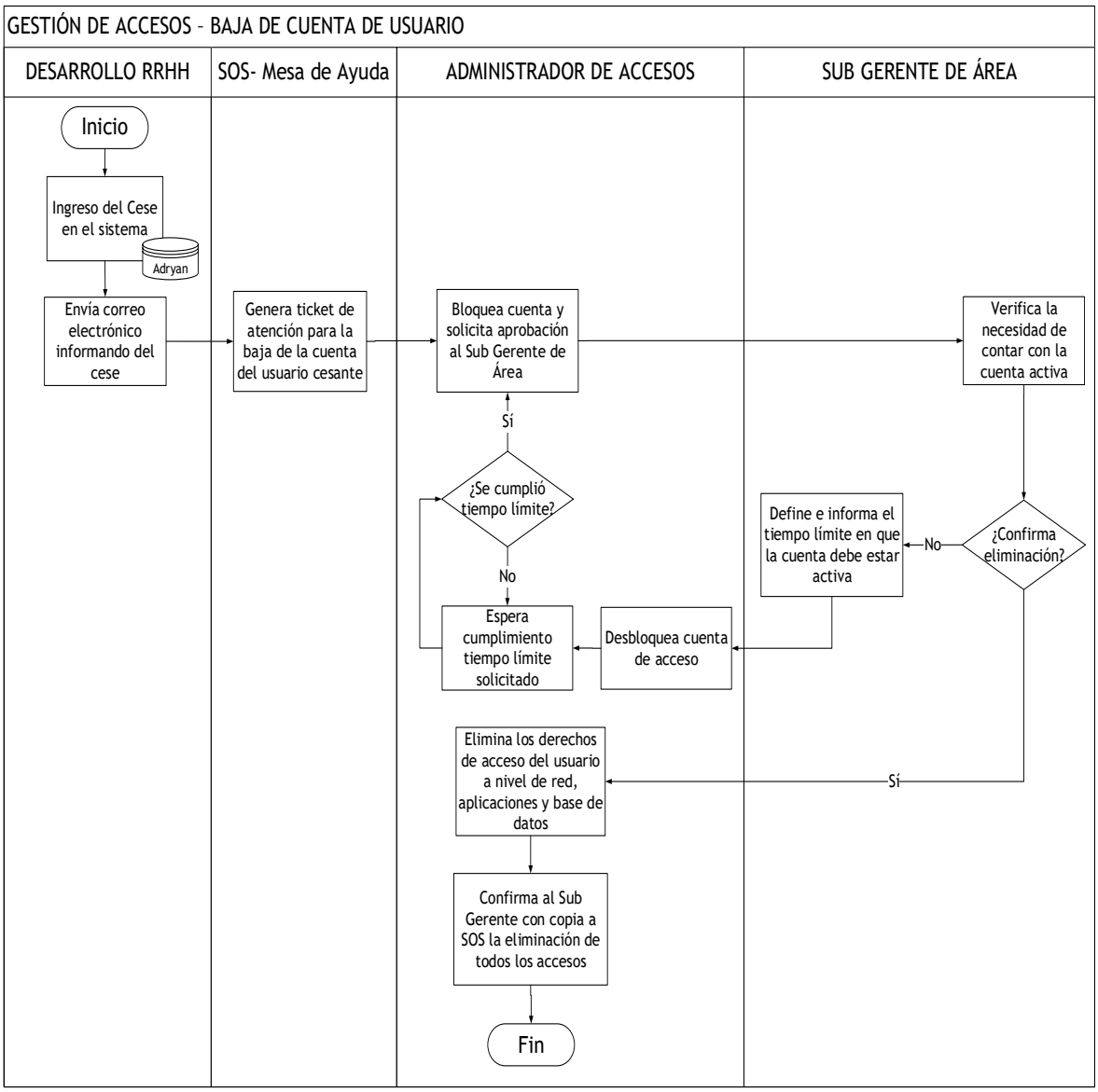


Figura B4. Gestión de Accesos - Baja de Cuenta de Usuarios.

Descripción del Procedimiento de Accesos a Producción para Personal de Desarrollo

Los accesos a producción para el personal de desarrollo son solicitados por los usuarios solo cuando se requiere soporte especializado.

El personal de sistemas / desarrollo puede acceder únicamente en forma de lectura al ambiente de producción y su trabajo debe ser netamente de soporte.

El periodo de acceso debe ser justificado y en ningún caso exceder de tres días.

El acceso de desarrolladores a ambientes de producción se encuentra prohibido con la excepción de casos en los cuales la 1era y 2da línea de soporte no pueda resolver el problema (cambios de emergencia).

Diagrama de Accesos a Producción para Personal de Desarrollo

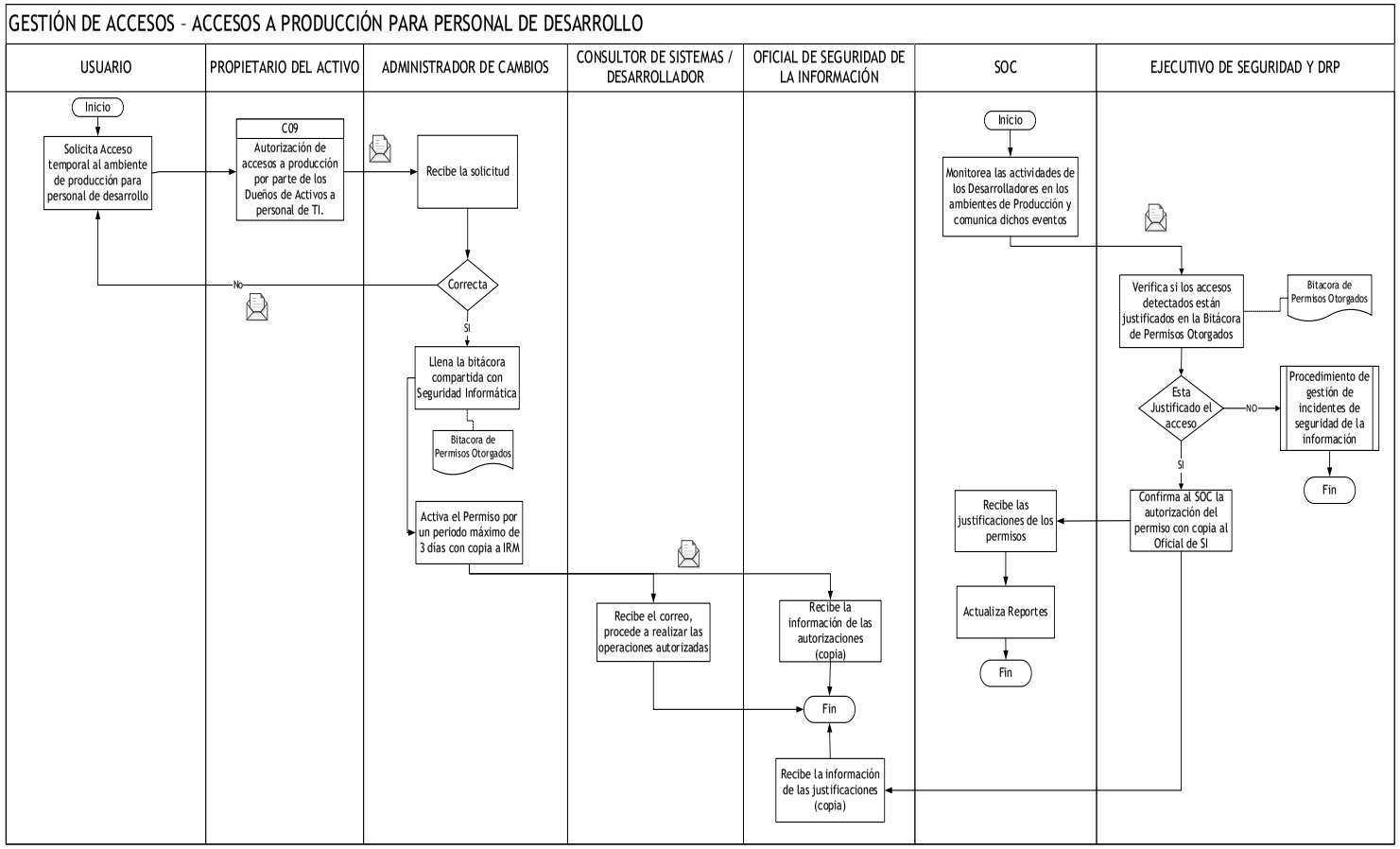


Fig. B5 Gestión de Accesos – Acceso a Producción para Personal de Desarrollo

Anexo C Administración de Datos

Tabla C1. Autorización de Uso de Medios.

Acta de autorización de usuarios que usan medios de almacenamiento, comunicación externa y equipos y medios móviles (Esta autorización debe estar considerada al momento de liberar de algún bloqueo – uso de DLP)

Fecha:

ITEM	Medios de almacenamiento y comunicación externa; equipos y medios móviles							DESCRIPCIÓN	USUARIO	NOMBRE DEL PROPIETARIO	CONTROL IMPLEMENTADO
	Disco Virtual	Correo de uso externo	Memoria USB	CDs, DVDs, cintas y	Tablets, Portátil	Celular	Otros				

Fuente: Elaboración propia.

Eliminación Segura de Medios

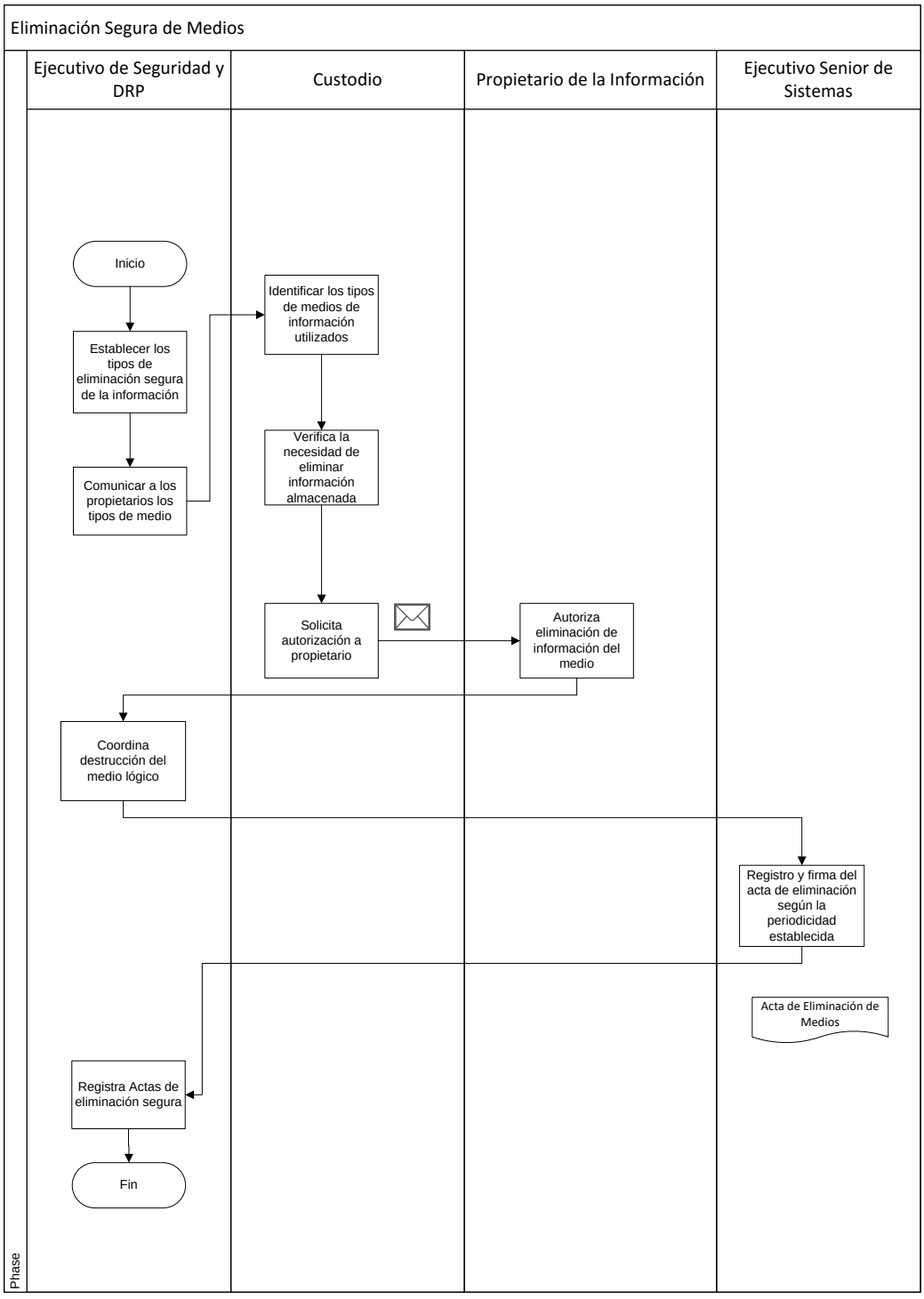


Figura C1. Eliminación Segura

Fuente: Elaboración propia.

Tabla C2 Acta de Eliminación Segura de la Información

En las instalaciones de la AFP sito en _____, a los (días) días del mes de (mes) de (año) siendo las (hora) a.m. / p.m., se reunieron los colaboradores: (NOMBRE DE LOS COLABORADORES) en la Oficina de (NOMBRE DE LA OFICINA), con el fin de dar inicio al proceso de eliminación de la información almacenados en los medios de información identificados en esta acta y aprobadas por sus propietarios, se procede a la destrucción de la siguiente información:

ITEM	MEDIO DE ALMACENAMIENTO					DESCRIPCIÓN	PROPIETARIO	MÉTODO DE ELIMINACIÓN
	Disco	Memoria USB	CDs, DVDs, similar	Cinta magnética	Otros			

Fuente: Elaboración propia.

Método de eliminación: Software de eliminación segura, Destrucción física, Imán y otros.

Firmas de las personas que intervienen en el proceso.

Descripción del procedimiento de respaldo y restauración

El procedimiento de respaldo y restauración garantiza que se restablezca la operación normal de servicio lo antes posible y se minimice el impacto al negocio**.**

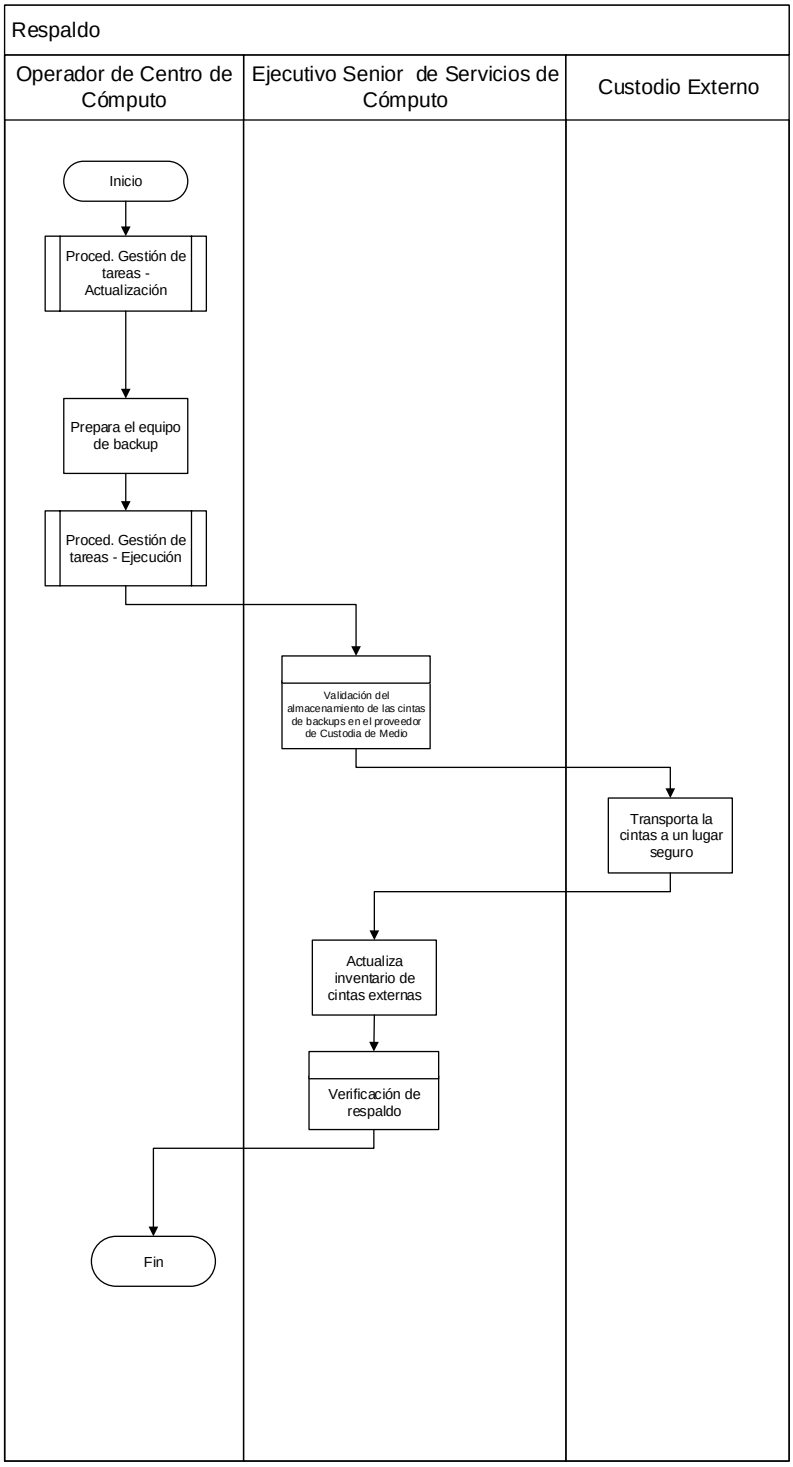


Fig. C2 Respaldo
Fuente: Elaboración propia

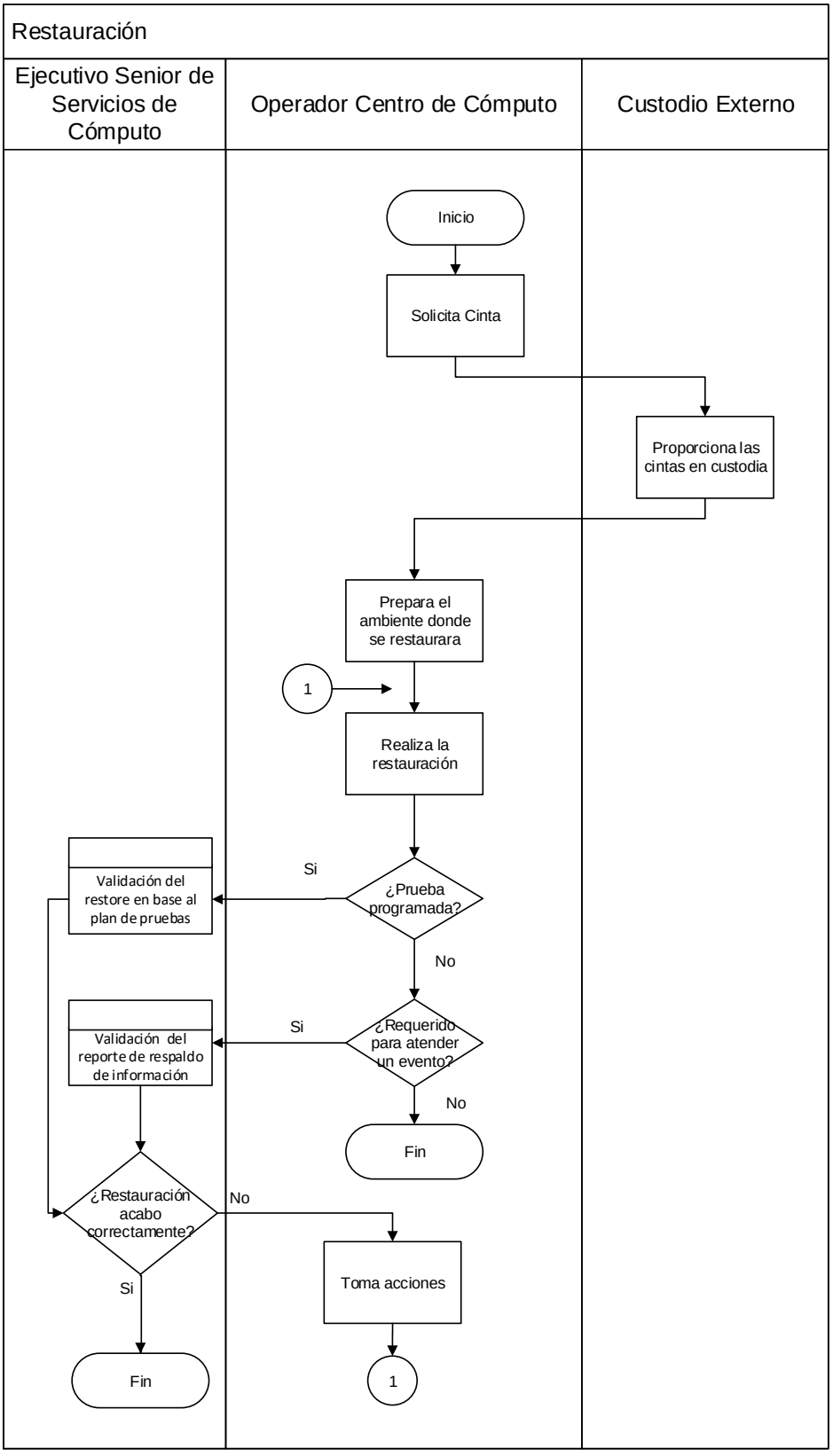


Fig.C3 Restauración
Fuente: Elaboración propia

Anexo D Gestión de Control de Cambios

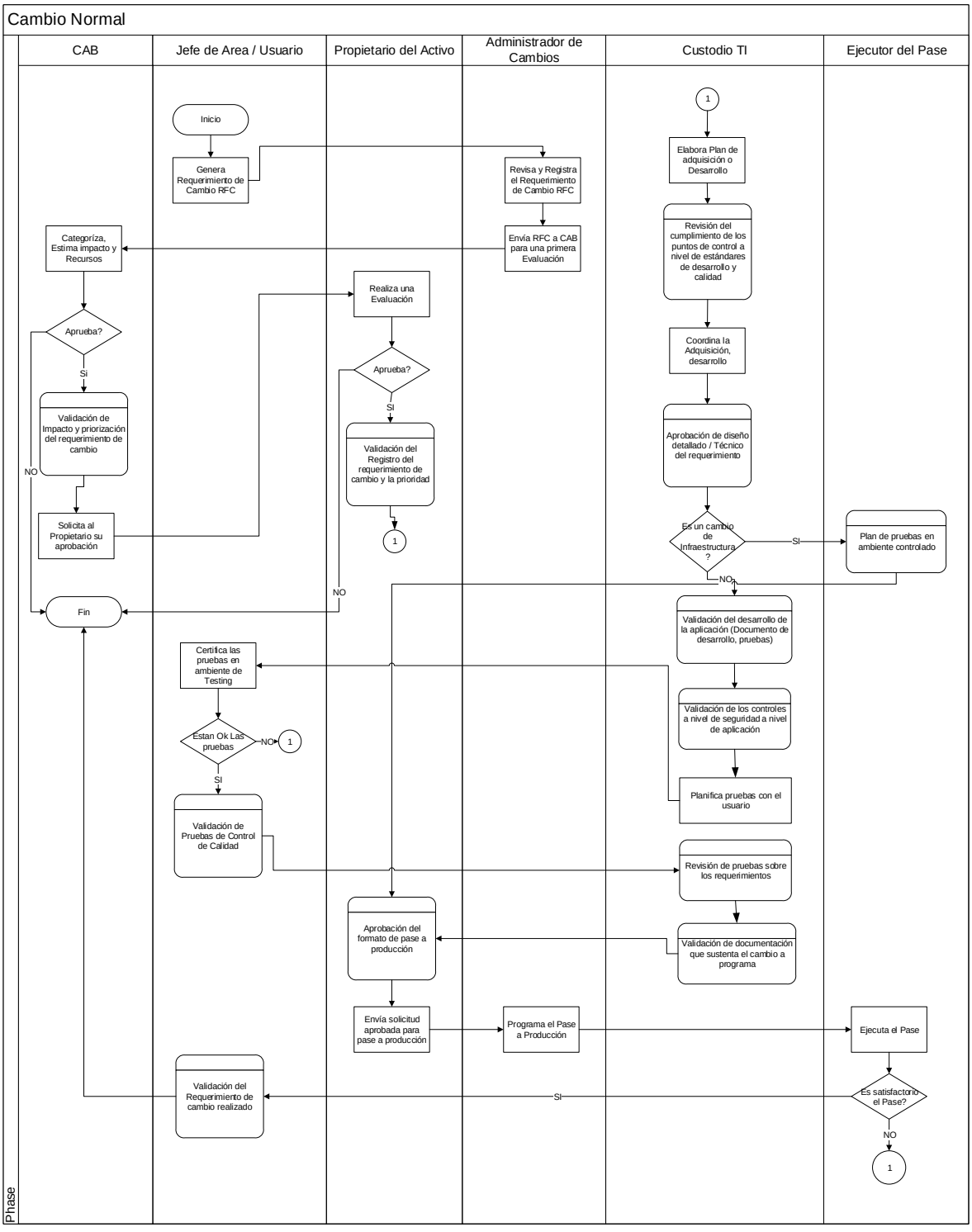


Fig. D1 Cambio Normal
Fuente: Elaboración propia

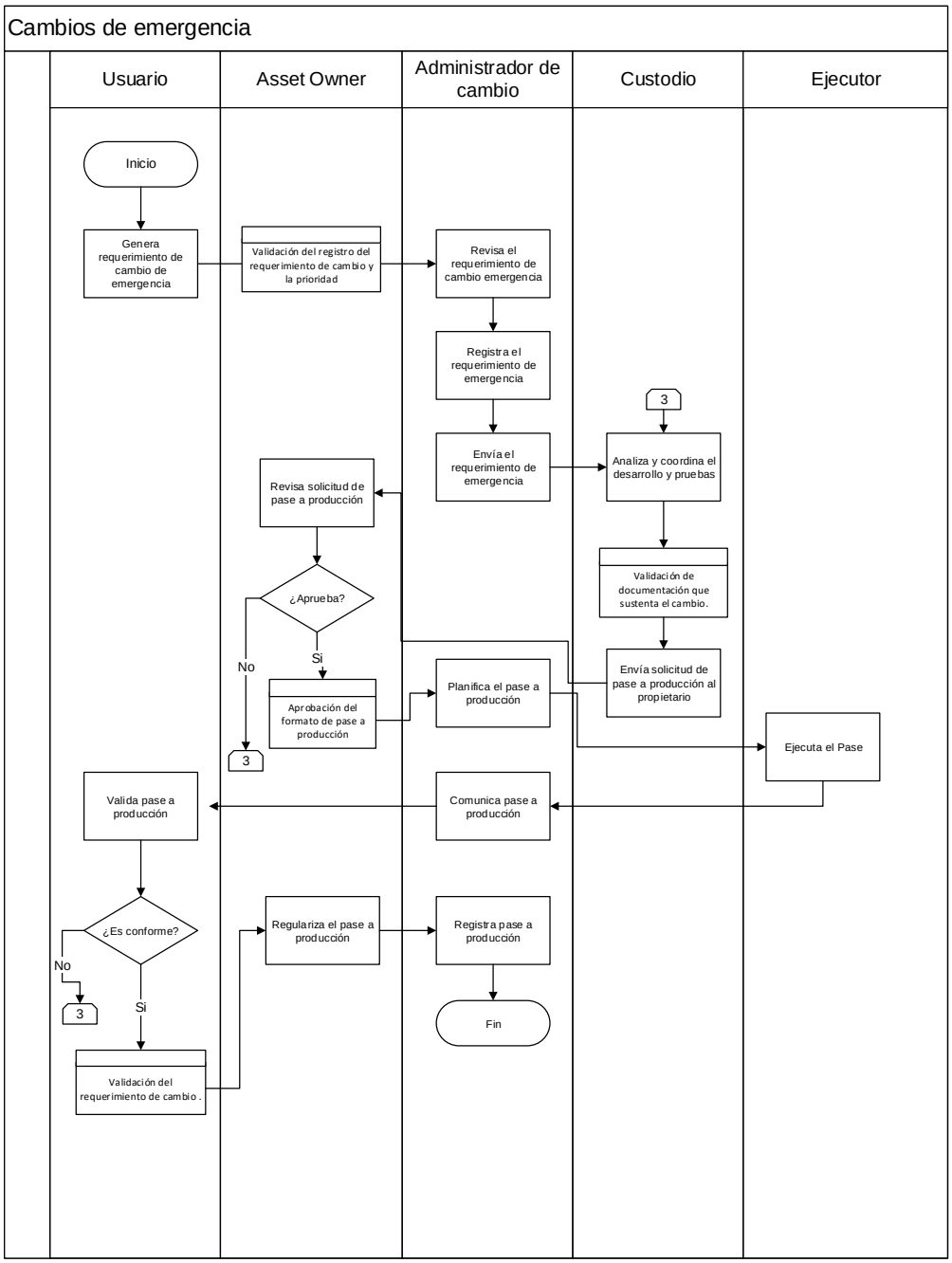


Fig. D2 Cambio de Emergencia
Fuente: Elaboración propia

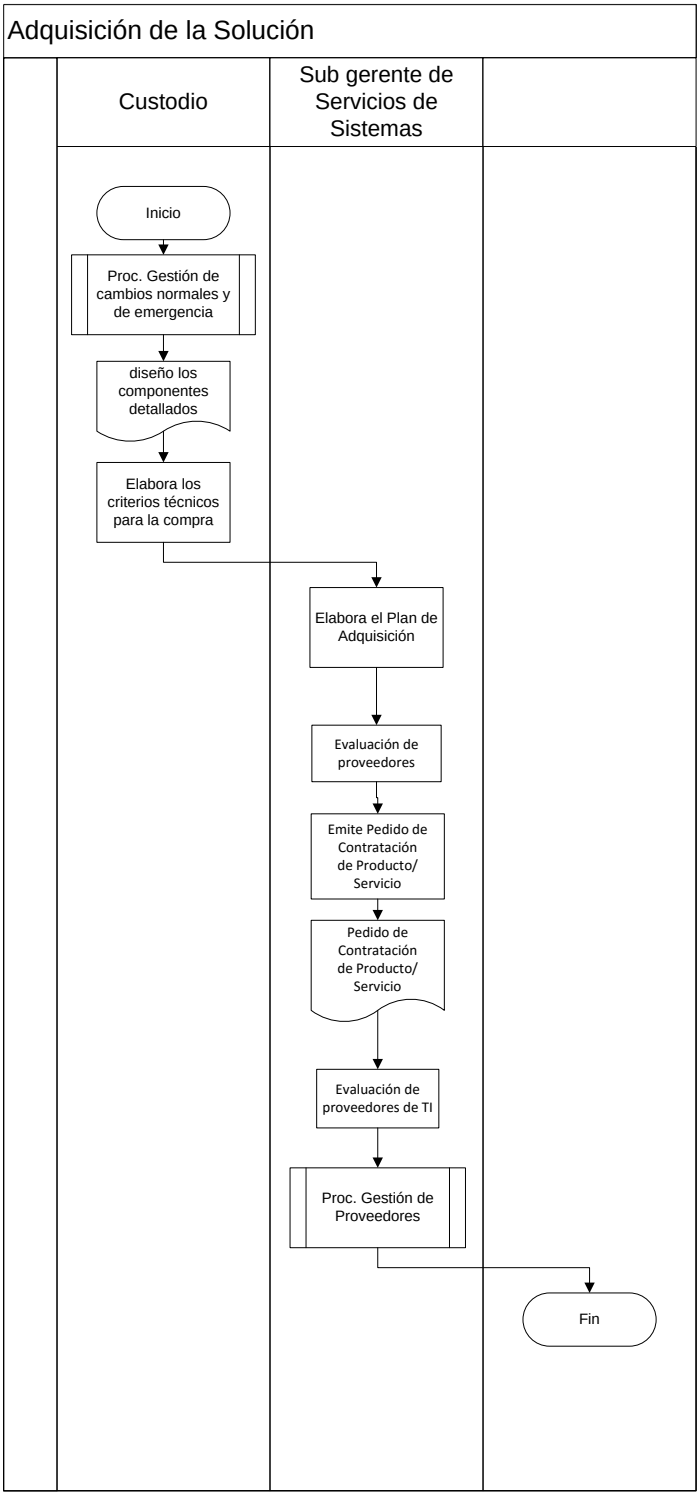


Fig. D3 Adquisición de la Solución
Fuente: Elaboración propia.

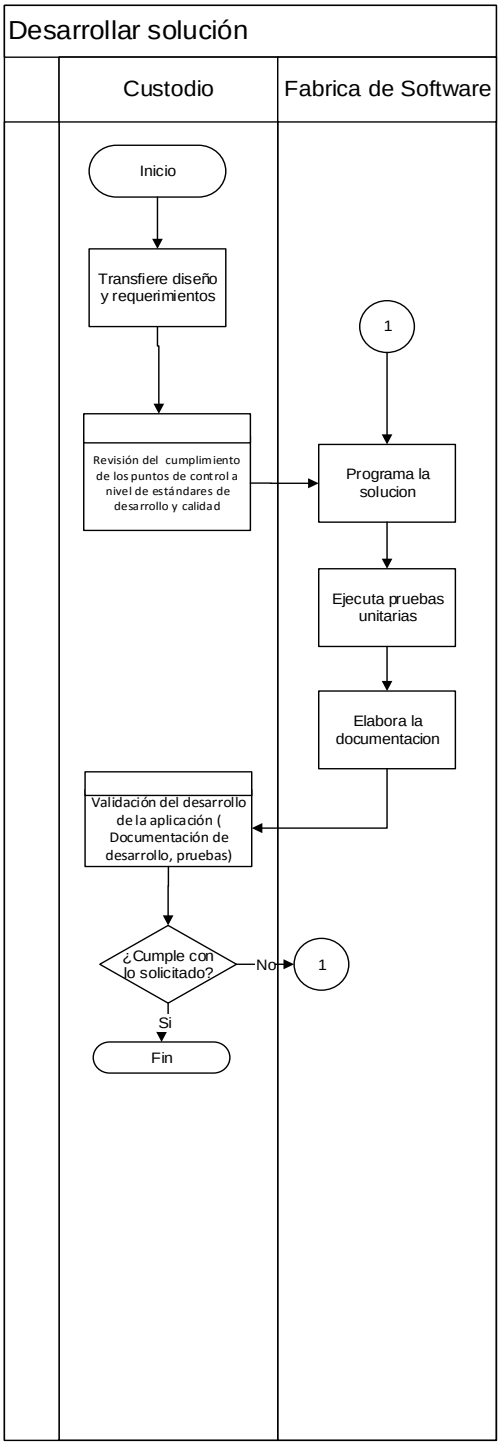


Fig. D4 Desarrollo de la Solución.
Fuente: Elaboración propia.

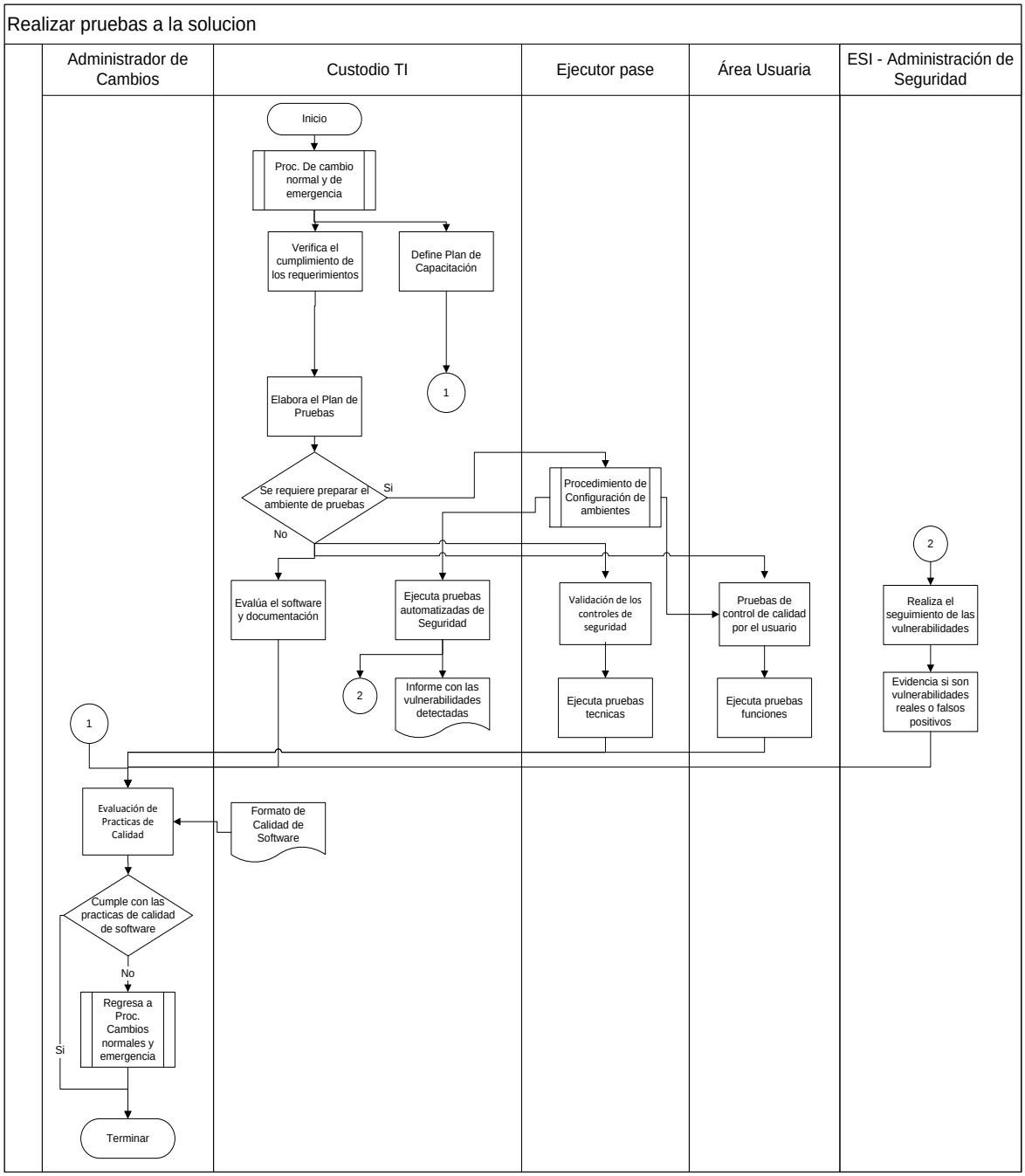


Fig. D5 Pruebas a la Solución.
Fuente: Elaboración propia.

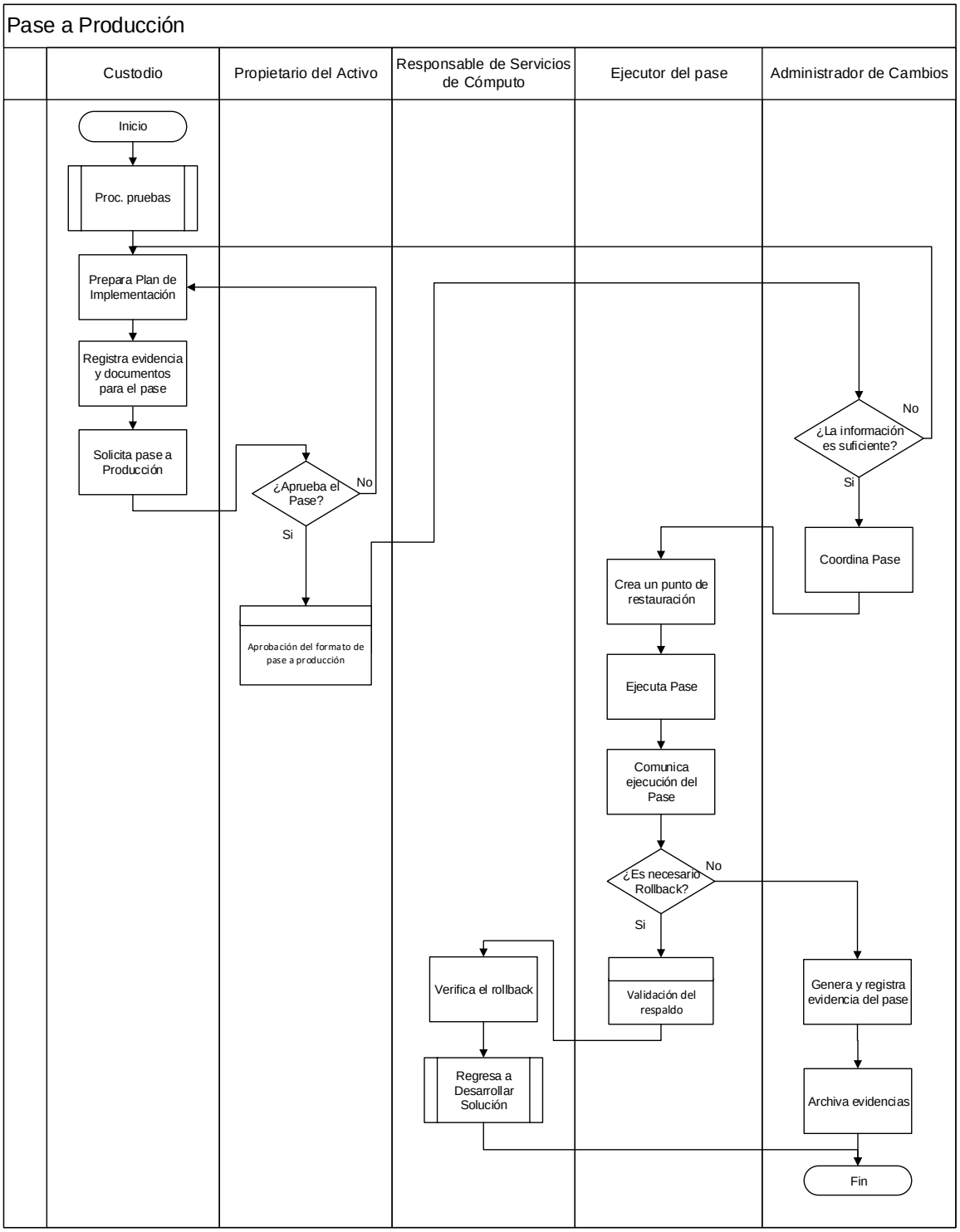


Fig. D6 Pase a Producción.
Fuente: Elaboración propia.

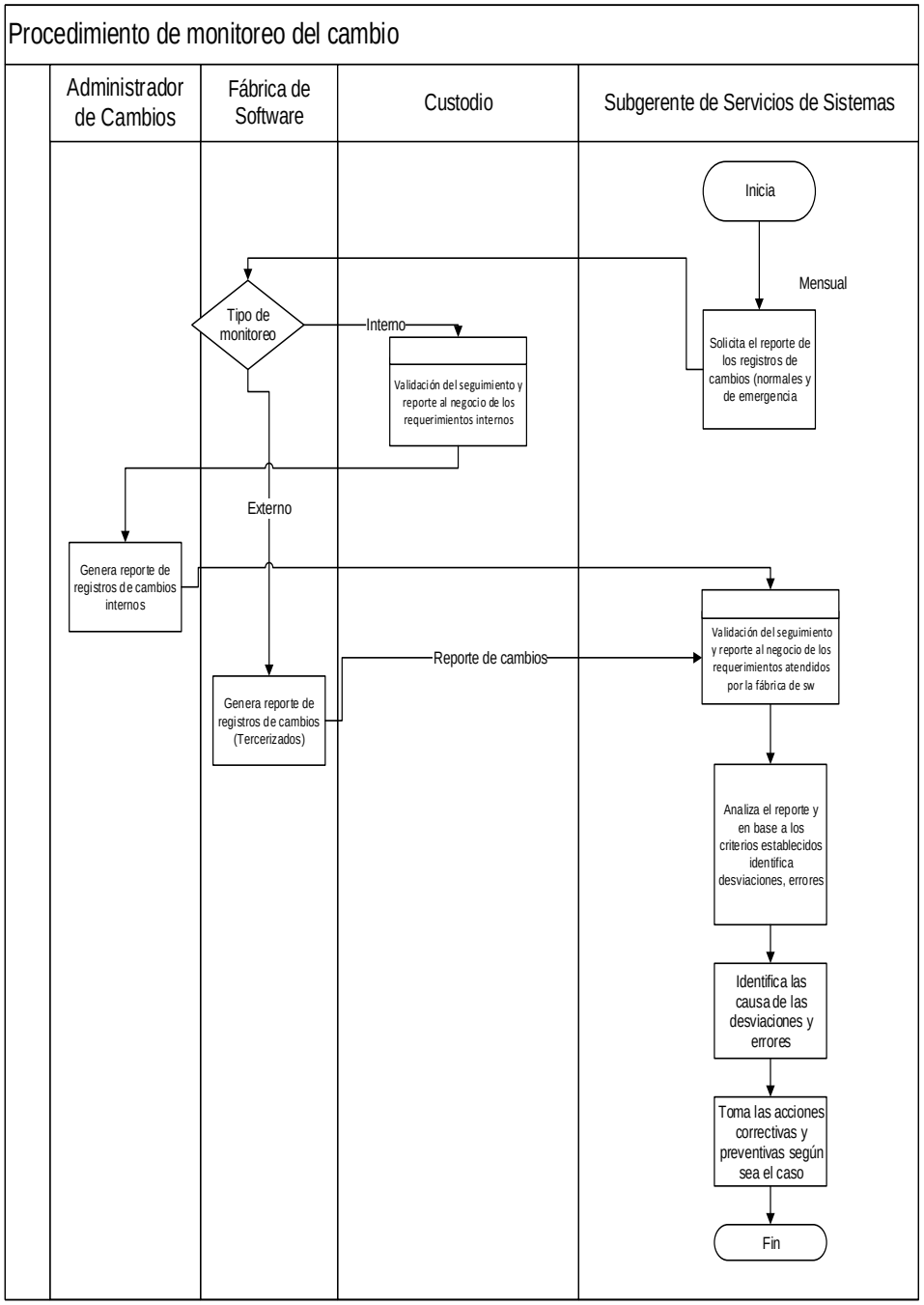


Fig. D7 Monitoreo del Cambio
Fuente: Elaboración propia.

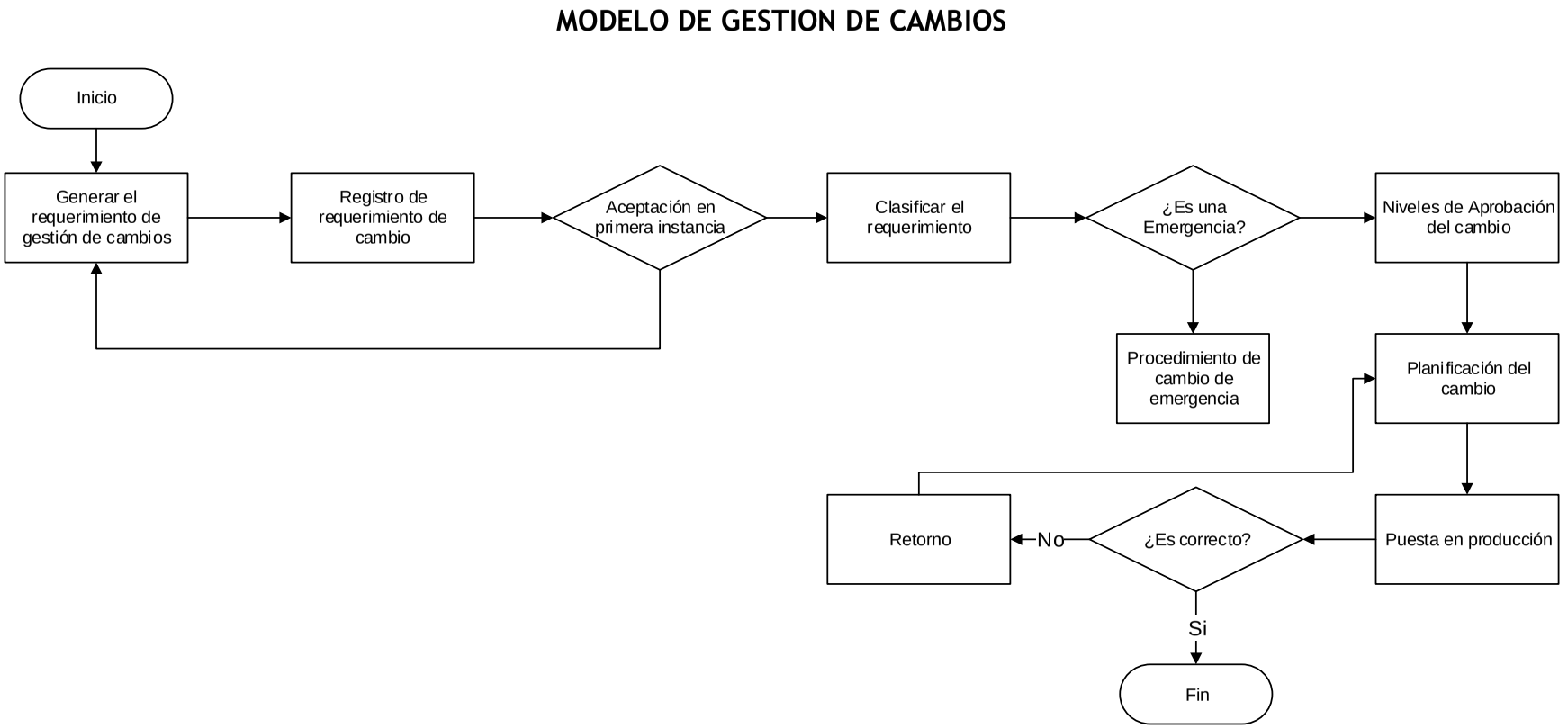


Fig. D8 Modelo de Gestión de Cambio.
Fuente: Elaboración propia.

Anexo E Desarrollo, Adquisición y Mantenimiento de Sistemas

Se identifican criterios para Aseguramiento de Calidad de Artefactos.

Los desarrollos se clasifican de acuerdo a su duración y costo, como se muestra en la siguiente tabla:

Tabla E1 Clasificación de los Desarrollos

Tamaño y Esfuerzo del trabajo	Duración máxima	Costo Estimado
Correctivos Urgentes	1 semana	Bajo
Pequeños y correctivos	1 mes	Bajo
Medianos	4 meses	Medio
Grandes y Proyectos	Más de tiempo	Alto

Fuente: Elaboración propia.

Descripción de los Artefactos

Los Artefactos que se desarrollan como parte del desarrollo, son evaluados para asegurarse que se está cumpliendo con la calidad.

Tabla E2 Descripción de los Artefactos

Categoría	Artefactos	Descripción
Artefactos de Gestión	Lista Maestra de Requerimientos	Registro de los requerimientos, permite trazabilidad de la relación entre el requerimiento y los diferentes trabajos
	Lista de Incidencias	Evidencia que justifica la urgencia y muestra el impacto actual en producción.
	Plan del Proyecto	Documento usado el responsable del proyecto para acompañar el progreso
	Actas de reunión	Registro de acuerdos con las áreas usuarias para llegar a acuerdos
	Documento de Pase a pruebas de aceptación	Registro con las instrucciones para realizar la migración del ambiente de desarrollo al ambiente de pruebas

	Documento de Pase a Producción	Registro con las instrucciones para realizar la migración del ambiente de pruebas al ambiente de producción.
	Acta de cierre de proyecto	Documento formal con que se finaliza el proyecto
	Manuales de Uso	Manuales para el usuario
	Documentación técnica	Casos de uso, conectores, etc
Artefactos de Pruebas	Casos de Prueba	Detalle de los escenarios probados
	Checklist de Seguridad - aplicaciones	Validaciones en el campo de Seguridad de la información
	Checklist de Calidad de Software	Registro que valida cualitativamente la calidad

Fuente: Elaboración propia.

Tipos de Casos de Prueba

El Caso de Prueba incluye uno o más tipos de prueba, dependiendo de lo determinado por los requerimientos.

Tabla E3 Tipos de Caso de Pruebas

Tipos de Prueba	Descripción
Pruebas de Unidad o Unitarias	Es la prueba de un programa o modulo individual, que aseguran que la operación interna del programa funciona en conformidad con las especificaciones.
Prueba de Interfaz o de integración	Una prueba de hardware o de software que evalúa la conexión de dos o más componentes que pasan información desde un área a otra.
Pruebas de sistemas	
Pruebas de Recuperación	Verificar la capacidad del sistema de recuperarse después de una falla de software o de hardware.
Pruebas de Seguridad	Asegurarse de que el sistema modificado/nuevo, incluya controles de acceso apropiados y no contenga ningún agujero de seguridad que pudiera comprometer otros sistemas.
Prueba de Carga	Probar una aplicación con grandes cantidades de datos para evaluar su rendimiento durante las horas pico.
Prueba de Volumen	Estudiar el impacto en la aplicación, probando con un volumen incremental de registros para determinar el volumen máximo de registros (datos) que la aplicación puede procesar.
Prueba de Estrés	Estudiar el impacto en la aplicación, probando con un número incremental de usuarios/servicios concurrentes en la aplicación para determinar el número máximo de usuarios/servicios concurrentes que la aplicación puede procesar.

Tipos de Prueba	Descripción
Prueba de desempeño	Comparar el rendimiento del sistema con otros sistemas equivalentes, usando estudios comparativos (benchmarks) bien definidos.
Pruebas de aceptación del usuario	Pruebas funcionales por parte del usuario para validar que se encuentren todos los requerimientos

Fuente: Elaboración propia.

Cumplimiento de los Artefactos

Los Artefactos que se revisarán dependen del tamaño y esfuerzo del desarrollo:

Tabla E4 Cumplimiento de los Artefactos.

Artefactos	Correctivas Urgentes	Pequeños y correctivos	Medianos	Grandes y Proyectos
Lista Maestra de Requerimientos		X	X	X
Lista de Incidencias (Error)	X			
Plan del Proyecto				X
Actas de reunión			X	X
Documento de Pase a pruebas de aceptación		X	X	X
Documento de Pase a Producción	X	X	X	X
Acta de cierre de proyecto				X
Manuales de Uso			X	X
Documentación técnica		X	X	X
Casos de Prueba	X	X	X	X
Checklist de Seguridad – aplicaciones				X
Checklist de Calidad de Software				X

Fuente: Elaboración propia.

Realización y Verificación de los Artefactos

Los Artefactos serán realizados y verificación de la siguiente forma:

Tabla E5 Verificación de los Artefactos

Artefactos	Elaborado	Verificación	Responsable de verificar
Lista Maestra de Requerimientos	Al recibir un requerimiento	Revisión mensual	El responsable de aseguramiento de calidad
Plan del Proyecto	Al formalizarse el proyecto	Revisión mensual	El responsable de aseguramiento de calidad

Artefactos	Elaborado	Verificación	Responsable de verificar
Actas de reunión	Semanalmente	Revisión mensual	El responsable de aseguramiento de calidad
Documento de Pase a pruebas de aceptación	Antes del Pase a Pruebas de aceptación	Pase a Pruebas de aceptación	El consultor de sistemas
Documento de Pase a Producción	Antes del Pase a Producción	Pase a Producción	Administrador de cambio
Acta de cierre de proyecto	Después de la revisiones post implementación	Cierre de proyecto	Sponsor del proyecto
Manuales de Uso	Antes del Pase a Producción	Pase a Producción	Administrador de cambio
Documentación técnica	Antes del Pase a Producción	Pase a Producción	Administrador de cambio
Casos de Prueba	Antes del Pase a Pruebas de aceptación	Pase a Producción	Administrador de cambio
Checklist de Seguridad - aplicaciones	Antes del Pase a Producción	Pase a Producción	Administrador de cambio
Checklist de Calidad de Software	Antes del Pase a Producción	Pase a Producción	Administrador de cambio

Fuente: Elaboración propia.

Revisión de la Calidad

Se considerara que un Desarrollo ha sido llevado con calidad si cumple los siguientes criterios:

- Se han elaborado los documentos que corresponden de acuerdo a los requerimientos.
- La persona responsable de verificar confirma la existencia y se encuentran correctamente llenados.

Técnicas y Herramientas para la Prueba de Calidad

Se consideran las siguientes técnicas para probar la calidad:

- A nivel de desarrollo se realiza revisiones de pares.
- A nivel de desarrollo según se considere necesario se realizan pruebas automatizadas de los casos de prueba.

Informe e Indicadores de los Resultados de las Revisiones

Los responsables de la ejecución de las pruebas de calidad y de la fábrica del software miden los resultados de las pruebas de calidad de sus respectivos desarrollos, utilizando la siguiente tabla:

Indicadores de Resultados de las Revisiones

Tabla E6. Indicadores de las Revisiones.

Lineamiento estratégico	Clase	Indicador	Umbral Verde	Umbral Amarillo	Umbral Rojo
Cumplimiento	Mantenimiento evolutivo y extracción de datos	Cumplimiento duración estimada	>=85.01	>= 75% y < 85.01%	< 75%
		Confiabilidad - % Errores Testing	< 10%	>= 10% y < 20%	>= 20%
	Mantenimiento Correctivo	Prontitud – OT's Criticas	< 1 día >= 90.01%	>= 1 y <2 días >= 80% y < 90.01%	<= 2 días < 80%
		Prontitud – OT's No Criticas	< 5 días >=85.01%	>= 5 y < 7 días >= 75% y < 85.01%	<= 7 días < 75%
Rentabilidad	Mantenimiento evolutivo y extracción de datos	Devolución con LI	< 15%	>= 15% y < 25%	>= 25%
Rentabilidad	Mantenimiento Correctivo	Devolución con PSC	< 15%	>= 15% y < 25%	>= 25%

Fuente: Elaboración propia.

Devolución con LI: se mide aquellas OT's que fueron devueltas dentro del periodo y cuyas incidencias han sido tipificadas como Error.

Devolución con PSC: se consideran las OT's que tuvieron Solicitudes de Cambio (especificaciones nuevas) dentro del periodo de medición.

Anexo F Gestión de Incidentes de Seguridad

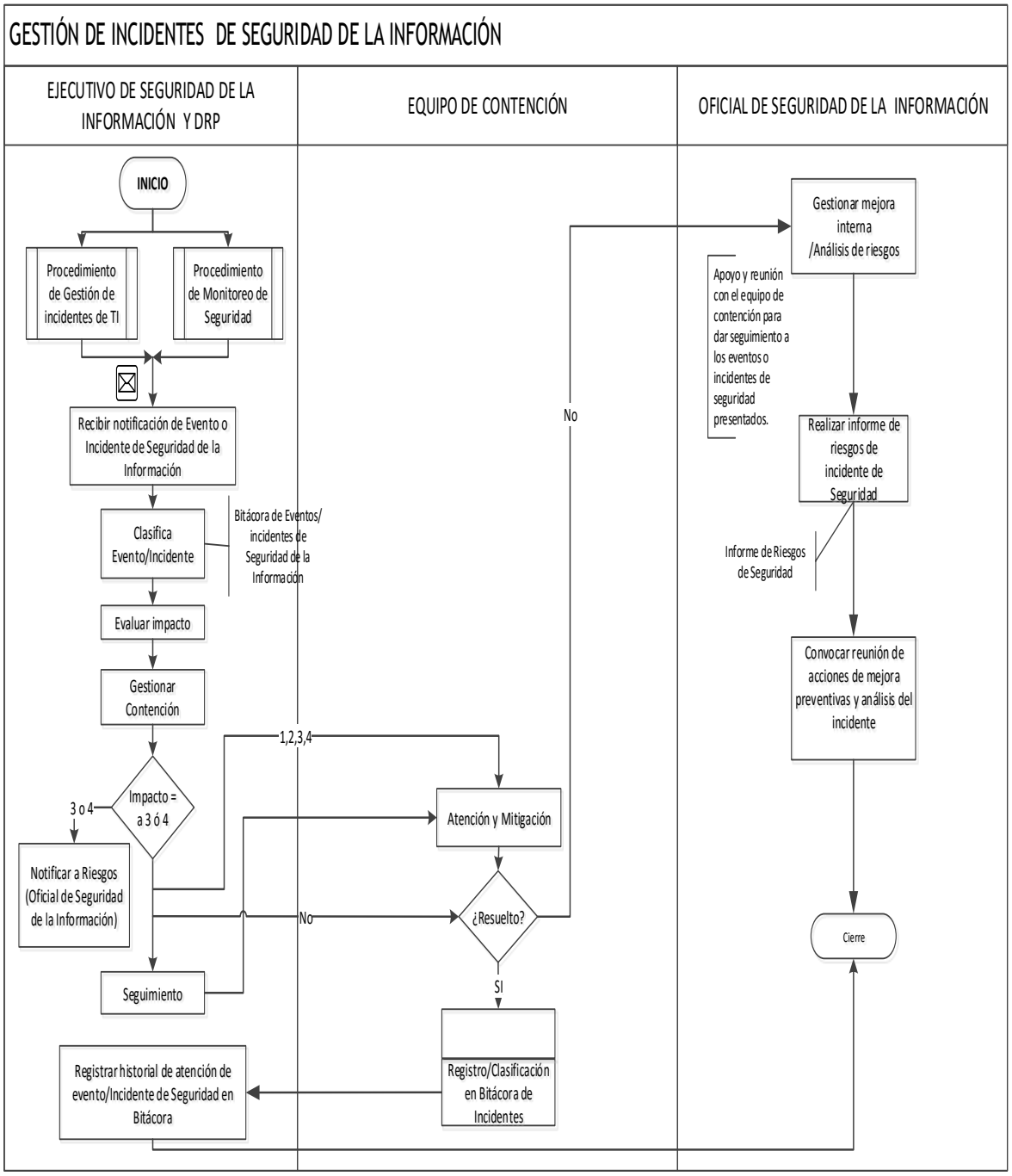


Fig. F1 Gestión de Incidentes de Seguridad de la Información
Fuente: Elaboración propia.

Tabla F1 Bitácora de Incidentes de Seguridad de la Información.

Fecha/Hora					Reportante				Descripción			Tipificación		Naturaleza/Origen	
Código de Reporte Generado	Día de Reporte	Hora de incidencia/evento	Hora de cierre de incidencia/Evento	Duración	Persona reportante	Empresa	Área reportante	Gerencia	Evento/ Incidente	Descripción	Detalle adicional de actividades desarrolladas para atender o dar seguimiento al evento o incidencia de SI	Categoría	Sub-Categoría	Naturaleza	Origen

Impacto				Empresa/Ubicación		Estatus	Seguimiento [SI/NO]	Causa Raíz	Solución	Observaciones	
Nivel de Impacto: Catastrófico: 5 Mayor: 4 Moderado: 3 Menor:2 Inferior:1	Gerencia Central Afectada	Área afectada	Proceso Afectado	Empresa	Ubicación (Lima/Provincia)	Estado de desarrollo de Informe [NO INICIADO / PROCESO / CERRADO / NO APLICA]	Informe derivado a RIESGOS EN CASO DE SER TIPO 4 o 5	Causa Raíz	Solución	Observaciones	Estado [ABIERTO/ CERRADO]

Fuente: Elaboración propia.

PROCESO DE MONITOREO DE SEGURIDAD E INFRAESTRUCTURA

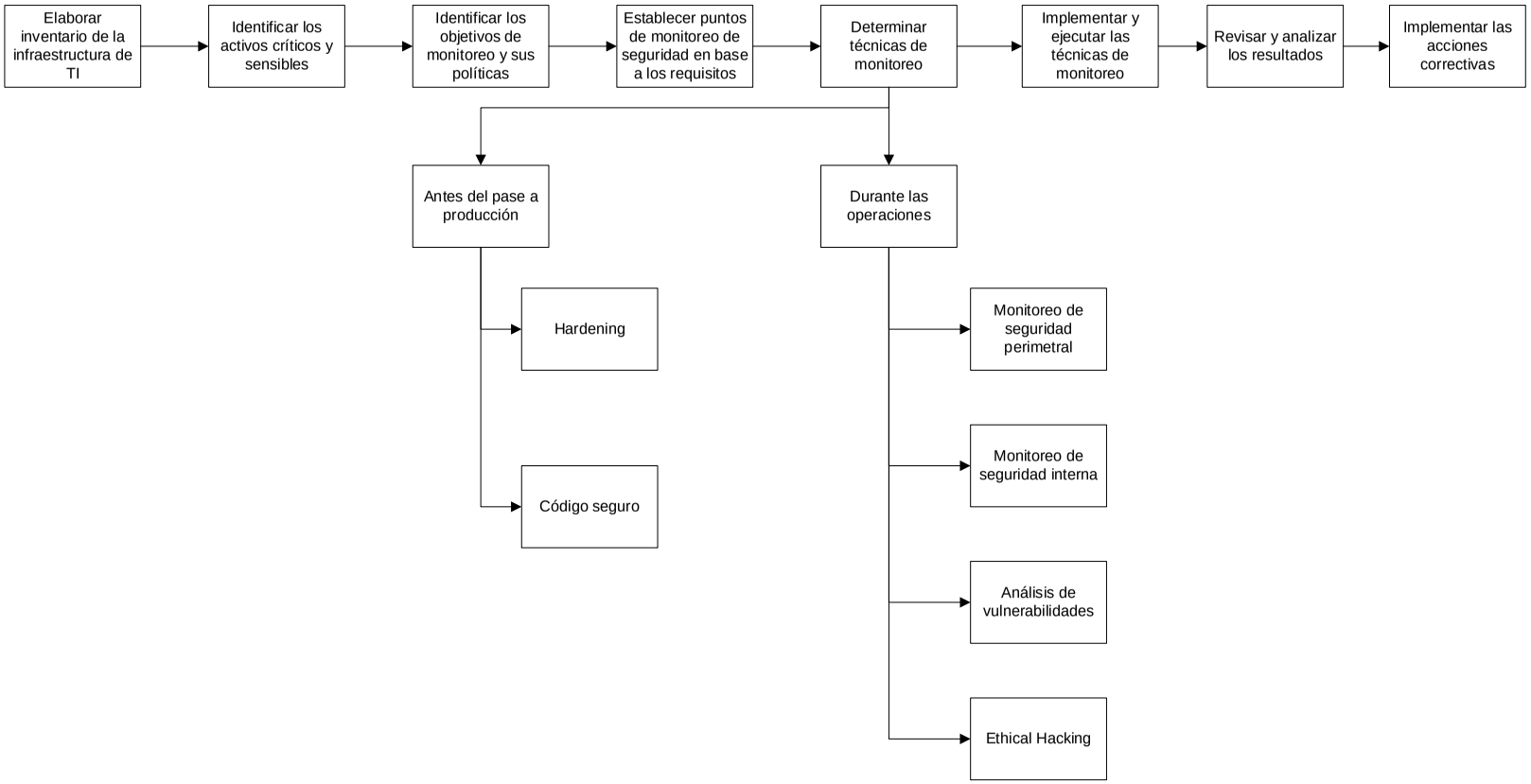


Fig. F2 Proceso de Monitoreo de Seguridad e Infraestructura.

Fuente: Elaboración propia.

Anexo G Gestión de Incidentes de TI

Descripción del Proceso de la Gestión de Incidentes

La gestión de incidentes garantiza que se restablezca la operación normal de servicio lo antes posible y se minimice el impacto al negocio.

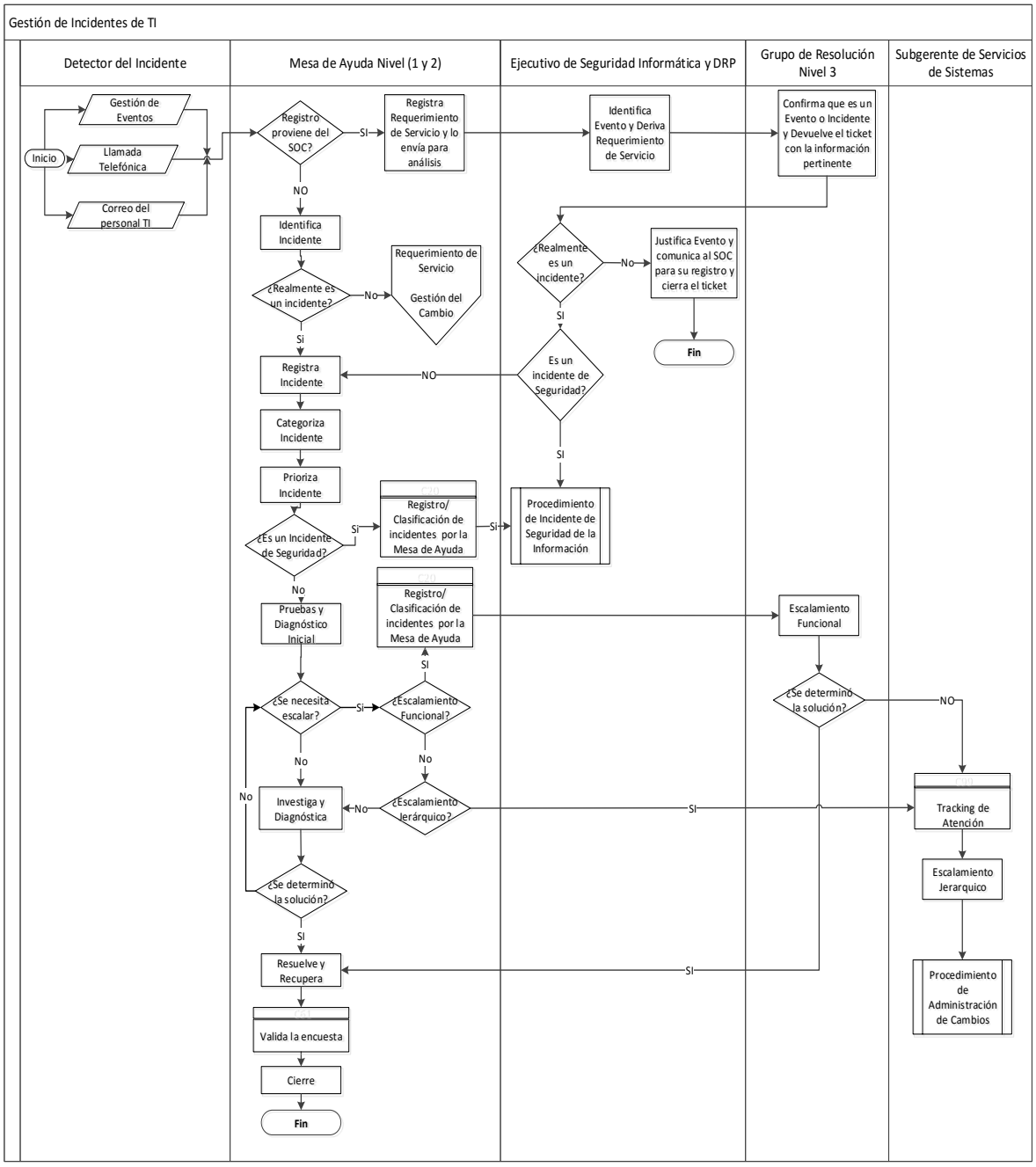


Fig. G1 Gestión de Incidentes de TI.
Fuente: Elaboración propia.

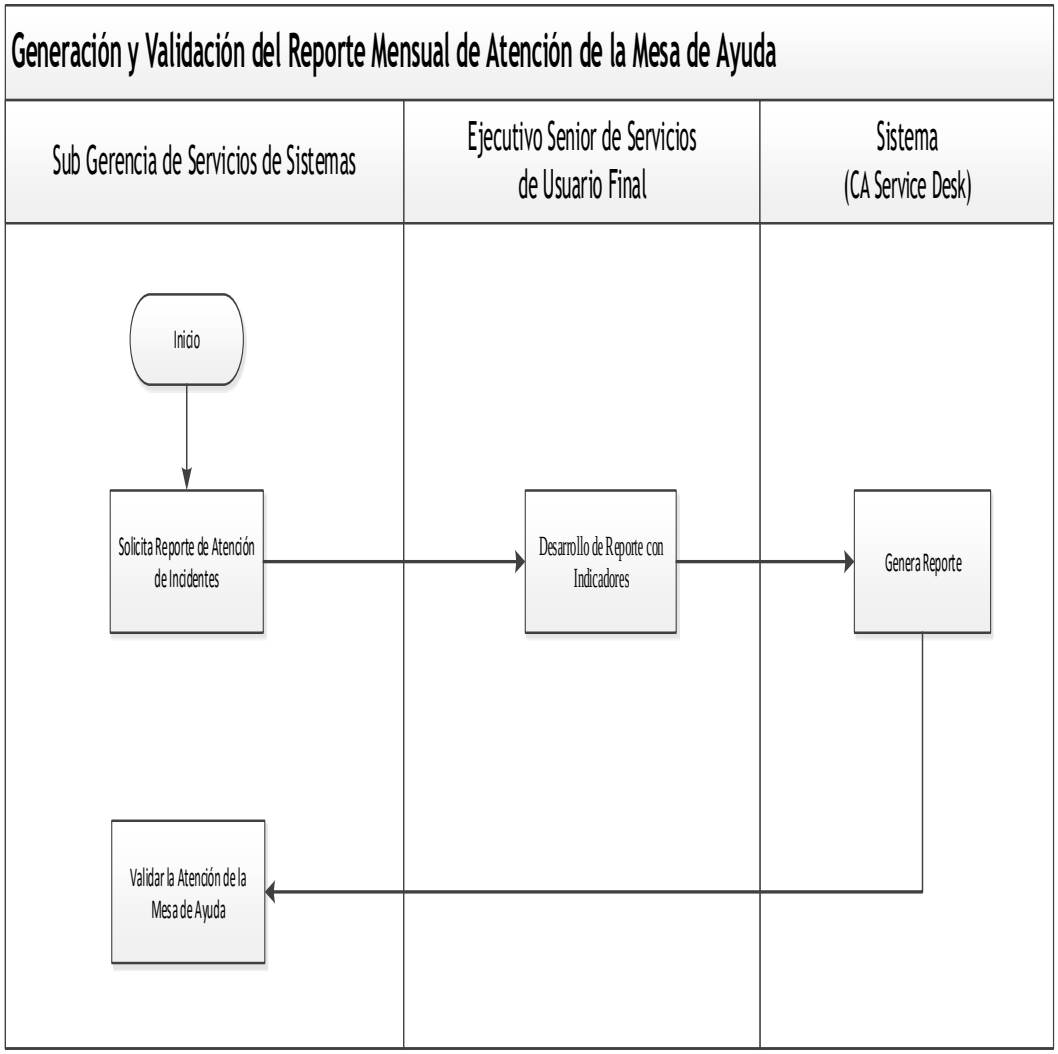


Fig. G2 Validación del Reporte de Mesa de Ayuda
Fuente: Elaboración propia.

Anexo H Gestión de Problemas

La gestión de problemas se orienta hacia la prevención de los problemas y como consecuencia de los incidentes que pudieran ocurrir. Aborda la eliminación de los incidentes recurrentes. Intenta reducir al mínimo el impacto de los incidentes que no se pueda prevenir.

Tabla H1 Urgencia vs. Impacto

		IMPACTO		
		Alto	**Medio**	**Bajo**
URGENCIA	Alta	1	2	3
	Media	2	3	4
	Baja	3	4	5

Fuente: ITIL Gestión de Servicios de TI.

Tabla H2 Tiempo de Respuesta según la Prioridad

Id Prioridad	Descripción	Tiempo de Resolución
1	Crítica	1 hora
2	Alta	8 horas

Fuente: Elaboración propia.

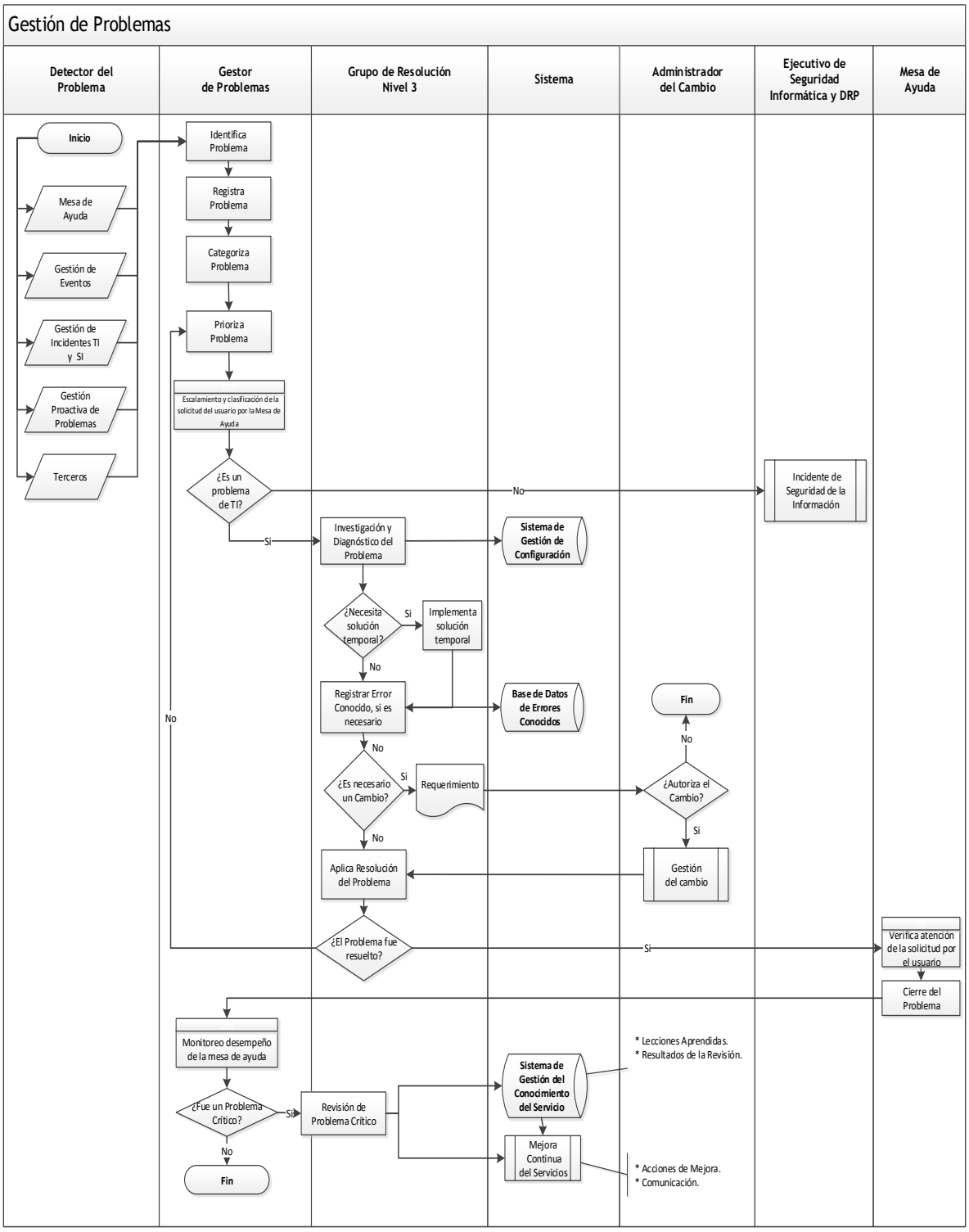


Fig. H1 Gestión de Problemas.
Fuente: Elaboración propia.

Anexo I Gestión de Talento Humano

Procedimiento de Elaboración del Plan de Capacitación de TI.

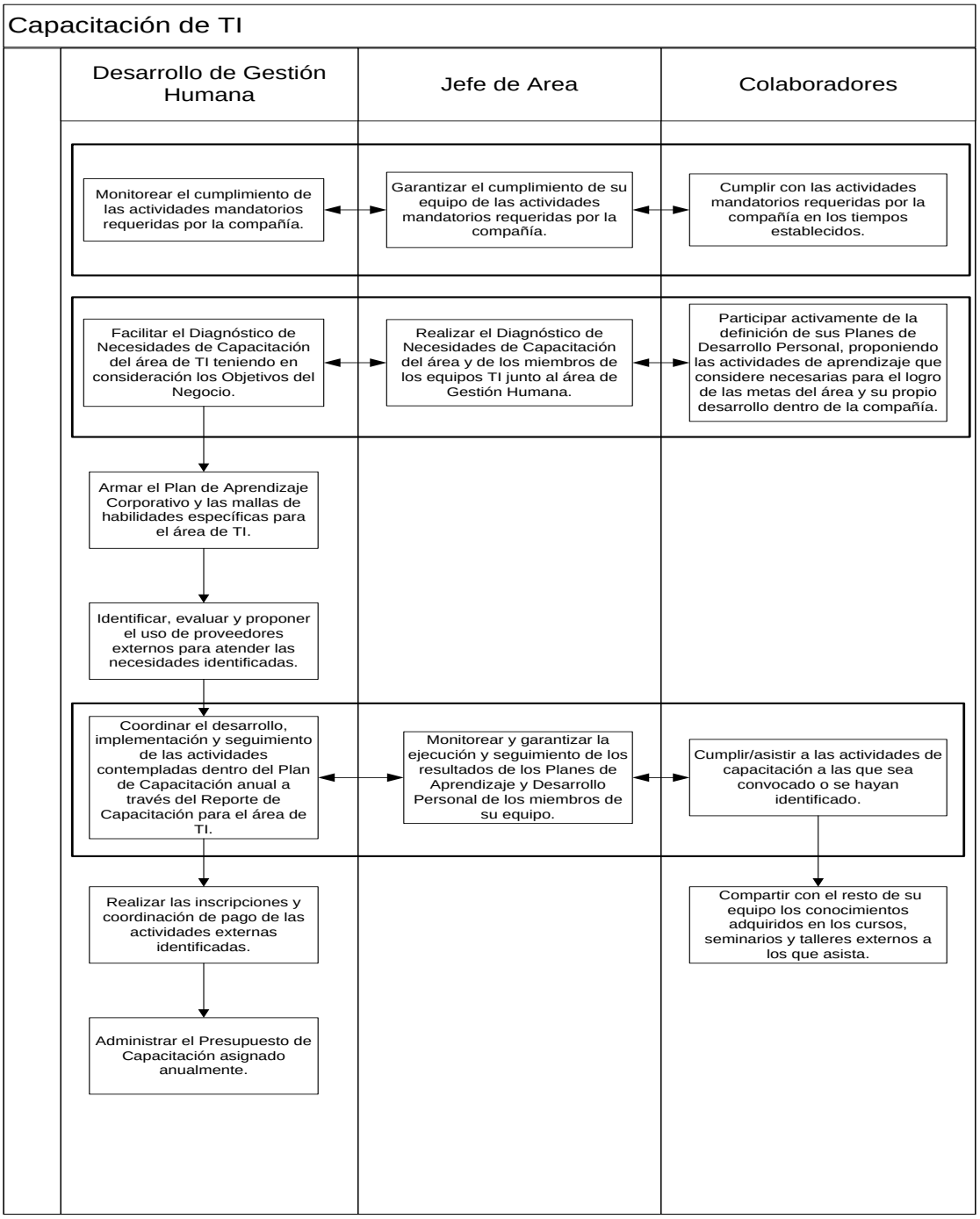


Fig. I2 Capacitación de TI.
Fuente: Elaboración propia.

Procedimiento de Elaboración del Plan de Concientización de Riesgos Operativos y Tecnología de Información.

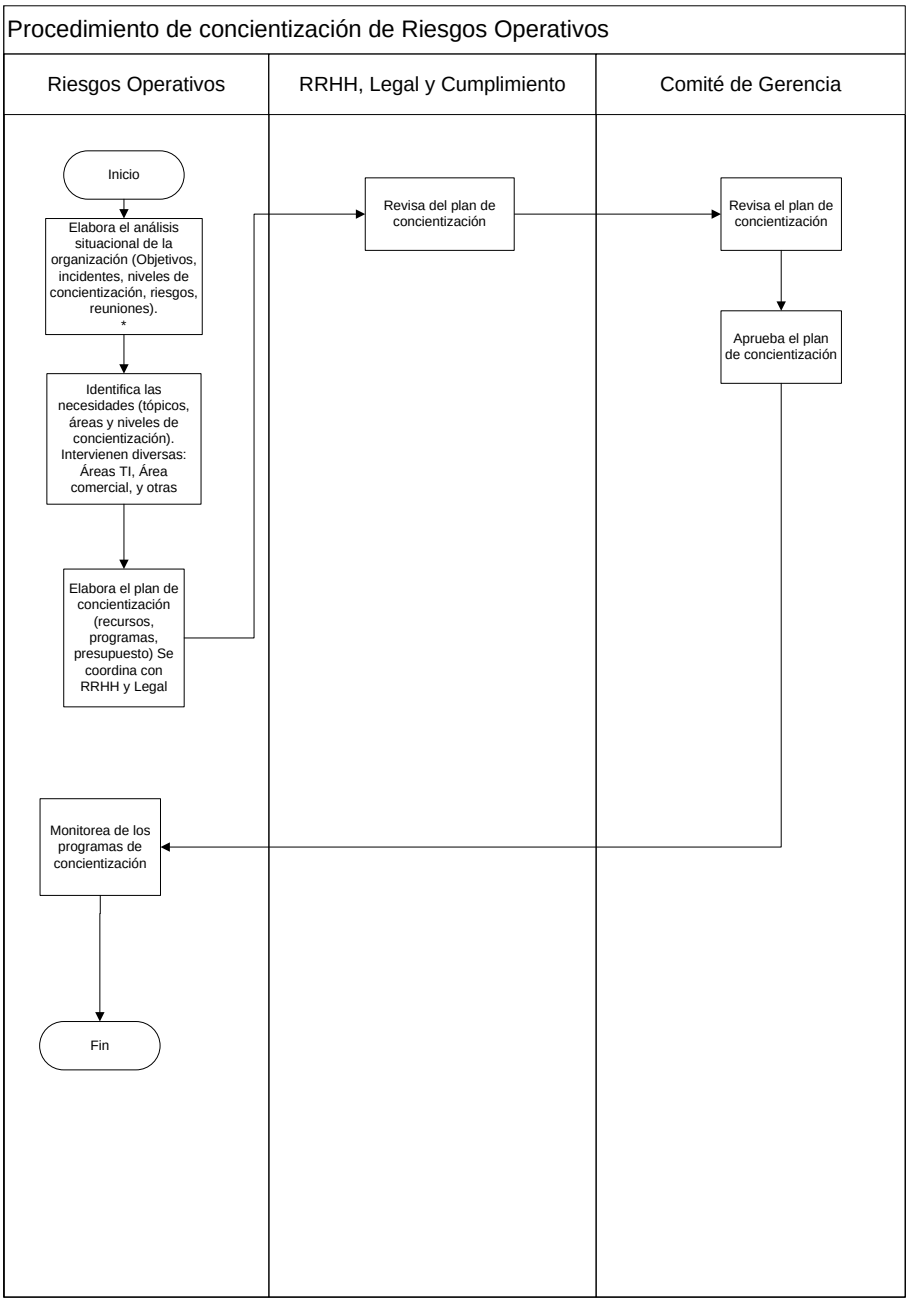


Fig. I3 Concientización de Riesgos Operativos.
Fuente: Elaboración propia.

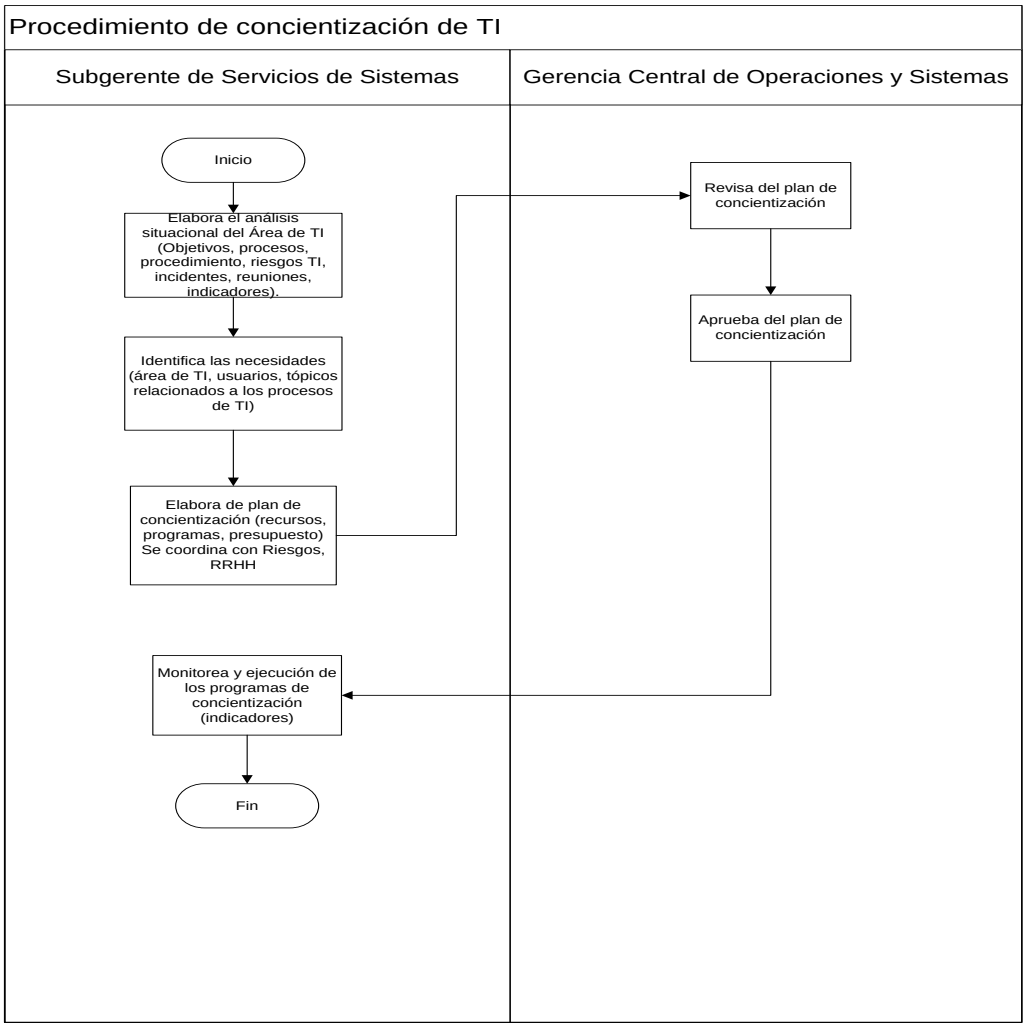


Fig. I4 Concientización de TI.
Fuente: Elaboración propia.

Matriz de técnicas de Concientización:

Tabla I1 Seguridad de la Información

Grupos	Curso de Inducción		Técnicas de publicación			Videos		
	Presencial	Virtual	Afiche	Protector de Pantalla	Boletines	Intranet	Lugares Públicos	Cursos
Área 1								
Área 2								
Área 3								

Fuente: Elaboración propia.

Tabla I2 Tecnología de Información

Grupos	Curso de Inducción		Técnicas de publicación			Videos		
	Presencial	Virtual	Afiche	Protector de Pantalla	Boletines	Intranet	Lugares Públicos	Cursos
Usuarios de TI								
Administradores de TI								
Desarrolladores de TI								

Fuente: Elaboración propia.

Se debe llenar de los tópicos y temas a tratar, estos deben ser seleccionados en base a los resultados de la evaluación de la concientización.

Procedimiento de Cambio de puesto y Funciones

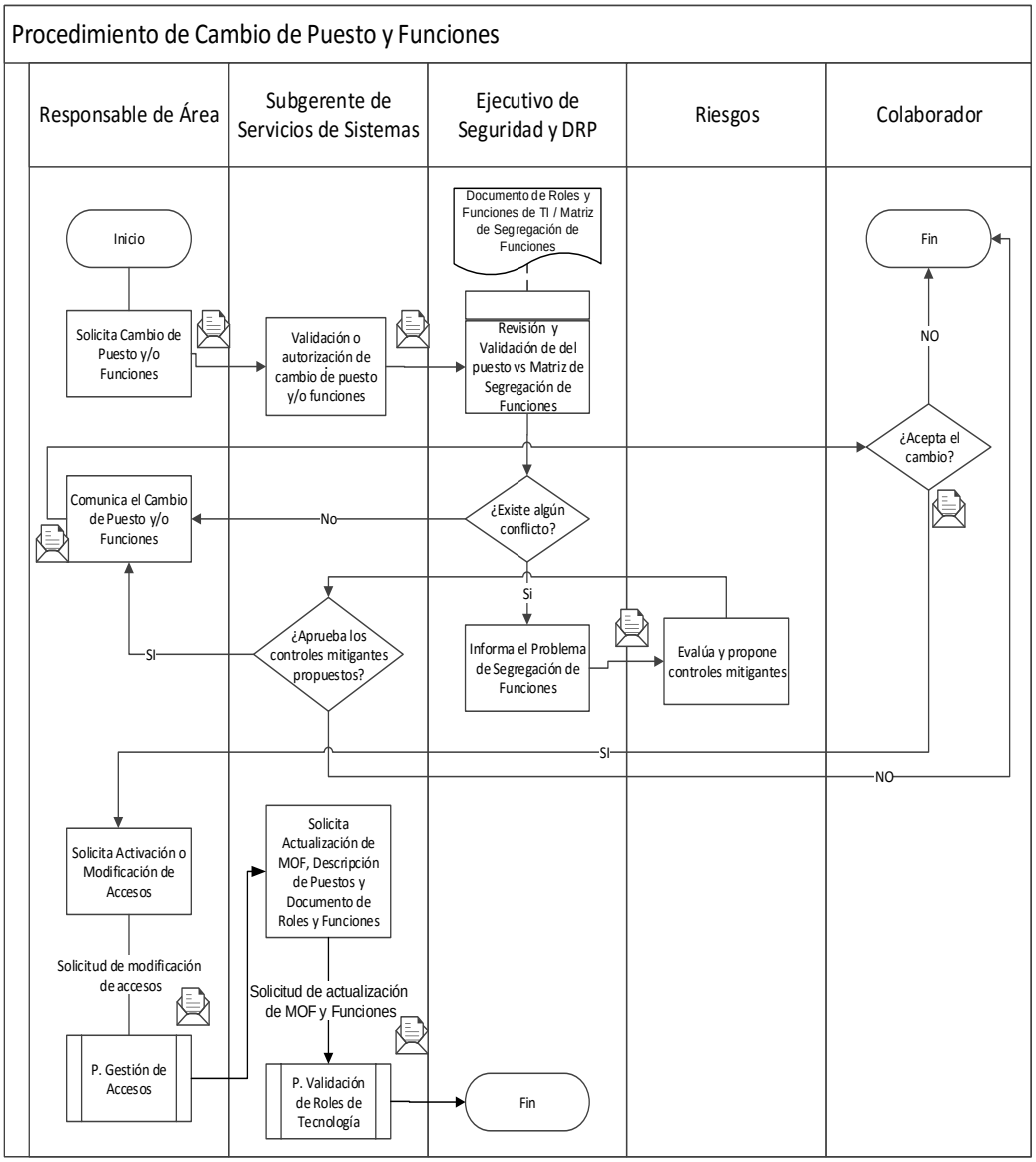
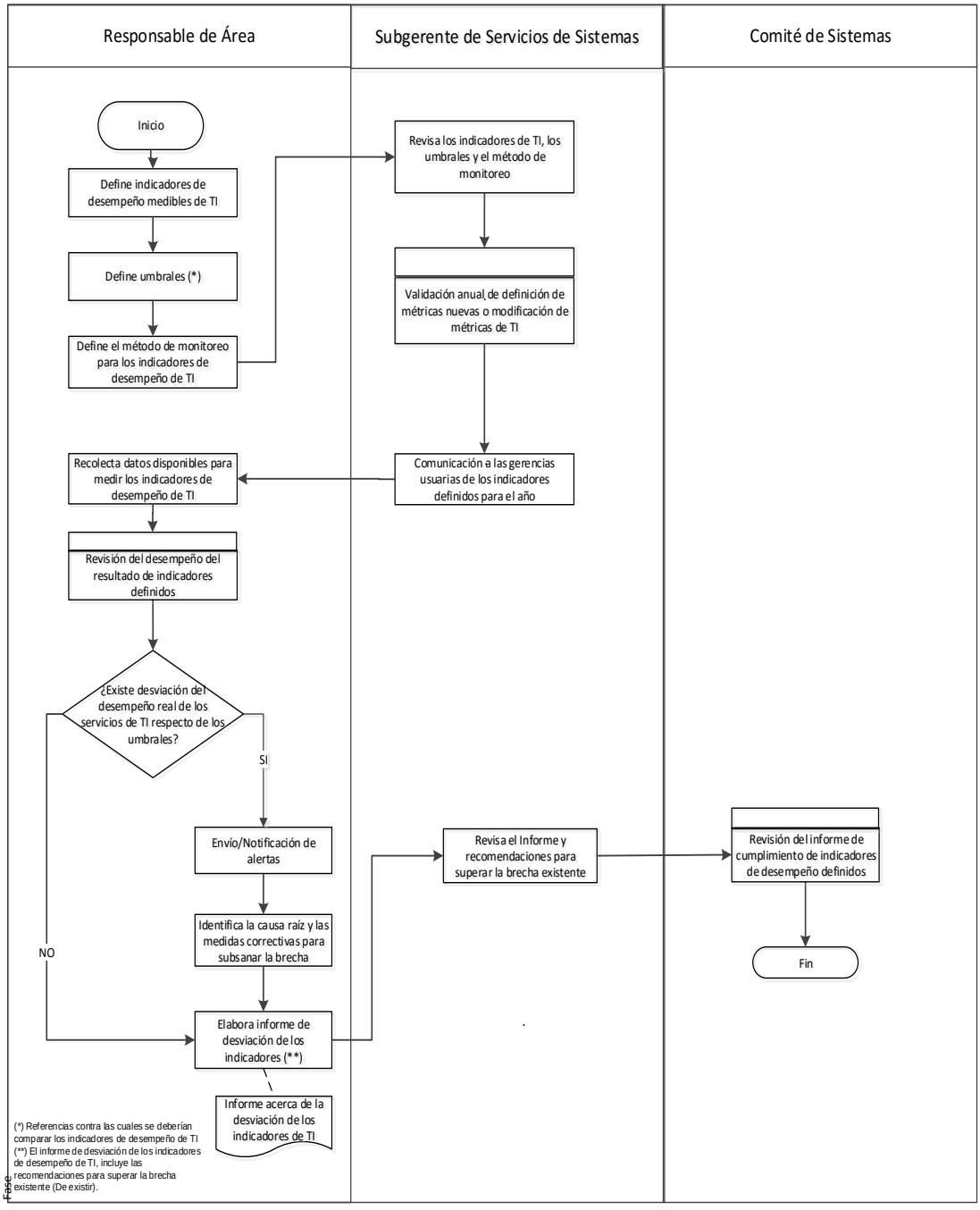


Fig. I5 Cambio de Puesto y Funciones.
Fuente: Elaboración propia.

.

Anexo J Gestión de Desempeño y de la Calidad.

Fig. J1 Monitoreo de Desempeño de los Servicios de TI.
Fuente: Elaboración propia.



Anexo K Marco de Trabajo de los Procesos de Tecnología

Gestión y Organización de Procesos de TI

Adicionalmente se puede consultar la tabla 4.18 Matriz de Segregación de Funciones

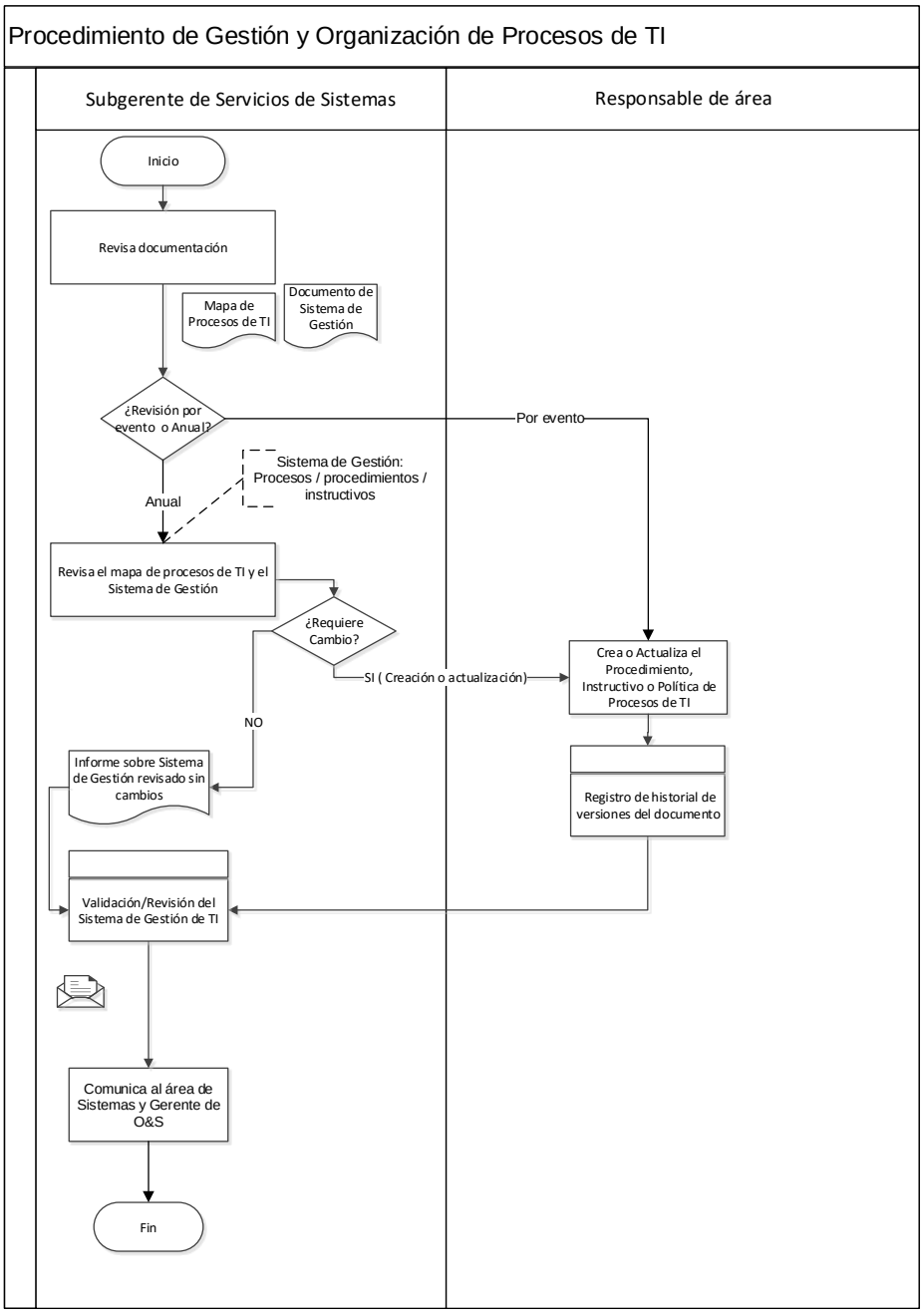
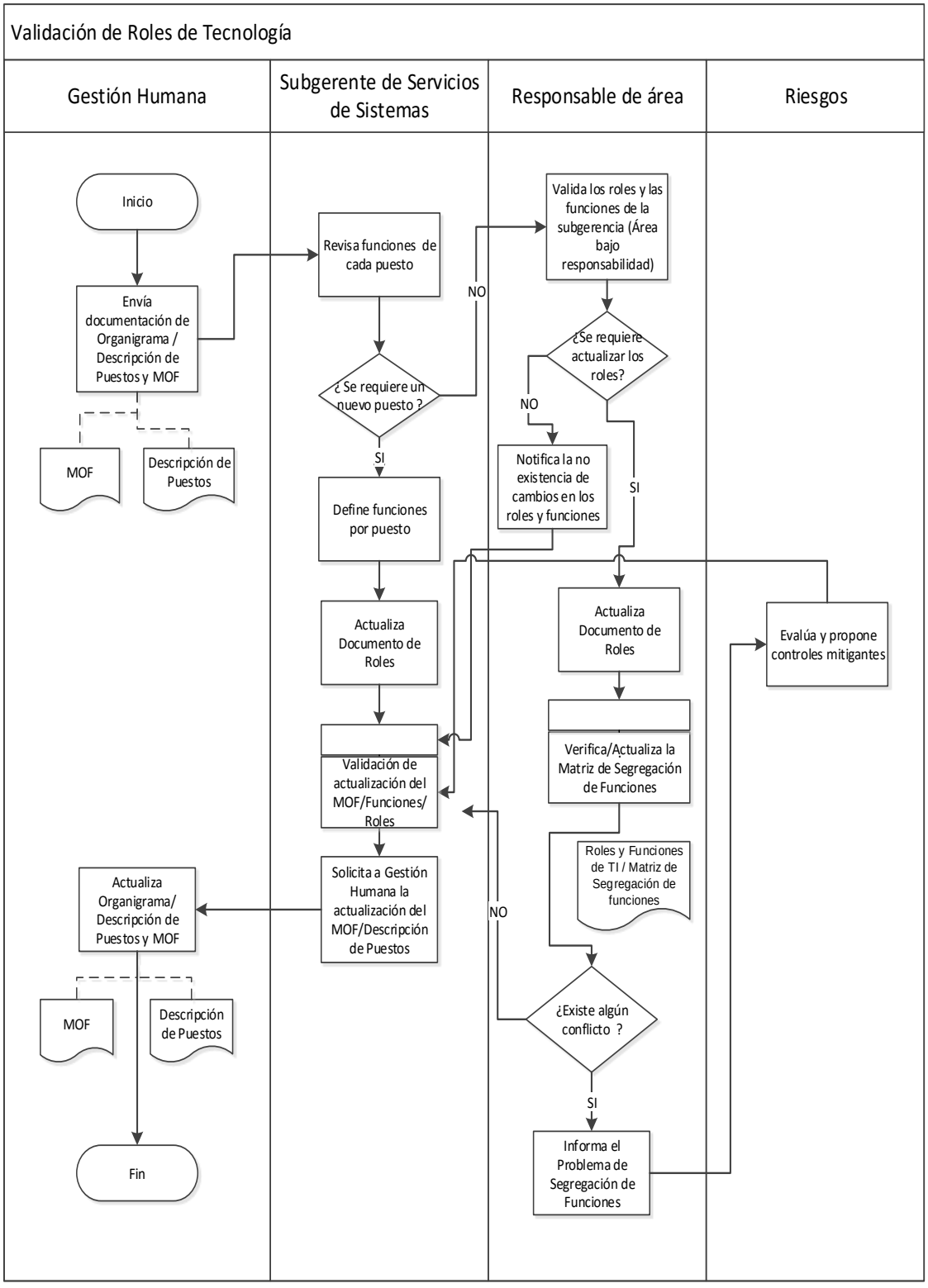


Fig. K1 Gestión y Organización de Procesos de TI.
Fuente: Elaboración propia.



F

Fig.K2 Validación de Roles de Tecnología.
Fuente: Elaboración propia.

MOF: Matriz de Organización y Funciones

Anexo L Monitoreo

Descripción del Proceso de Monitoreo de Seguridad e Infraestructura.

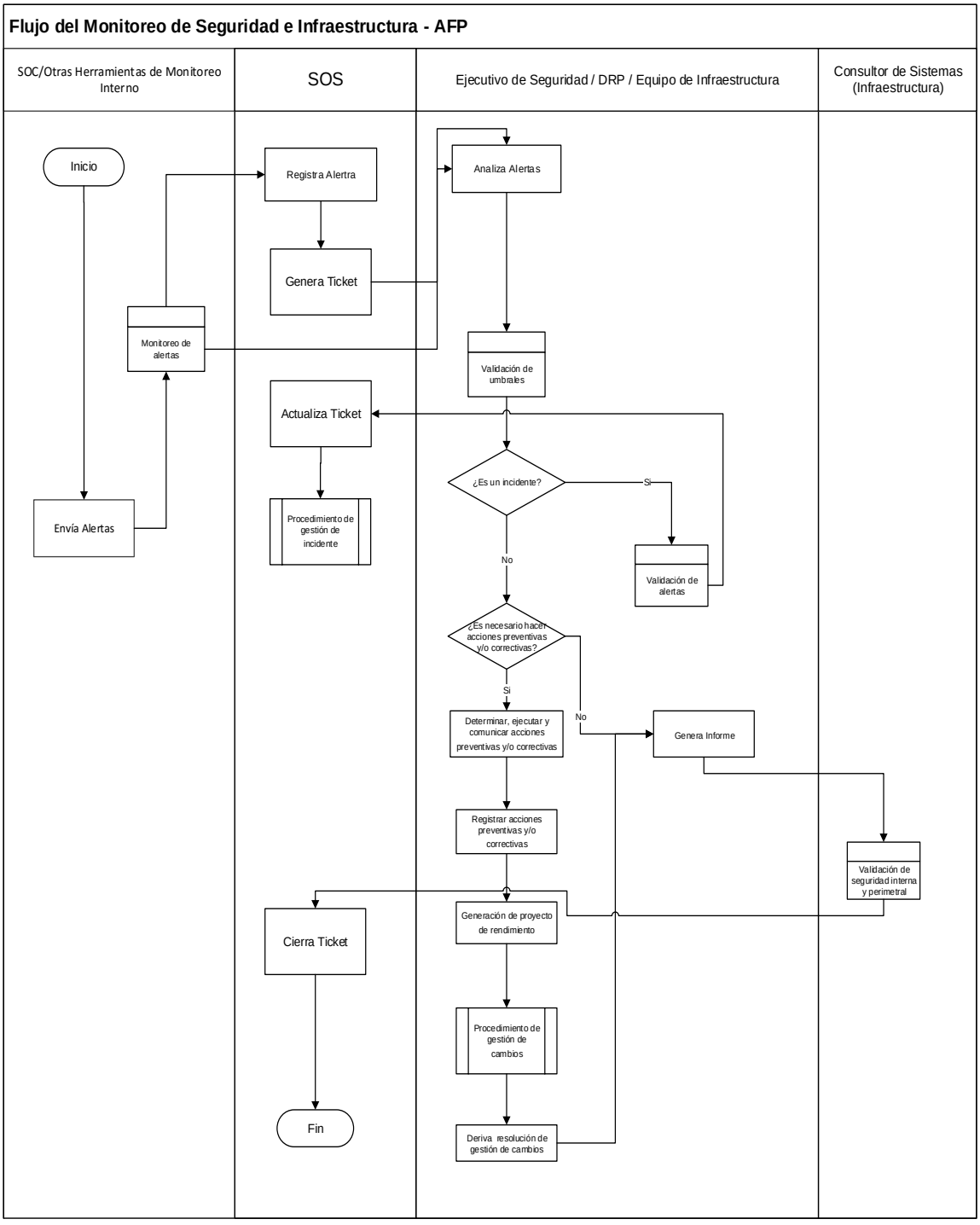


Fig. L1 Monitoreo de Seguridad e Infraestructura.
Fuente: Elaboración propia.

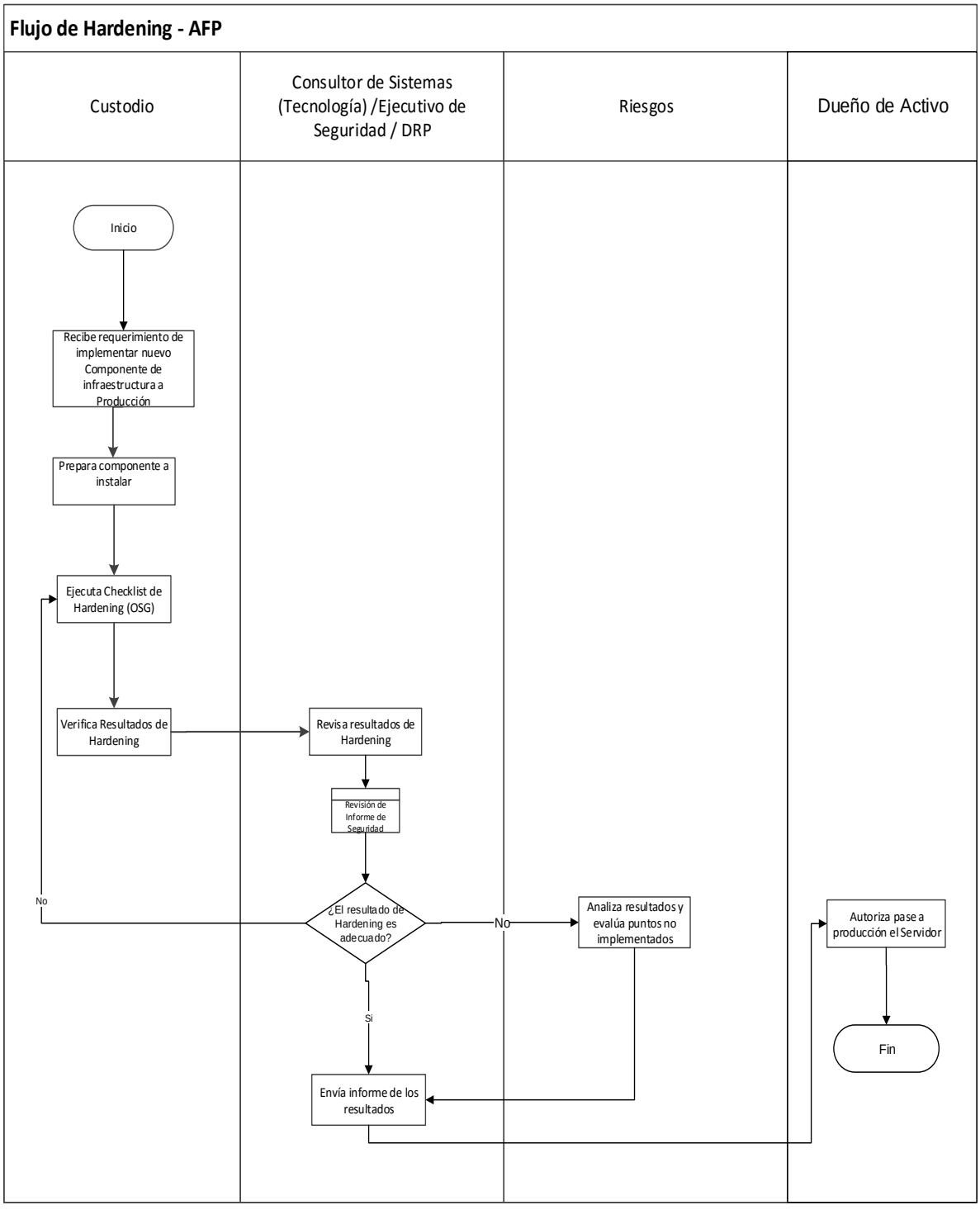


Fig. L2 Flujo de Hardening.

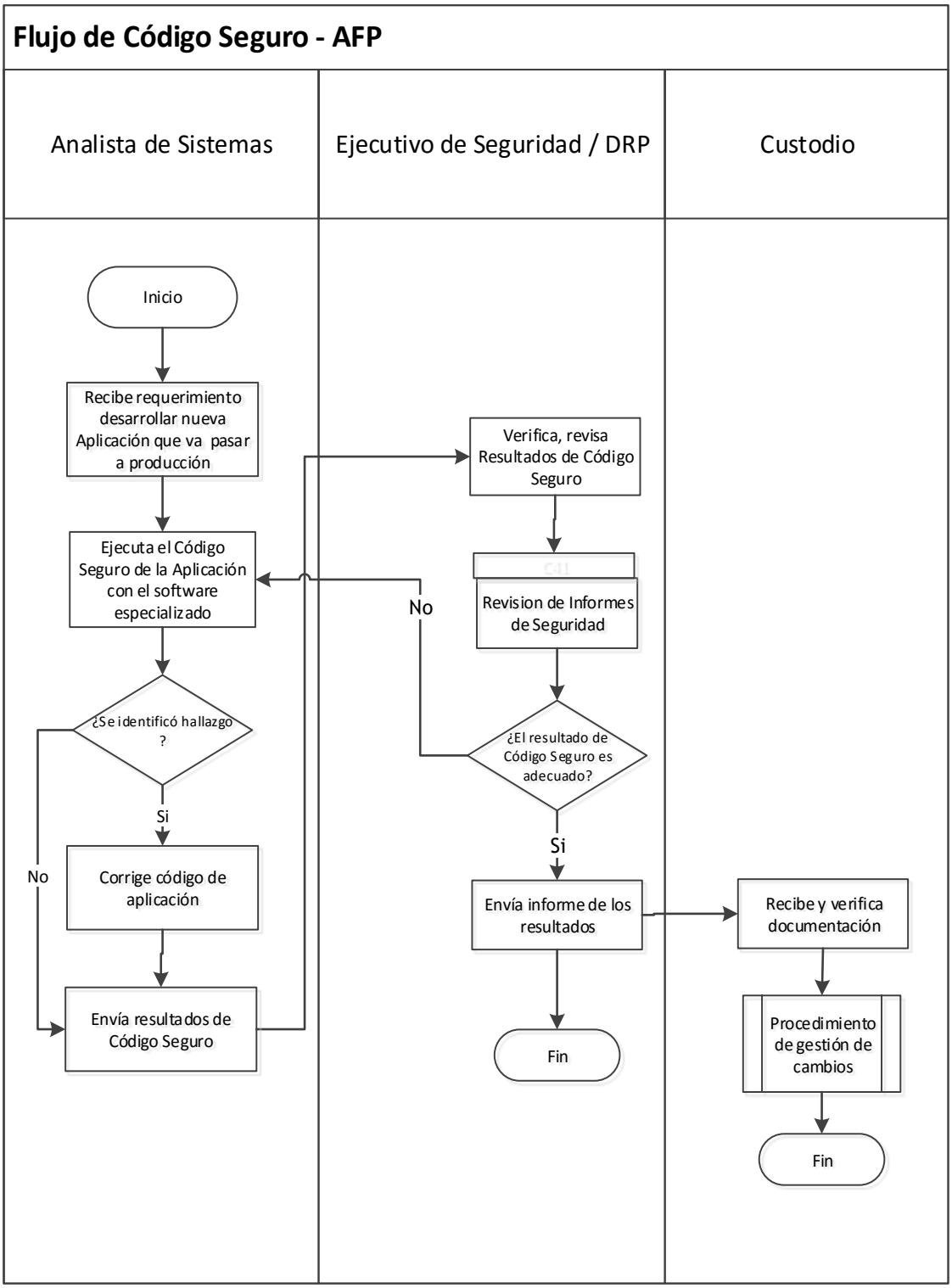


Fig. L3 Código Seguro.
Fuente: Elaboración propia.

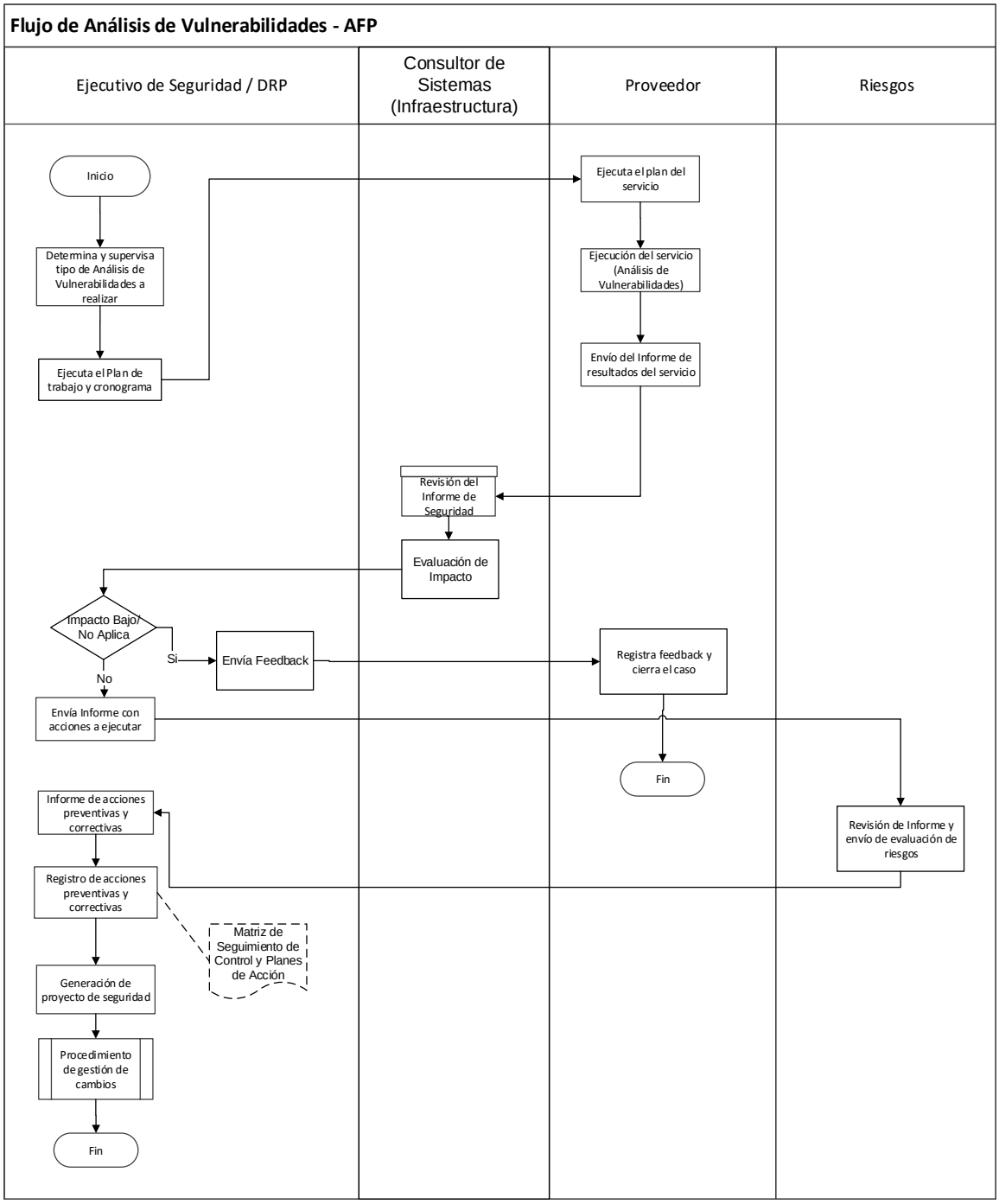


Fig. L4 Análisis de Vulnerabilidad.
Fuente: Elaboración propia.

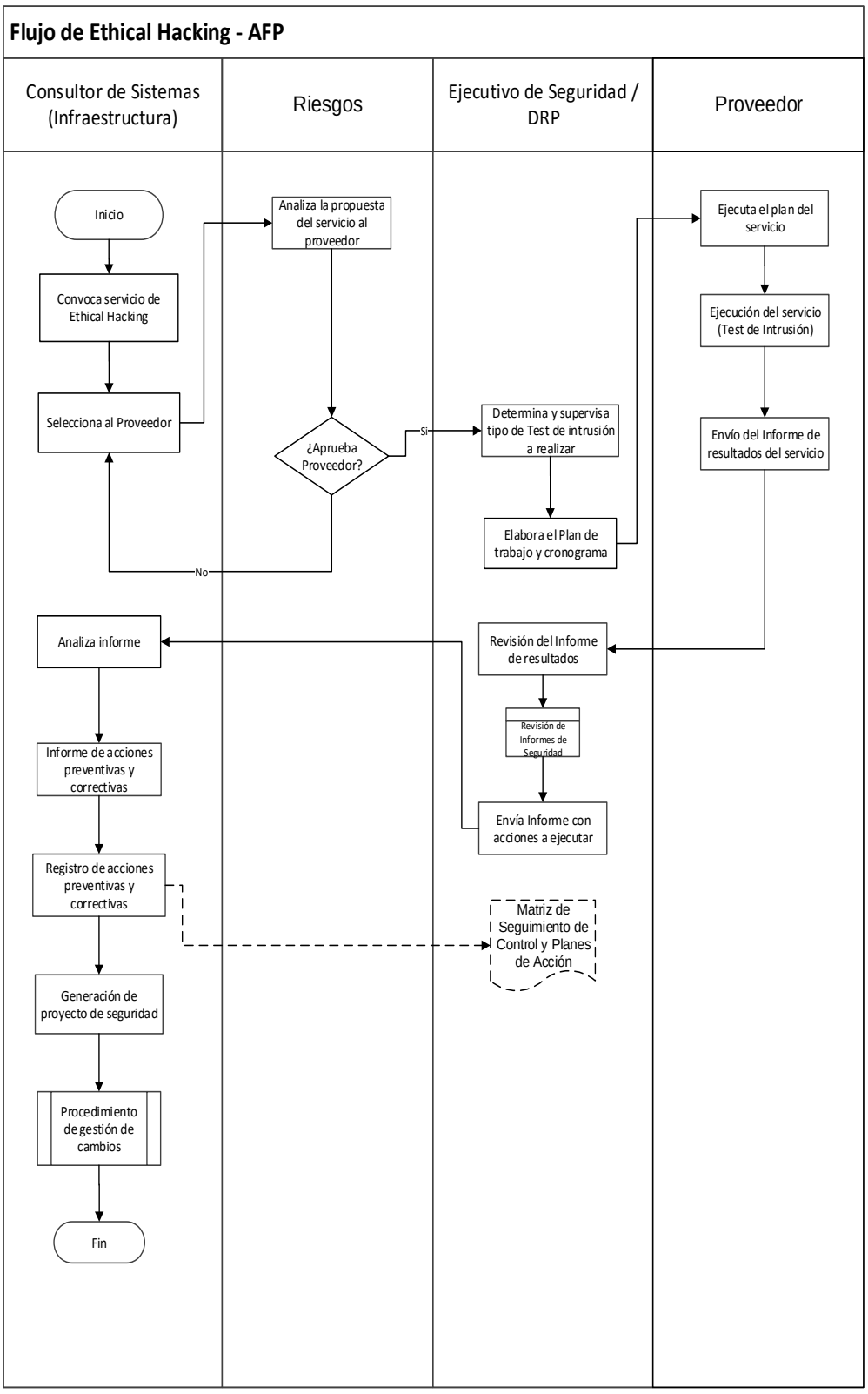


Fig. L5 Ethical Hacking.
Fuente: Elaboración propia.

Anexo M Operaciones

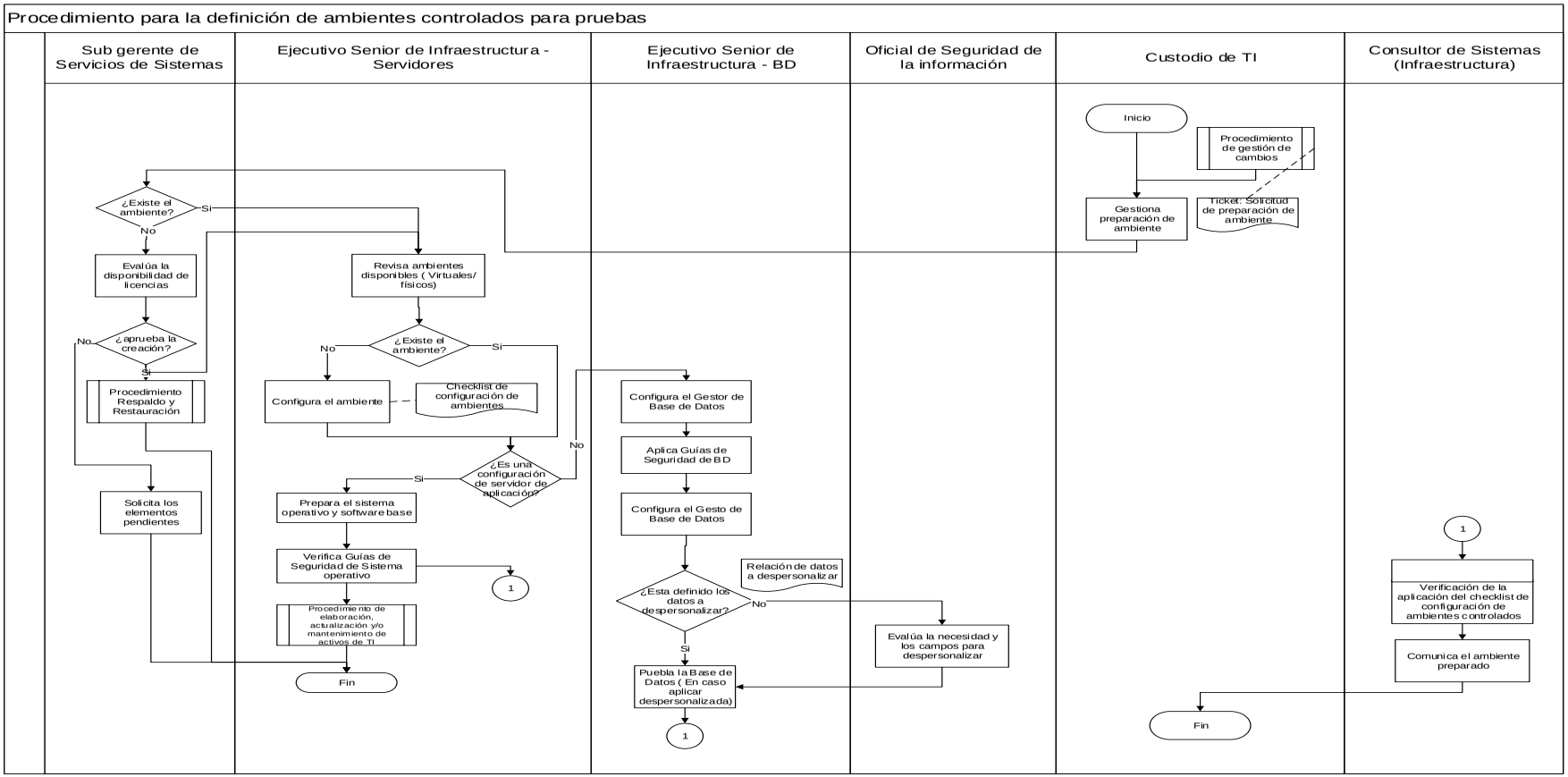


Fig. M1 Ambientes controlados para pruebas.
Fuente: Elaboración propia.

Diagrama de flujo detallado del procedimiento de gestión de tareas.

El procedimiento de gestión de tareas garantiza realizar, con cierta periodicidad, determinadas acciones o tareas definidas por el responsable de la administración del Centro de Cómputo.

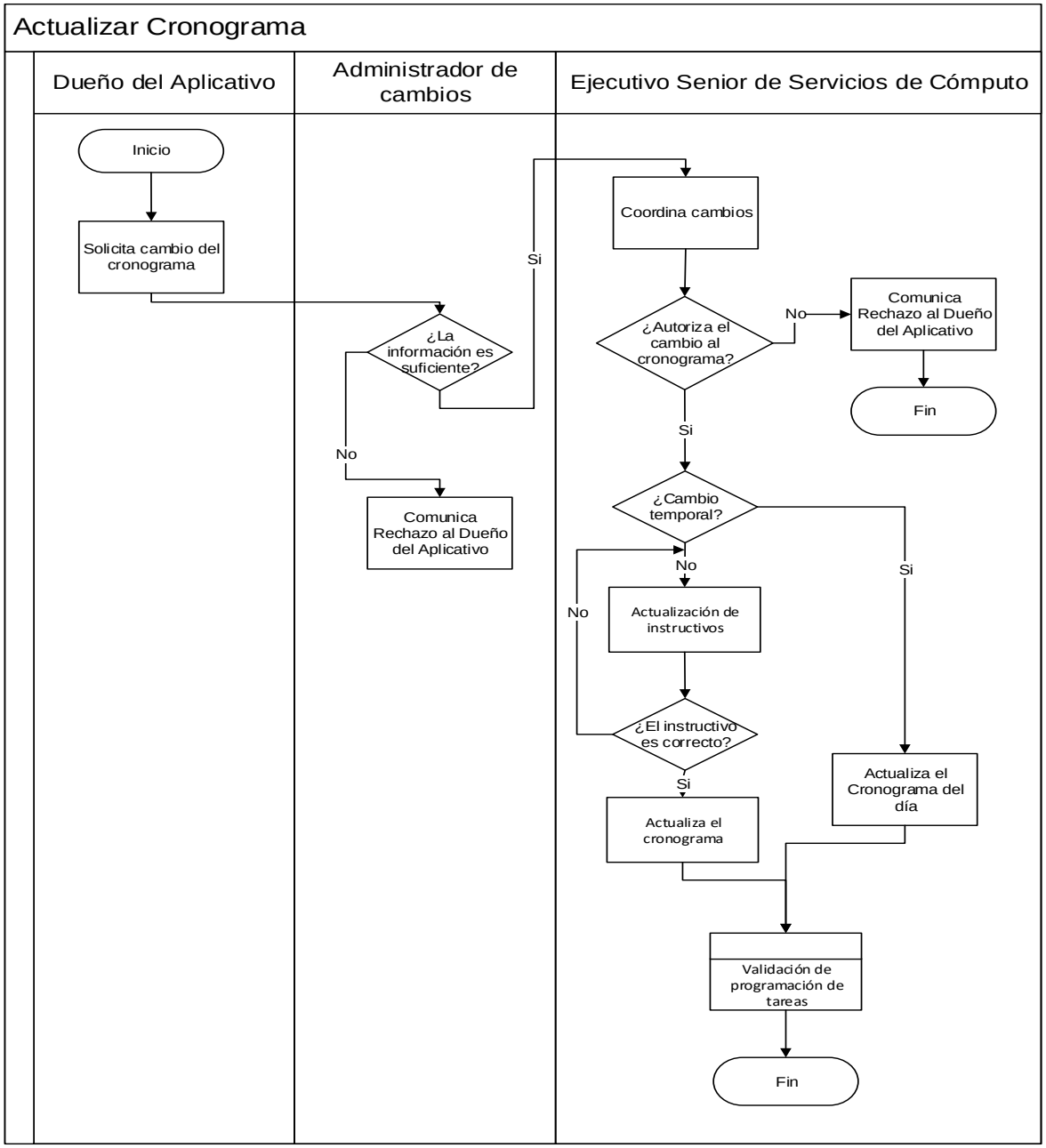


Fig. M2 Actualización de Cronograma
Fuente: Elaboración propia.

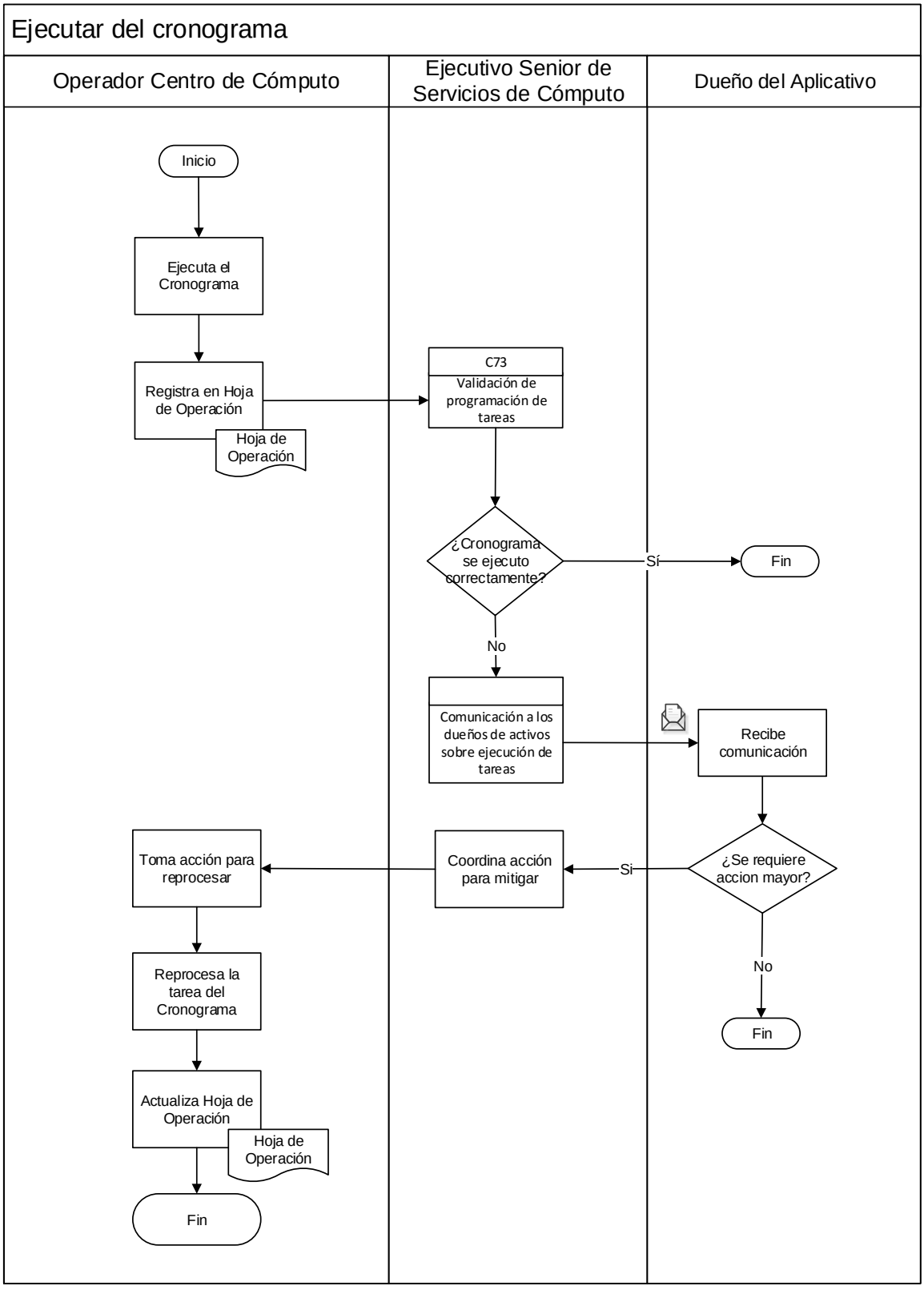


Fig. M3 Ejecución del Cronograma.

Fuente: Elaboración propia.

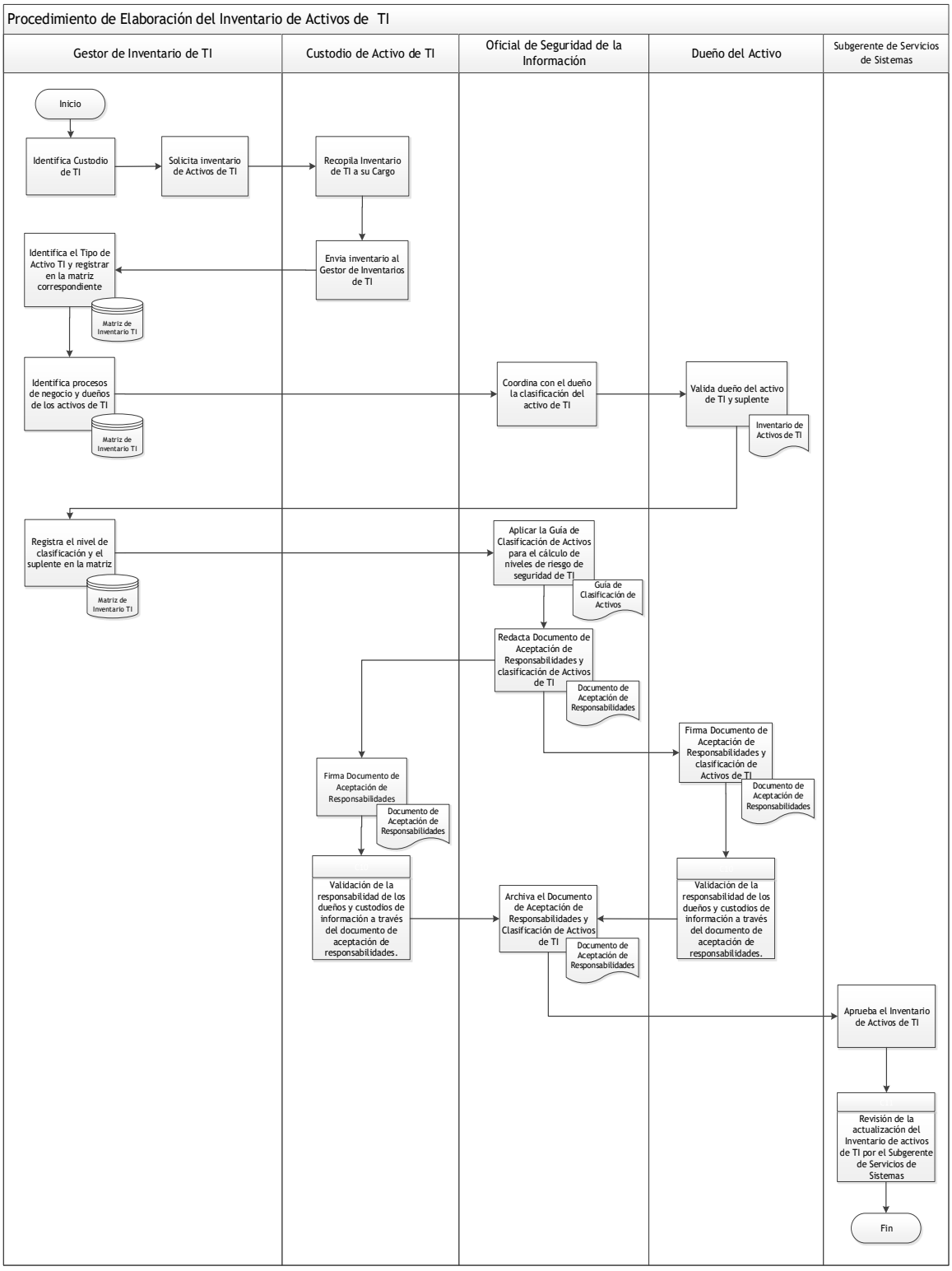


Fig. M4 Elaboración de Inventario de Activos.
Fuente: Elaboración propia.

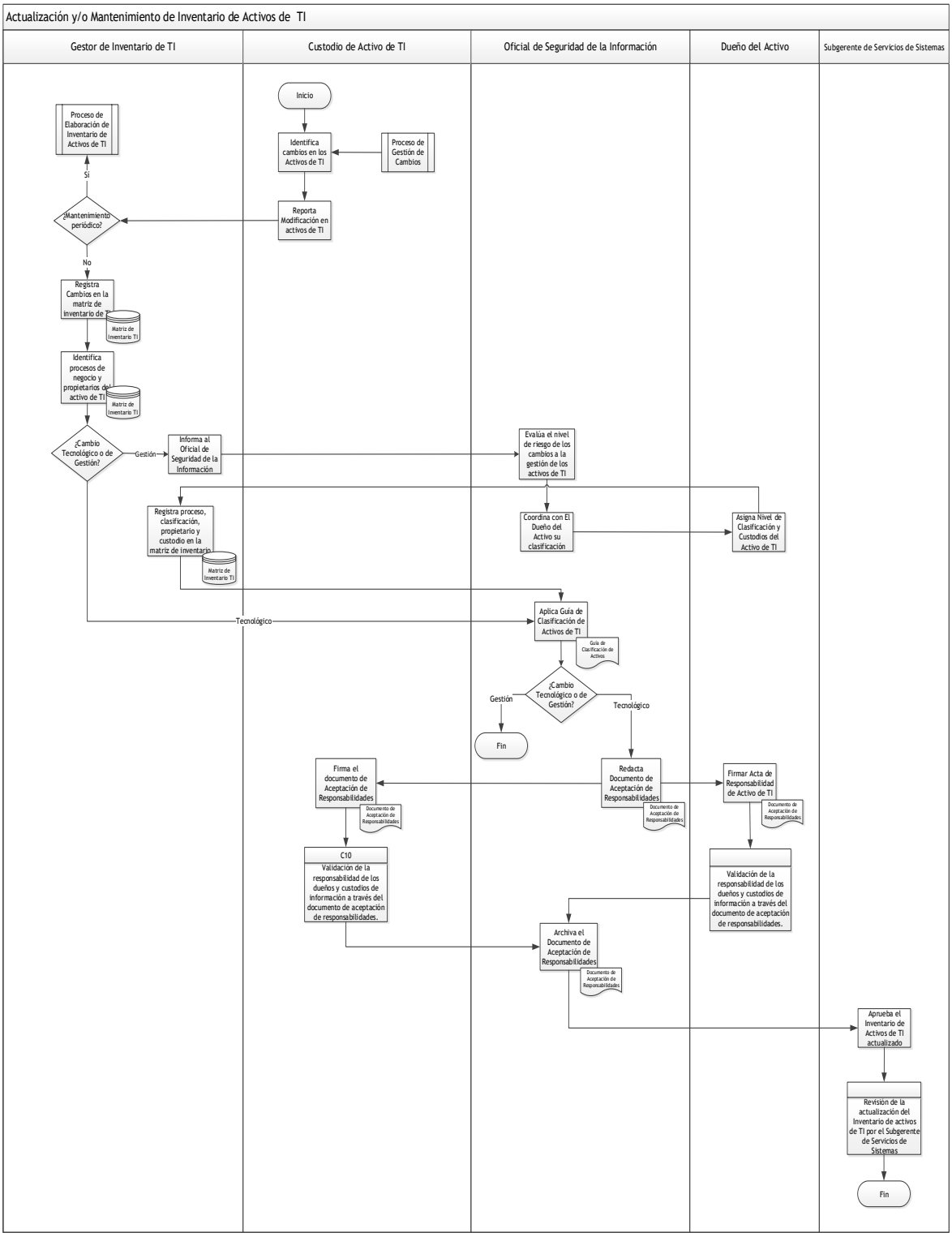


Fig. M5 Actualización y Mantenimiento de Inventario de Activos.
Fuente: Elaboración propia.

Criterios para la definición de los niveles de criticidad de los activos de TI:

En este anexo, se muestran los criterios a tomar en cuenta para la determinación del nivel de criticidad con relación a la Confidencialidad, Integridad y Disponibilidad de la información que son procesados en por activos de TI que son inventariados.

Para la identificación, se debe utilizar por cada uno de los activos de TI el formato mostrado, en la Tabla 7.20 para cada activo se debe llenar el formato y marcar los criterios según corresponda, ello permitirá que se calcule en forma automática el nivel de criticidad final.

Tabla M1 Confidencialidad

	LOW 1	MEDIUM 2	HIGH 3	CRITICAL 4
Type of Data Loss	✓ Material de marketing ✓ Estados financieros publicados. ✓ Datos no relacionados a datos de clientes ni empleados. ✓ Datos no relacionados a datos financieros. ✓ Datos no relacionados a un nuevo producto. ✓ Información pública de AFP (ejemplo: Web Portal) ✓ Material de Prensa.	✓ Agendas y actas de reunión. ✓ Intranet. ✓ Boletines internos. ✓ Los datos de clientes no vinculados a datos de cuentas o datos financieros. ✓ Datos financieros sin datos del cliente. ✓ Que contengan información personal de agentes y empleados sin información de Payroll (ejemplo: planes de entrenamiento y planes de carrera) ✓ Información no financiera usada para soportar aplicaciones financieras. ✓ Precios de productos. ✓ Políticas y Estándares Mínimos. ✓ Información de proveedores. ✓ Quejas de Clientes y de Proveedores (ejemplo: quejas de nivel de servicio, no recepción oportuna de documentación, etc.).	✓ La información de clientes con data financiera (Salario de Clientes Valores de Fondos, Estado de Cuenta de nuestros afiliados, etc.) ✓ Información de nuevo producto. ✓ Reporte de Auditoría, Riesgos, Incidentes o de reporte de Investigación. ✓ OSG de seguridad. ✓ Información de Empleados (planillas liquidación de remuneraciones) información asociada a Whistleblower) y de Agentes de Ventas no empleados de AFP (cálculo de comisiones, premios, concursos, etc.). ✓ Información de Empleadores. ✓ Datos médicos de nuestros clientes (Pensionistas Invalidez) y de nuestros Empleados. ✓ Cuentas vinculadas a los ingresos internos y los márgenes de AFP (Finanzas y Contabilidad). ✓ Información sobre beneficiarios de pólizas de seguro ✓ Información de productos patentados AFP. ✓ Licitación de proveedores (sobres con propuestas) ✓ Información Contable y Presupuestos. ✓ Información de tarjetas de créditos o cuentas corrientes bancarias (tanto de clientes como empleados). ✓ Acceso a recursos físicos, salvo data centers ✓ OSG y procedimientos específicos de seguridad. ✓ Composición del portfolio de inversiones (típicamente en un Sistema de Inversiones). ✓ Información técnica de IT relevante (ejemplo: CMDB, direcciones IP, fichas técnicas, arquitectura, reportes de pruebas de penetración, revisión de código, escaneo de vulnerabilidades, etc.). ✓ Repositorio central de código fuente de aplicaciones de negocio.	✓ Activos que procesan y/o almacenan: ✓ ✓ Pre-lanzamiento financieros o declaraciones de reglamentación. ✓ Fusiones y Adquisiciones de Empresas (Pre-Anuncio del evento). ✓ Contraseñas (passwords) incluyendo "one time passwords" de VPN's, PIN's, certificados digitales, etc. ✓ Secretos comerciales. ✓ Los datos de clientes que se pueden utilizar para iniciar las transacciones, (Ejemplo: una tabla en base de datos que contiene datos de tarjeta de crédito, nombre, dirección, ciudad, etc.). ✓ Acceso a Data centers. ✓ Estrategia de Inversiones (definición de donde se invertirán los fondos a futuro, típicamente en forma de minutas de reuniones y planillas Excel).
Regulatorio	✓ Poco o ningún impacto.	✓ Observación regulatoria.	✓ Riesgo de investigación del controlador/regulador.	✓ Riesgo de investigación del controlador/regulador

	LOW 1	MEDIUM 2	HIGH 3	CRITICAL 4
	✓No hay responsabilidad legal si la confidencialidad del sistema es violada.	✓No genera procesos legales. ✓No hay responsabilidad Legal si la Confidencialidad del Sistema es violada.	✓Potenciales procesos legales. ✓Responsabilidad legal esperada como consecuencia de la falta de confidencialidad. ✓Da lugar a incumplimiento de acuerdos de confidencialidad. ✓Demandas y juicios laborales/legales (ejemplos: inventario de juicios, documentación de los casos, etc.).	✓Procesos legales grandes o colectivos contra AFP. ✓Violación de Confidencialidad que da lugar a pérdida irreparable del negocio, acciones legales a gran escala en contra de AFP, perdida de Licencia para operar.
Perdida directa en el negocio (si se divulga a terceros)	✓Pérdida de ingresos o market share inmaterial.	✓Pérdida de market share o ingresos que se recupere en menos de un año. ✓Resultado en pérdida notable de cuota de mercado que requiere ajuste de producto / precio para la recuperación.	✓Pérdida de market share o ingresos que se recupere en menos de 5 años.	✓Pérdida de market share o ingresos que se recupere en más de 5 años.
Costos Adicionales	✓Costos adicionales no mayores a 10 K[1].	✓Costos adicionales menores a 30 K.	✓Costos adicionales menores a 300 K.	✓Costos adicionales mayores a 300 K.
Fraude	✓Ningún impacto.	✓Ningún impacto.	✓La información perdida puede generar fraude para AFP o los clientes.	✓La información perdida puede generar fraude para AFP o los clientes
Reputación	✓Sin publicidad.	✓Riesgo de que los medios de comunicación local tenga o generen daño contra AFP en un periodo de tiempo corto (1 semana).	✓Riesgo de que los medios de comunicación local tenga generen daño contra AFP en un periodo de tiempo medio (1 mes) a nivel local. ✓Atención continua de la Prensa. (frente a incidentes y/o eventos negativos).	✓Riesgo sustancial de que los medios de comunicación local tenga generen daño contra AFP en un periodo de tiempo alto (más de 1 mes). ✓Alta exposición en los medios.

Fuente: Elaboración propia.

Tabla M2 Integridad

	LOW 1	MEDIUM 2	HIGH 3	CRITICAL 4
Type of Data Loss	✓Cambios en la información que no tiene impacto directo en el negocio. ✓La modificación de información no impacta en las decisiones de la Administración. ✓No genera costos adicionales en caso de Incidente. ✓Aplicación que no almacena ni procesa datos de clientes, productos, empleadores, proveedores, margen y/o datos detallados de ingresos.	✓Datos básicos de funcionamiento en el equipo de Gestión, a nivel de departamento. ✓Anuncios de Prensa. ✓Información sobre precios y margen internos. ✓Información que alimenta la contabilidad, pero que no está en el alcance de auditorías externas (revisoría fiscal, superintendencia, etc), SOX u otra normativa aplicable. ✓Información interna de comisiones y el margen. ✓Información que no contiene transacciones financieras. ✓Información relacionada con incidentes, quejas de Clientes y Proveedores. ✓Información general de Recursos Humanos (planes de carrera, capacitación y boletines internos). ✓Materiales de marketing.	✓Información que alimenta la contabilidad, que está en el alcance de auditorías externas (revisoría fiscal, superintendencia, etc.), SOX u otra normativa aplicable. ✓Estados Financieros (Reportes y sistemas) a nivel del Business Unit. ✓Cuentas que están linkeadas a los ingresos y márgenes de la compañía. ✓Modificación de datos de Proveedores. ✓Modificación de datos de clientes (RIA, fondos, edad). ✓Modificación de datos de Empleadores (Deudas, Pagos en Exceso). ✓Sitio Web expuesto al exterior (Modificación de su contenido). ✓Aplicación de los procesos principales del negocio (por ejemplo: Sistema de pagos / recaudación, venta, siniestros, sistemas core, etc.). ✓Cuentas que están linkeadas a los ingresos y márgenes de la compañía. ✓Datos de clientes (por ejemplo: salario, fondos, edad, etc.). ✓Datos de Empleadores (Deudas, Pagos en Exceso, etc.).	✓Sistemas de Pago (Transacciones bancarias) (ACH / Check Payment / etc.). ✓Los datos de la cuenta vinculada con ambos, datos al cliente y márgenes internos e ingresos, ej. cuenta bancaria para pago del afiliado, junto con su nombre, cédula, dirección, etc. ✓Los datos de estrategia o resultados financieros (antes de ser publicados) utilizados para la presentación de informes a : ➢Asamblea de Accionistas. ➢Los gobiernos, las autoridades. ➢Juntas ejecutivas o Directorio.
Regulatorio	✓Poco o ningún impacto. ✓No hay responsabilidad legal si la integridad del sistema es violada.	✓Observación regulatoria sin multas. ✓Violación de la Integridad que dan como resultado costos esperados de responsabilidad jurídica sin proceso legales o en tribunales.	✓Riesgo de investigación del controlador / Regulador ✓Violación de la Integridad que dan como resultado costos esperados de responsabilidad jurídica y potencial proceso legales o en tribunales.	✓Perdida de la Licencia para operar. ✓Riesgo de investigación del controlador / Regulador. ✓Violaciones de la Integridad que dan como resultado costos esperados de responsabilidad Jurídica y proceso en Tribunales. ✓Procesos legales grandes o colectivos contra AFP.

	LOW 1	MEDIUM 2	HIGH 3	CRITICAL 4
Reputación	✓Sin publicidad ✓Pérdida de ingresos o market share inmaterial.	✓Riesgo de que los medios de comunicación local tenga generen daño contra AFP en un periodo de tiempo corto (Dará lugar a 1 semana en la prensa nacional.) ✓Capacidad para engañar a los clientes en cuanto a pretender ser AFP, por ejemplo, intrusión en ✓Exchange para publicar números de teléfonos falsos. ✓Pérdida de market share o ingresos que se recupere en menos de un año.	✓Riesgo de que los medios de comunicación local tengan generen daño contra AFP en un periodo de tiempo medio (1 mes) y a nivel local. ✓Resultado en pérdida notable en cuota de mercado que requiere un año para recuperarse. ✓Pérdida de market share o ingresos que se recupere en menos de 5 años. ✓Que requiere cambio en presupuesto para corregir problemas.	✓Riesgo sustancial de que los medios de comunicación local tenga generen daño contra ✓AFP en un periodo de tiempo largo (más de un mes), y/o a nivel internacional ✓Resultado en pérdida notable en cuota de mercado e ingresos, que requiere + 5 años para recuperarse. ✓Cambio de presupuesto para corregir problemas.
Costos Adicionales	✓No genera costos adicionales en caso de Incidente. ✓<1% del total de los recursos humanos del Business Unit deben parar sus funciones por menos de un día. ✓Consecuencias para otras "cadenas de Valor"	✓Costos adicionales menores a 30 K. ✓<1% del total de los recursos humanos del Business Unit deben parar sus funciones por más de un día. ✓Consecuencias para otras "cadenas de Valor"	✓Costos adicionales menores a 300 K. ✓>1% del total de los recursos humanos del Business Unit deben parar sus funciones por menos de un día. ✓Consecuencias para otras "cadenas de Valor" Criticas.	✓Costos adicionales mayores a 300 K. ✓>1% del total de los recursos humanos del Business Unit deben parar sus funciones por más de un día. ✓Consecuencias para otras "cadenas de Valor" Criticas.
Fraude	✓La modificación de información no puede generar un fraude.	✓La modificación de información no puede generar un fraude.	✓La información perdida puede generar fraude para AFP o los clientes.	✓La información perdida puede generar fraude para AFP o los clientes.

Fuente: Elaboración propia.

Tabla M3 Disponibilidad

	LOW 1	MEDIUM 2	HIGH 3	CRITICAL 4
Type of Data Loss	✓RTO[2] > 48 hrs. (La aplicación no pertenece a una cadena de valor del negocio - La aplicación no tiene requerimientos críticos de Disponibilidad Operacional (BCP).	✓RTO → 4 - 48 hrs. (Alineado con definición para BCP (como mínimo). Por razones de servicio o competitividad podría ser un RTO menor al del BCP.)	✓RTO → 2 - 4 hrs. Alineado con definición para BCP (como mínimo). Por razones de servicio o competitividad podría ser un RTO menor al del BCP.	✓RTO → < 2 hrs. Alineado con definición para BCP (como mínimo). Por razones de servicio o competitividad podría ser un RTO menor al del BCP.

Fuente: Elaboración propia.

Leyenda: 1: K = miles de Euros.
2: RTO = Return Time to Operation
3: BCP = Business Continuity Planning

Acta de Aceptación de Responsabilidades del Propietario de Activos de TI

Aceptación de Responsabilidad del Propietario de Activos

En conformidad con las Políticas de Seguridad Informática de la compañía, a continuación se muestran las responsabilidades asociadas al Propietario del Activo.

Administración de Usuarios:

- Aprobar o rechazar solicitudes, de acceso físico o lógico, asociadas a los activos asignados, incluyendo el acceso a archivos / directorios, conexiones de red y préstamos de activos físicos.
- Participar junto al área de Servicios de Sistemas de las revisiones de acceso anual a los activos que tienen a su cargo, asegurando que los usuarios cuenten con los accesos adecuados de acuerdo a la función que desempeñan en la compañía.
- Desarrollar una matriz de acceso para cada activo que está bajo su control considerando segregación de funciones.
- Informar al grupo de Administración de Cuentas y Accesos los ceses y cambios de accesos a usuarios sobre los activos asignados.

Desarrollo y Mantenimiento de Aplicaciones / Sistemas:

- Aprobar o rechazar los sistemas y las solicitudes de cambio a sistemas existentes de acuerdo al procedimiento y política de Administración de Cambios de la compañía.
- Evaluar, con el apoyo del Custodio TI, el impacto potencial de cualquier cambio sobre los activos asignados.
- Aprobar o rechazar el uso de información de producción en los ambientes de pruebas, incluyendo la aprobación de despersonalización de datos.
- Aprobar o rechazar la implementación de cambios en los ambientes de producción.

Clasificación de Activos:

- Asegurar que los aplicativos estén clasificados bajo los términos de Confidencialidad, Integridad, y Disponibilidad (Frecuencia de revisión: 3 años).

Evaluación de Riesgos

- Apoyar al área de Riesgos Operativos en la realización de las evaluaciones de riesgos de los activos asignados.
- Participar en la investigación sobre las incidencias de seguridad asociadas a los activos que tiene a su cargo.

Proveedores:

- En caso un proceso o servicio ha sido tercerizado a un proveedor y este maneje información confidencial de la compañía, se deberá informar al área de Riesgos Operativos para que realice la evaluación de riesgos respectiva. Asimismo, el propietario del proceso tercerizado será responsable de gestionar y garantizar la implementación de los controles necesarios para la seguridad de la información manejada por los proveedores.

Cualquier actividad no cubierta por las políticas, procedimientos y estándares relacionados a la seguridad de la información deberá ser comunicada a la brevedad al Área de Riesgos Operativos.

Será responsabilidad del Propietario del Activo recomendar, inducir y crear las directrices correspondientes para no incurrir en actividades que podrían comprometer la seguridad de los activos de información relacionados.

Nombre	Puesto	Firma
Propietario y Suplente del Activo		

Acta de Aceptación de Responsabilidades del Custodio de Activos de TI

Aceptación de Responsabilidad del Custodio de Activos

En conformidad con las Políticas de Seguridad Informática de la compañía: Acceso a Usuarios, Seguridad en Plataforma, Resilencia en TI, Control de Cambios y Monitoreo de Seguridad.

A continuación se muestran las responsabilidades asociadas a los Custodios de Activos:

- Ayudar al propietario del activo a identificar los mecanismos de control de seguridad de la información asociados a los activos.
- Verificar que se cumpla con el desarrollo, implementación y mantenimiento de los mecanismos de control asociados a los activos. Así mismo tiene que encargarse de verificar que funcionen de manera correcta y efectiva.
- Reportar al propietario del activo los problemas e incidentes que puedan afectar al activo.
- El custodio del activo junto al propietario tienen que informar el alta o baja de un activo con el fin de mantener actualizado el inventario de los activos de información de la compañía.
- Responsable de la ejecución de los controles definidos en los mínimos estándares de Change Management, User Access, Platform Security, IT Resilience, IT Sourcing, Security Monitoring y Foundation Controls.
- Responsable de la administración de creación, cambio y eliminación de accesos a los activos.
- Responsable de la ejecución de los controles definidos en el procedimiento de Administración de Cambios (Identificación y requerimiento de cambio, Análisis, Diseño, Construcción, Pruebas y Pase a producción).
- Responsable de la implementación de las OSG´s (Operating Security Guideline) de los activos.

Cualquier actividad no cubierta por las políticas, procedimientos y estándares relacionados a la seguridad de la información deberá ser comunicada a la brevedad al Departamento de Riesgos Operativos.

Será responsabilidad del Custodio de Activos recomendar, inducir y crear las directrices correspondientes para no incurrir en actividades que podrían comprometer la seguridad de los activos de información relacionados.

Nota: La firma del presente documento implica su aceptación

Nombre	Puesto	Firma
Custodio del Activo		

Tabla M4 Formato de Matriz de Inventario de Activos de TI

La matriz de inventario de activos de debe contener en forma mínima los siguientes campos:

#	Activo	Proceso	Descripción	Propietario	Tipo de activo	Custodio	C	I	D	Criticidad del Activo

Fuente: Elaboración propia.

Leyenda:
C: Confidencialidad
I: Integridad
D: Disponibilidad

Tabla M5. Formato de Matriz Inventario de Servidores Físicos y Virtuales

Inventario de Servidores

Fecha:

Avance Revision Accesos	
Avance Revision OSGs	

											AÑO:							Dueños				
Plataforma	Status	Unidad de Negocio	Descripcion	Nombre	Comentarios IT	Categoría	Configuracion	Físico Virtual	IP	Aplicaciones (Mayor clasificación)	C	I	D	Risk Level	Ultima revision accesos	Revision OSGs	SOX	Titular	Suplente	Administrador	Bckup Information	License Information

Servidores Producción	0
Servidores Pre-Producción	0
Servidores Testing	0
Servidores Desarrollo	0
Servidores Contingencia	0
Total	0

Físicos	0
Virtuales	0

SOX 1

Fuente: Elaboración propia.

Tabla M6 Formato de Matriz Inventario de Aplicativos

Inventario de Activos - Aplicativos

Avance Revision Accesos		
Avance Revision OSGs		

												A.CIA-rating												
ID	UNIDAD DE NEGOCIO	Proceso de Negocio	TITULAR ASSET OWNER	Nuevo Titular Asset Owner	SUPLENTE	Nuevo Suplente	RESPONSABLE TI	Nuevo Responsable TI	PLATAFORMA	CODIGO	NOMBRE APLICACION/ MODULO	DESCRIPCION	CONFD	INTEG	DISPO	RISK SM	SOX	REPOSITORIO HARVEST	Aprobado x Dueño	Ultima Revision CIA	Ultima revision accesos	Ultima revision OSGs	ADMINISTRADOR	Backup Information	License Information

Fuente: Elaboración propia.

Tabla M7 Formato de Matriz Inventario de Equipos de Comunicación

Inventario de Activos Equipos de Comunicación		Avance Revision Accesos	
Fecha		Avance Revision OSGs	

Plataforma	Status	Unidad de Negocio	Nombre Activo	Descripción	Cantidad	Antigüedad (años)	IP	Proceso	AÑO:			Risk Level	Ultima revision accesos	Revision OSGs	SOX	Dueños		Administrador	Bckup Information	License Information
									C	I	D					Titular	Suplente			

Fuente: Elaboración propia.

Tabla M8 Formato de Matriz Inventario de Equipos de Seguridad

Inventario de Activos Equipos de Seguridad		Avance Revision Accesos	
Fecha:		Avance Revision OSGs	

Plataforma	Status	Unidad de Negocio	Nombre Activo	Descripción	Cantidad	IP	Proceso	AÑO:			Risk Level	Ultima revision accesos	Revision OSGs	Dueños		Administrador	Bckup Information	License Information
								C	I	A				Titular	Suplente			

Fuente: Elaboración propia.

Tabla M9 Formato de Matriz Inventario de Servicios Genéricos

Perú	Inventario de Servicios Genericos Nombre de la empresa Fecha:									
Tipo	Servicio	CARGO DEL DUEÑO DE PROCESO	SUPLENTE	AÑO:			Risk Level	Dueños		Administrador
				C	I	D		Titular	Suplente	

Fuente: Elaboración propia.

Tabla M10. Formato de Matriz Inventario de Conexiones Externas

Perú

Risk & Control Self Assessment
Identificación de Activos - Conexiones Externas
Comité de Evaluación de Conexiones Externas

Fecha: Actualizado xxxxxxxx

Listed all external connection of AFP Integra (Y2011)

N°	ID Name	Description Connection Services	Clasificación CIA			Nivel de Confianza		Propietario del Activo Owner	Suplente	Cargo del propietario Owner	Propietario de la Infraestrucura Owner	Expiration Date
			Confidencialidad	Integridad	Disponibilidad							
I. Conexiones Fisicas												
II. Conexiones Dial Up												
III. Otras Conexiones												
IV. Servicios de Internet												

Sub Gerente de Riesgos Operativos	Consultor de Sistemas	Sub Gerente de Servicio de Sistemas	Gerente Central de Operaciones y

Fuente: Elaboración propia.

Tabla M11. Criterios para la definición de los niveles de criticidad de los activos de TI

GUÍA DE CLASIFICACIÓN DE ACTIVOS DE TI

Unidad de negocio:	PERU
Custodio de TI:	
Nombre del Activo:	
Código:	
Dueño del activo:	
Fecha de clasificación:	

Nivel de criticidad		Bajo 1	Medio 2	Alto 3	Crítico 4
CONFIDENCIALIDAD	**Type of Data Loss**				
	Regulatorio				
	Pérdida directa en el negocio (si se divulga a terceros)				
	Costos adicionales				
	Fraude				
	Reputación				
INTEGRIDAD	**Type of Data Loss**				
	Regulatorio				
	Reputación				
	Costos adicionales				
	Fraude				

Disponibilidad				
Type of Data Loss				

Criticidad del Activo

	Nivel de criticidad
Confidencialidad	
Integridad	
Disponibilidad	

Dueño de Activo

Custodio de TI

Responsable de Riesgos Operativos

Fuente: Elaboración propia.

Anexo N Resilencia y Seguridad Física

El procedimiento de monitoreo de controles ambientales y físicos del centro de cómputo garantiza la protección contra factores ambientales y el acceso no autorizado.

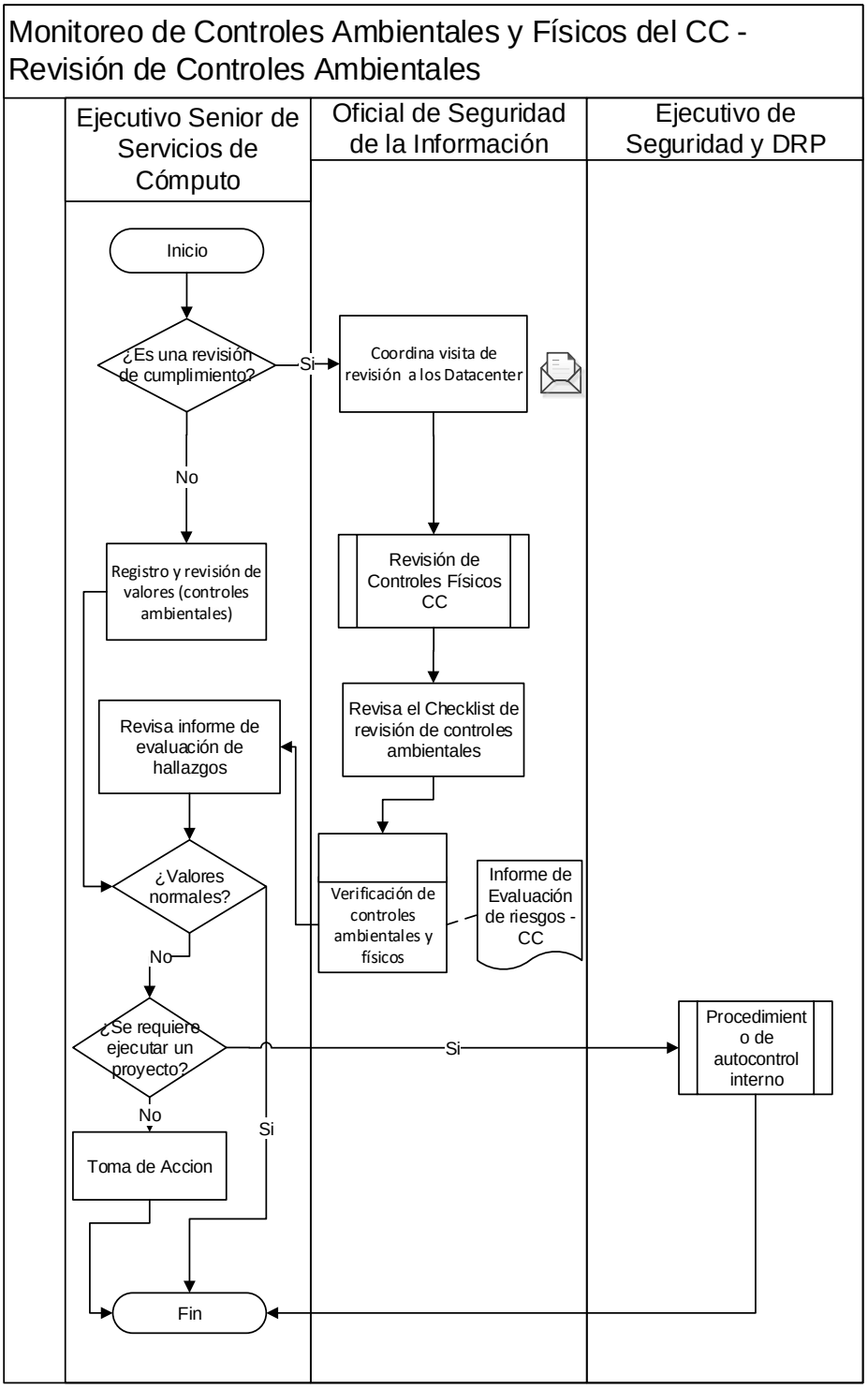


Fig. N1 Monitoreo de Controles ambientales y Físicos en el Centro de Cómputo.
Fuente: Elaboración propia.

Lineamiento de Uso del Centro de Cómputo.

Con el propósito de mantener la seguridad e integridad del Data Center (CDD), es importante seguir los siguientes lineamientos:

- Todo acceso al (CDD) deberá ser autorizado previamente. Se requiere que los visitantes registren a la entrada, antes de que se les conceda el acceso y notificarse igualmente la hora de salida del mismo.

- Solo las personas registradas en la lista de autorización permanente, pueden ingresar no acompañados, el resto de personas ingresantes son considerados visitantes y deben de justificar su visita y estar acompañados por personal de TI.

- Las tarjetas de control de acceso no podrán ser prestadas a nadie más que no sea la persona a la cual se le ha entregado.

- Materiales inflamables o peligrosos (como por ejemplo cartón, cajas, papel o cualquier otro material similar), no podrán ser almacenados dentro de ningún espacio de la sala de servidores en el Data Center.

- Al finalizar cualquier trabajo en el Data Center, se deberá asegurar que todos sus cables estén bien instalados y ordenados, dentro de sus gabinetes, así como asegurarse que todas las puertas están cerradas.

- El Data Center debe mantenerse limpio y ordenado en todo momento.

- No se permiten comidas ni bebidas.

- Se prohíbe fumar dentro del Data Center.

- No se permite tomar fotos ni el uso de cámaras fotográficas o cámaras de video.

- Los visitantes no pueden introducir ni utilizar ninguno de los siguientes materiales en el Data Center:

    - ✓ Productos derivados del Tabaco
    - ✓ Explosivos
    - ✓ Armas
    - ✓ Químicos
    - ✓ Drogas ilegales
    - ✓ Artículos electromagnéticos
    - ✓ Materiales radioactivos
    - ✓ Cámaras fotográficas o de video
    - ✓ Cualquier otro artículo similar a los antes mencionados, que a la sola discreción de la empresa, considere como peligrosos o dañinos.

- La empresa se reserva el derecho de inspeccionar todos los objetos que entran o salen del Data Center, así como de sacar de las instalaciones cualquier objeto especificado en el documento. Se solicitará a cualquier persona que entre o salga del Data center con paquetes, que señale cuál es el contenido del mismo.

Tabla N Control de Acceso al Centro de Cómputo (Personal no autorizado)

Fecha	Nombre Completo	Doc. de Identidad	Area o Empresa	Hora de Entrada	Tarea a Realizar	Hora de Salida	Firma	Nombre Autorizador	Firma Autorizador

Fuente: Elaboración propia.

Anexo Ñ Gestión de Seguridad en Plataforma.

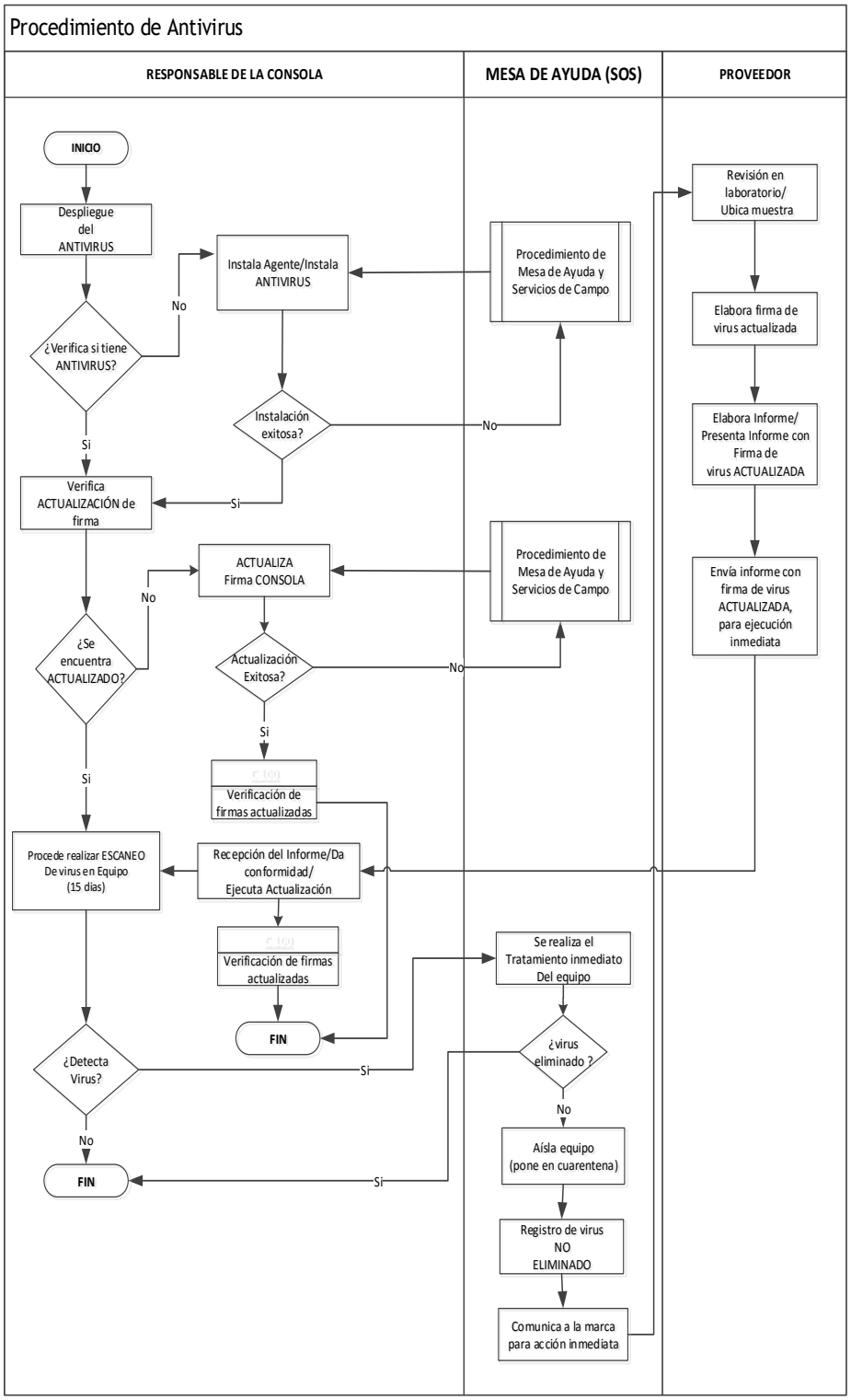


Fig. Ñ1 Antivirus
Fuente: Elaboración propia.

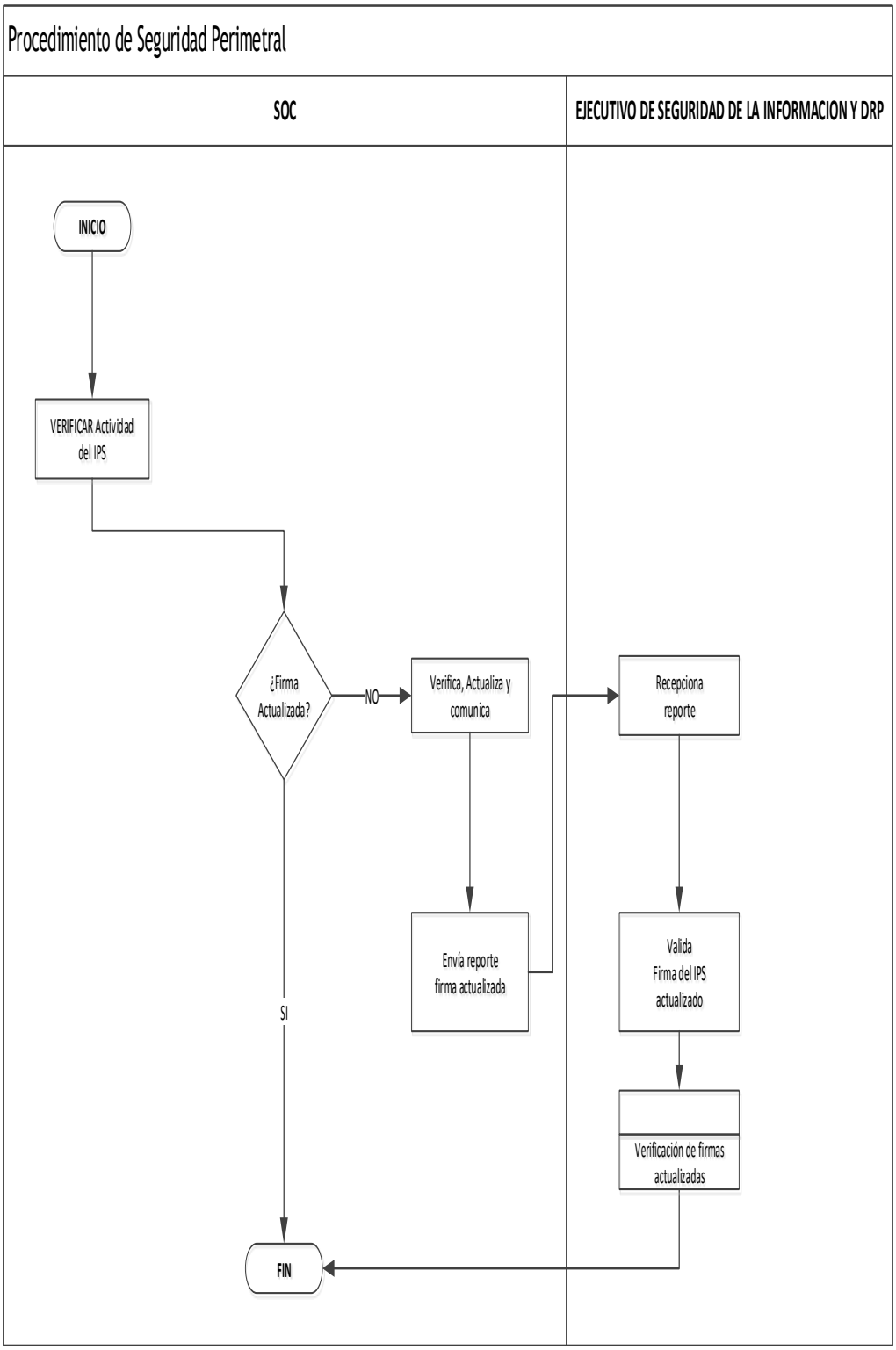


Fig. Ñ2 Seguridad Perimetral.
Fuente: Elaboración propia.

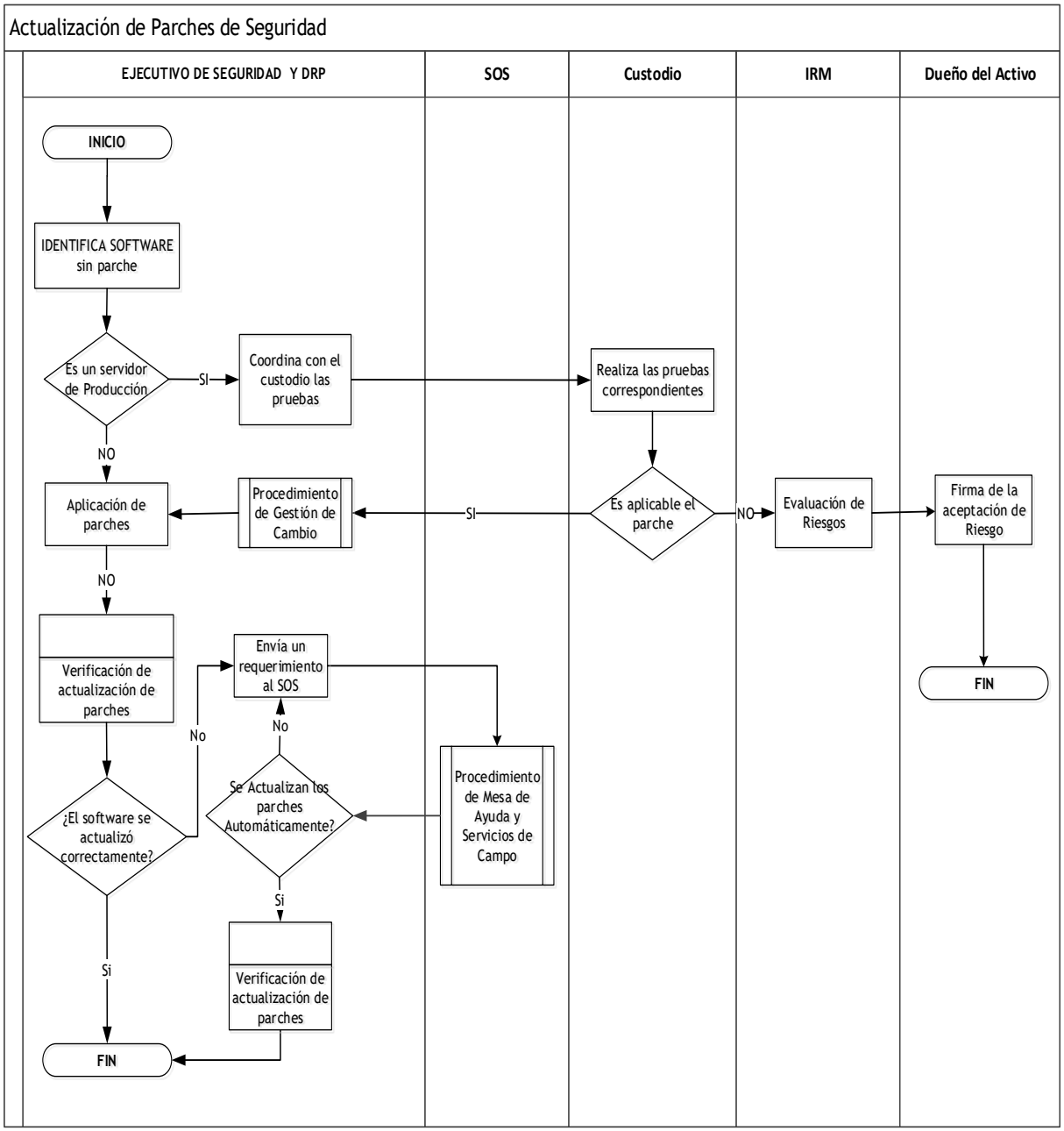


Fig. Ñ3 Parches de Seguridad.

Fuente: Elaboración propia.

Anexo O Gestión de los Niveles de Servicio.

La gestión del Nivel de Servicio es un proceso vital para la provisión de los servicios TI, ya que es responsable de acordar y documentar los objetivos de nivel de servicio y las responsabilidades establecidas en los SLAs “Service Level Agreement” y SLRs “Service Level Requirement”, con el respaldo de los OLAs “Operational Level Agreement” y UCs “Underpinning Contracts”.

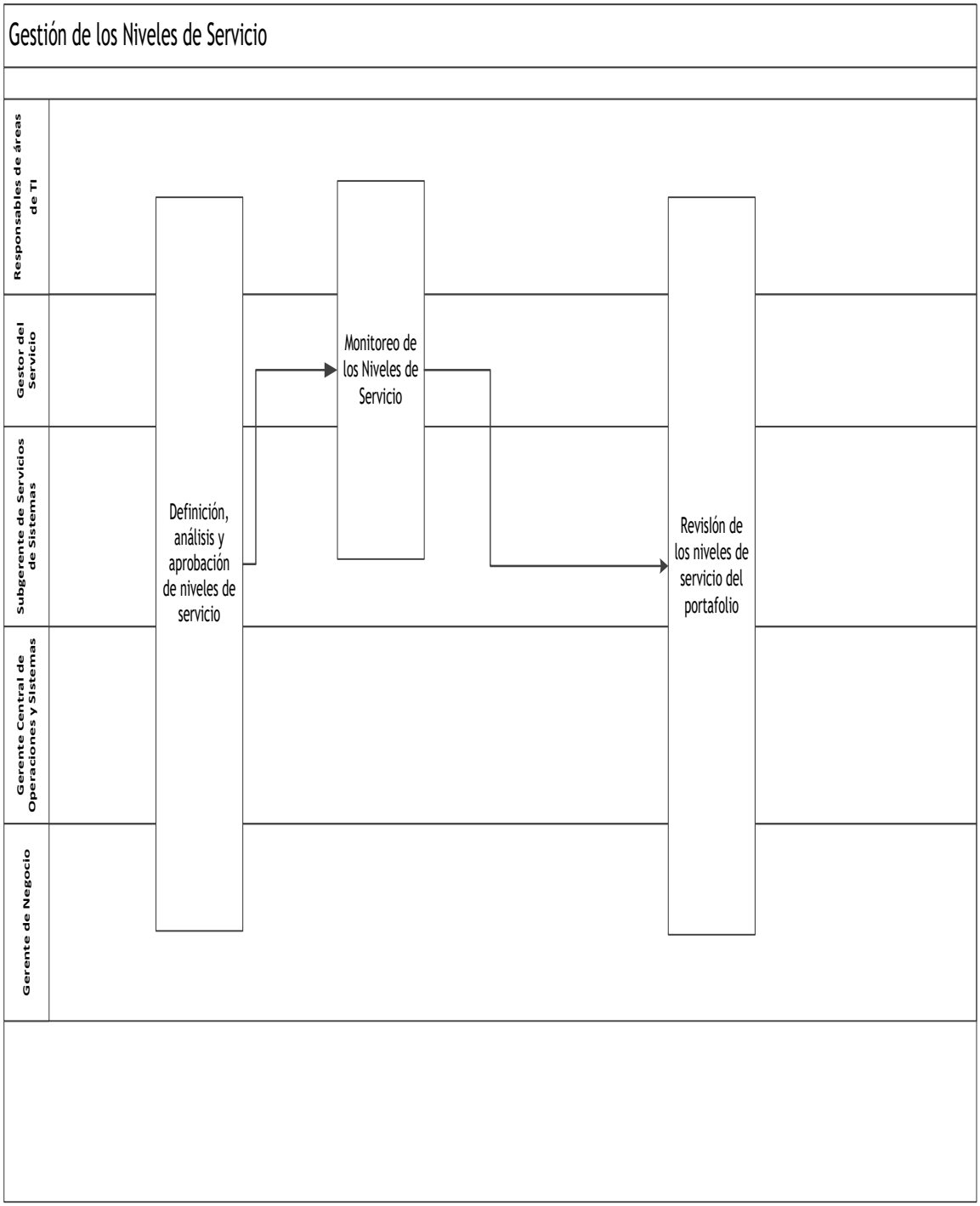


Fig.O1 Gestión de Niveles de Servicio.
Fuente: Elaboración propia.

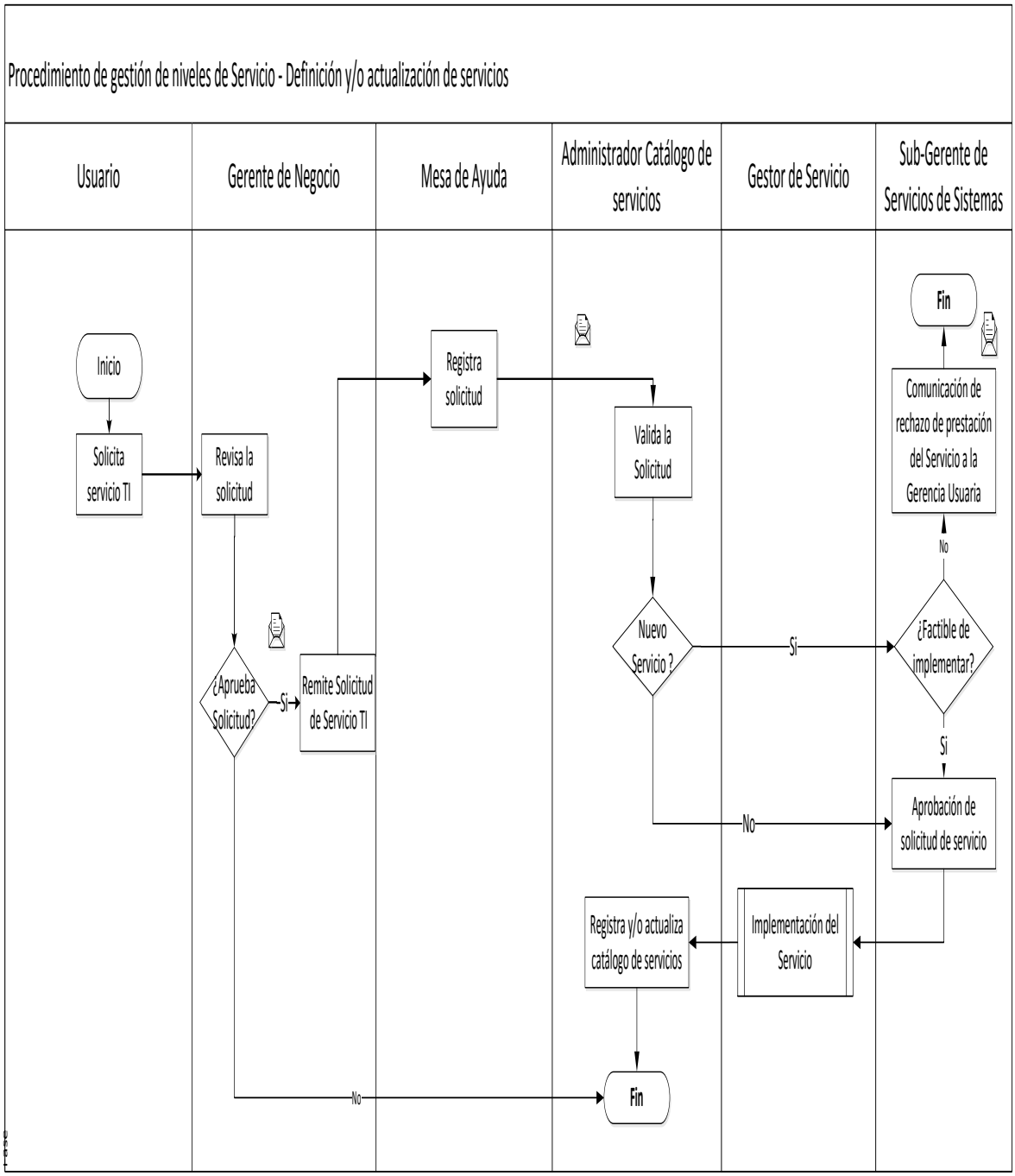


Fig. O2 Actualización de Niveles de Servicio.
Fuente: Elaboración propia.

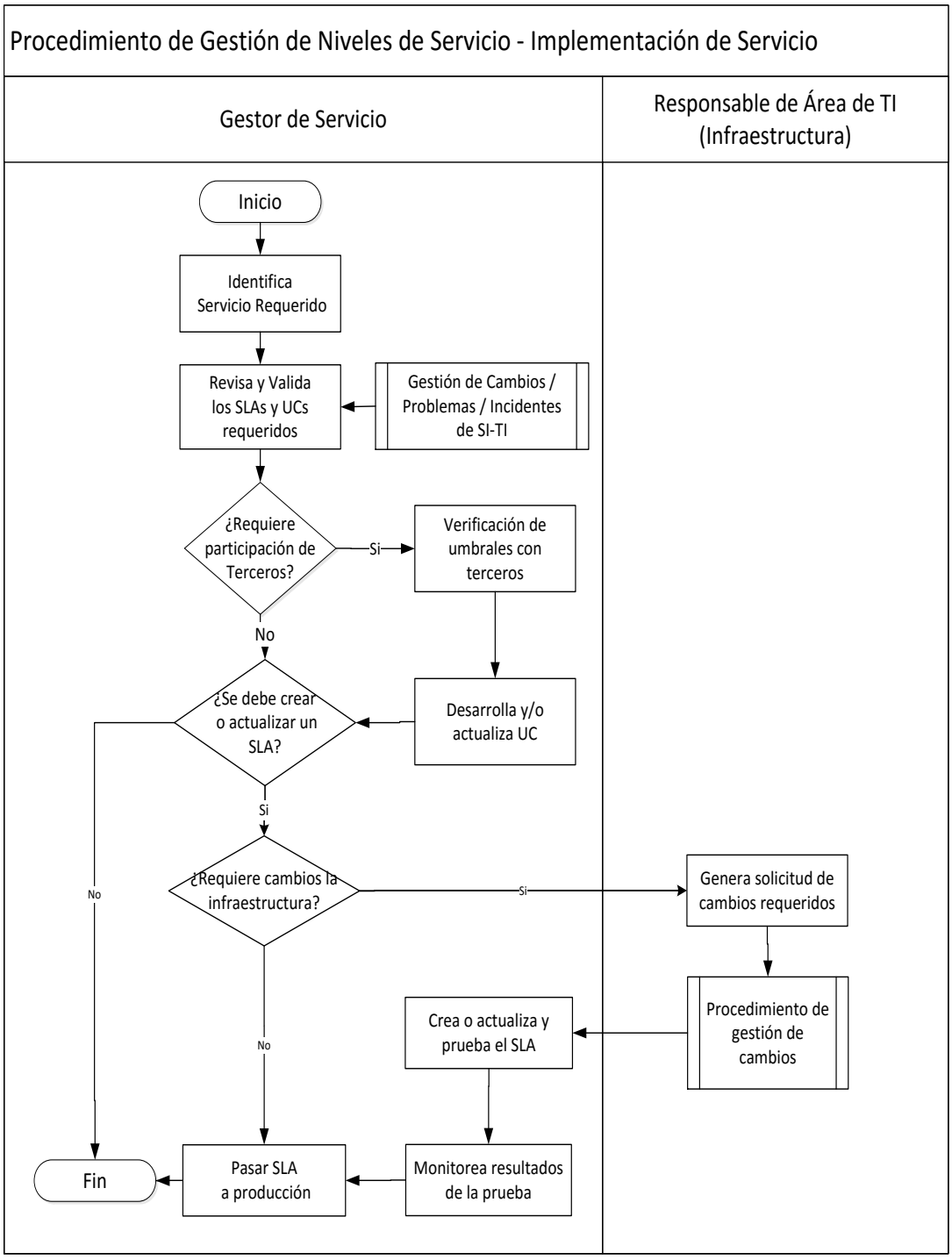


Fig. O3 Implementación de Servicio.
Fuente: Elaboración propia.

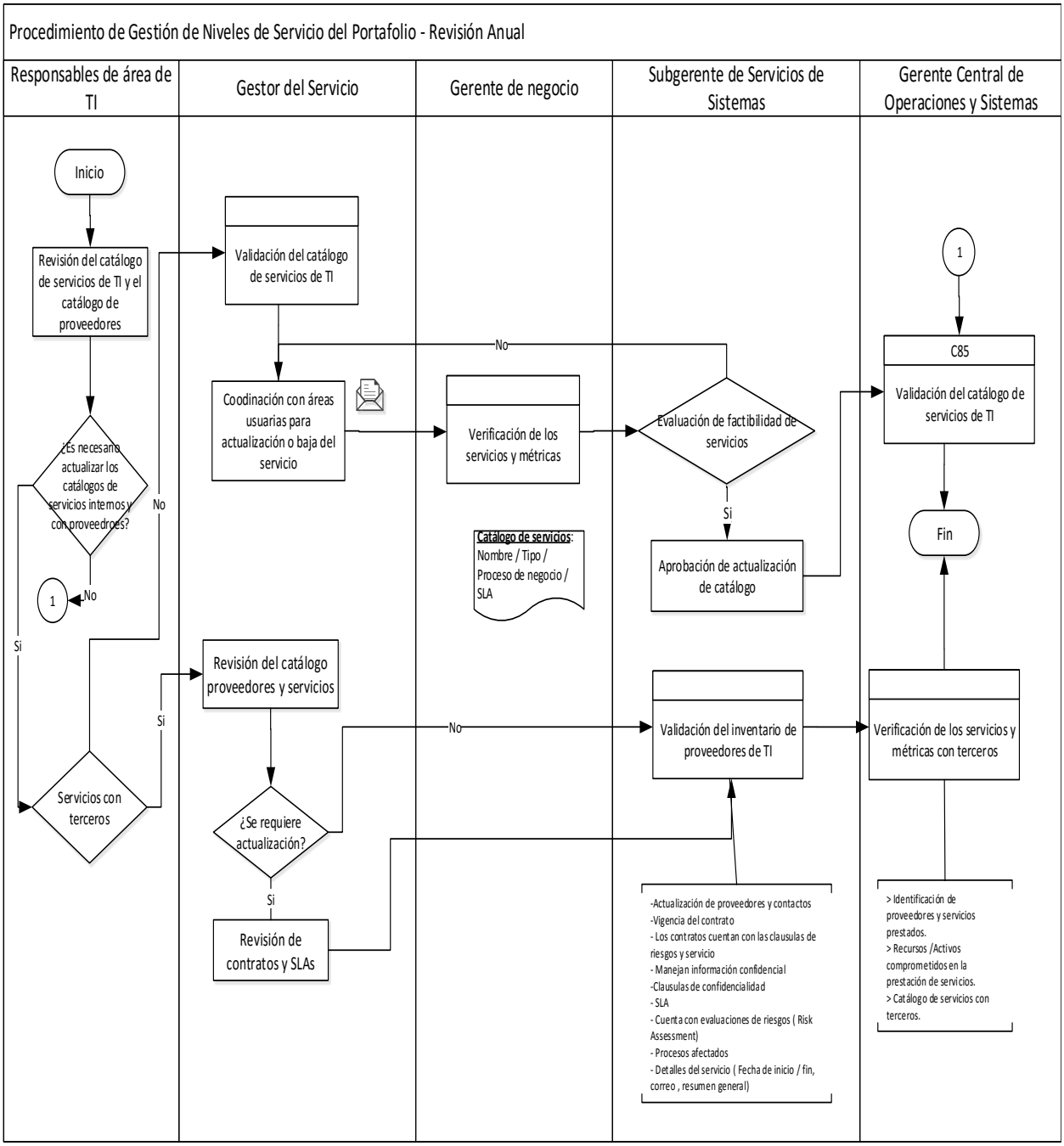


Fig. O4 Niveles de Servicio del Portafolio - Revisión Anual.
Fuente: Elaboración propia.

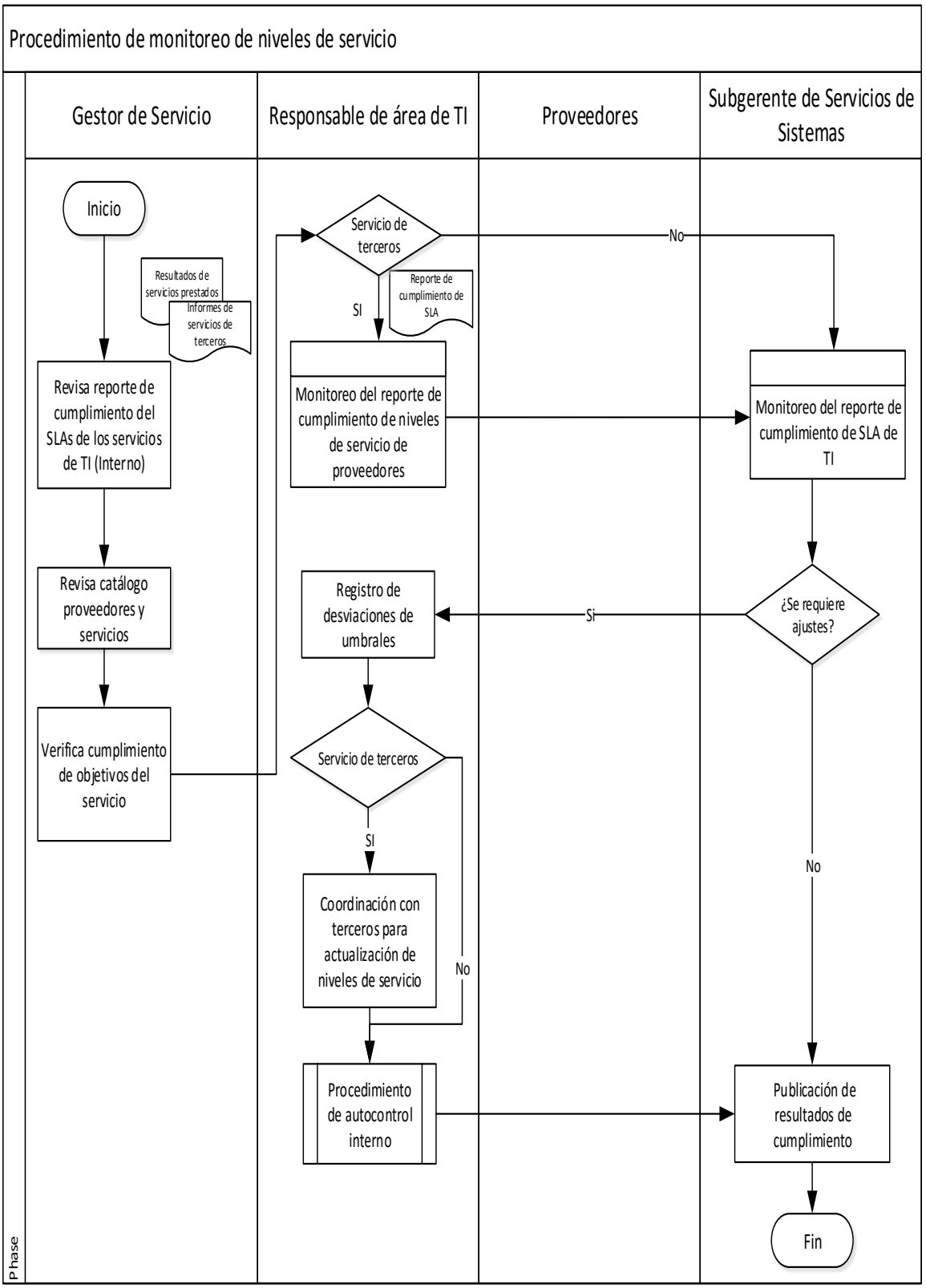


Fig. O5 Monitoreo de Niveles de Servicio.
Fuente: Elaboración propia.

Anexo P Gestión de Mesa de Ayuda.

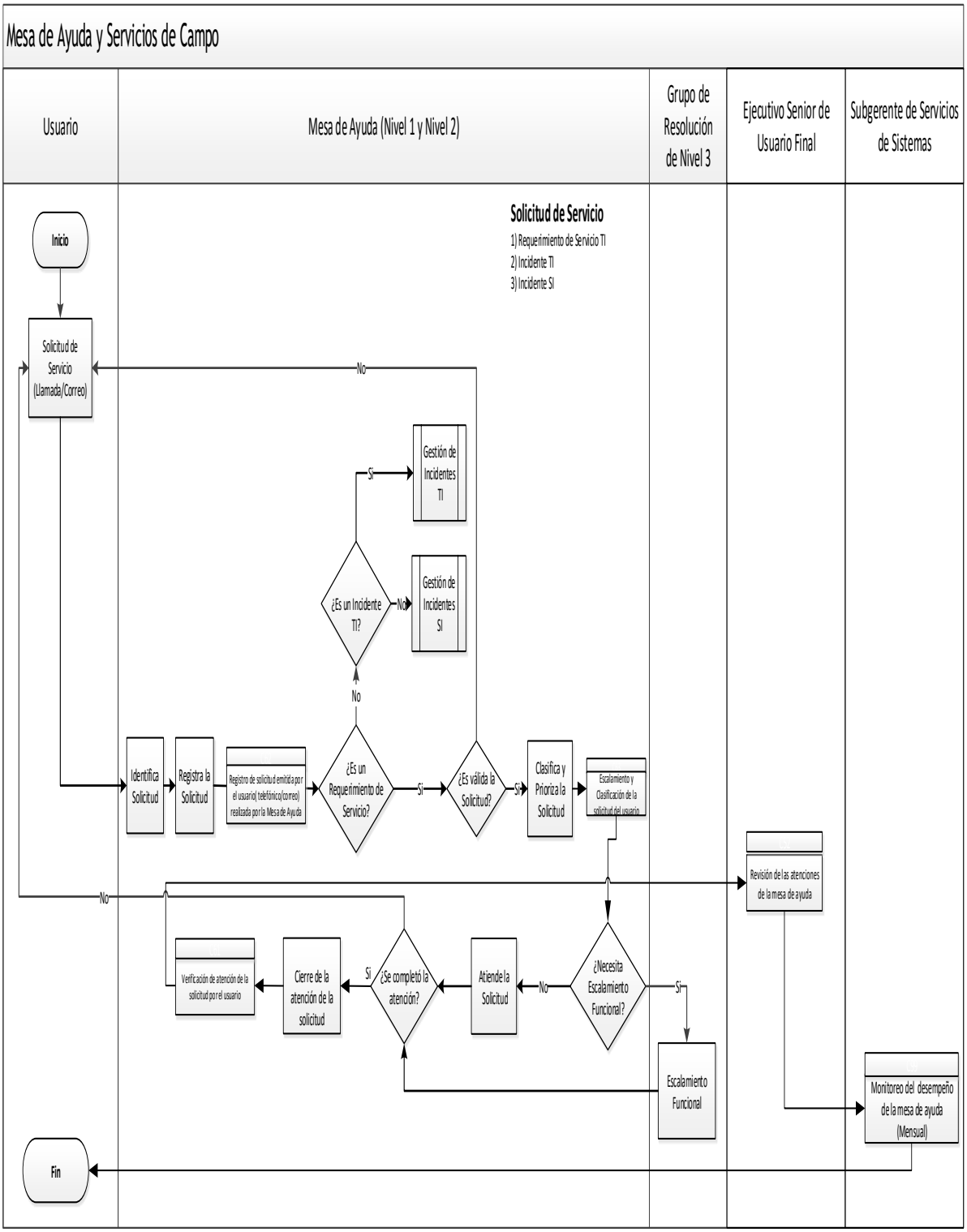


Fig. P1 Mesa de Ayuda y Servicio de Campo.
Fuente: Elaboración propia.

Anexo Q Gestión del Catálogo de Servicios.

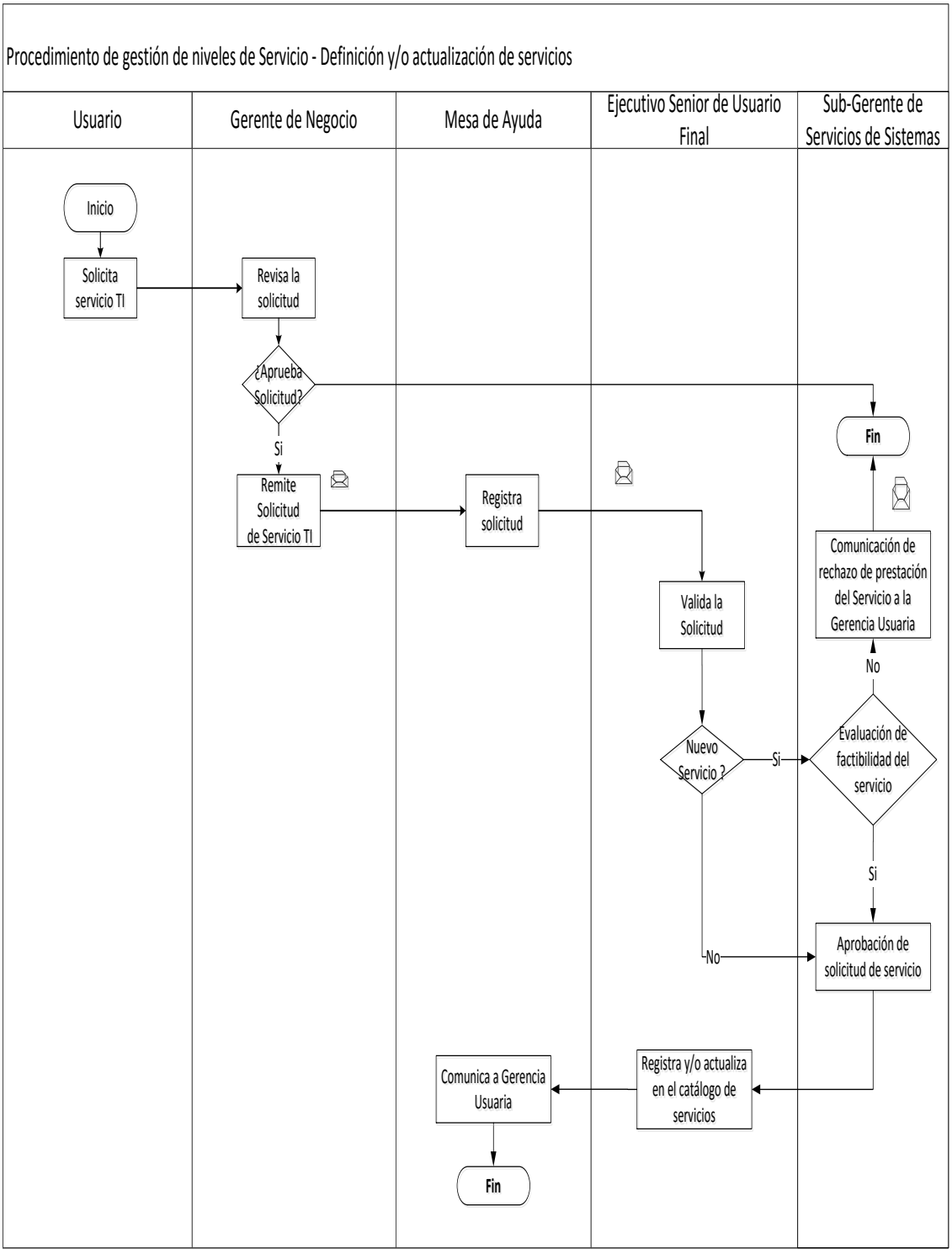


Fig. Q1 Gestión de Niveles de Servicio - Definición - Actualización de Servicios.
Fuente: Elaboración propia.

Anexo R Gestión de la Configuración de Servidores Críticos.

La gestión de configuración garantiza que se restablezca la operación normal de servicio lo antes posible y se minimice el impacto al negocio.

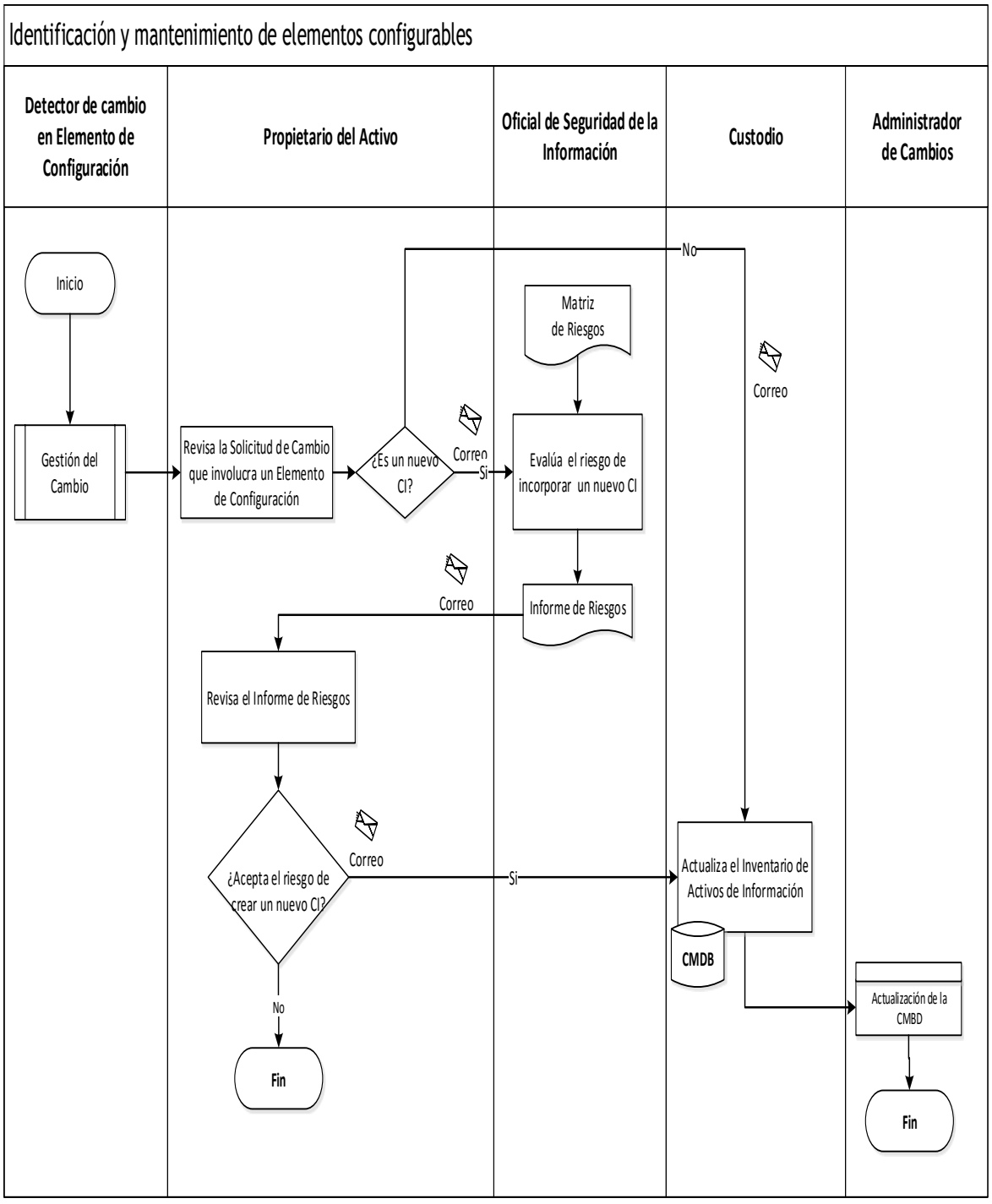


Fig. R1 Identificación y Mantenimiento de Elementos Configurables.
Fuente: Elaboración propia.

Anexo S Definir un Plan Estratégico

Descripción del Procedimiento de Elaboración y Seguimiento del Plan Estratégico de TI

Metodología de Elaboración del PETI

Para la elaboración del Plan Estratégico de Tecnologías de Información se debe seguir 4 fases, ésta metodología está concebida en concordancia con el modelo conceptual a través de la integración de la visión estratégica de negocios y organización y la visión estratégica de TI.

FASE 1 - Situación Actual:

Todo el proceso comienza con un análisis de la situación actual, que produce un modelo funcional imperante en la empresa. En este paso se evalúa el entendimiento de la estrategia de negocios, la eficiencia de los procesos operativos y la aceptación de TI en la organización.

FASE 2 - Modelo de Negocios y Organización:

Relacionada con la creación de un modelo de la organización, inicia con un análisis del entorno y establecimiento de las estrategias de negocio (el proceso de planeación se basa en una transformación de dichas estrategias). Continua con el diseño en detalle de los modelos operativos, que van a producir en parte los requerimientos de TI para mejorar la eficiencia y la productividad de la empresa (esta aproximación es soportada por una re-ingeniería de procesos o una automatización incremental, que se concentran en identificar deficiencias operativas, con el propósito de rediseñarlas, modificarlas y automatizarlas).

Posteriormente se construye la estructura de la organización, que especifica puestos, perfiles, habilidades, etc. Necesarios para administrar la empresa.

La fase termina con la construcción de una arquitectura de información, que identifica las necesidades globales de información de la empresa. El modelo es descrito con términos y conceptos de negocio y organización independientemente del soporte computacional.

FASE 3 - Modelo de TI:

Trata del desarrollo de un modelo de TI. Como parte inicial tiene como objetivo la transformación de las estrategias de negocio en una estrategia de TI. Sigue con la construcción de la arquitectura de sistemas, que establece un marco para la especificación de aplicaciones y la integración de la información.

Luego se definen los elementos clave y las características de la arquitectura tecnológica (Hardware y Comunicaciones), que establecerá la plataforma en que los sistemas van a funcionar. Continúa el diseño en detalle de los modelos operativos de TI, que describen el funcionamiento del área de informática. Finaliza con la definición sobre la estructura de la organización de TI, necesaria para administrar los requerimientos informáticos.

FASE 4 - Modelo de Planeación:

Se concentra en la elaboración de un modelo de planeación. Primero se establecen las prioridades para la implantación de TI. Y los procesos operativos, luego se define un plan de implantación, que determina el desarrollo de los proyectos de negocios, organización y TI. Continua con un estudio de la recuperación de la inversión, a través de una análisis de costo / beneficio. Todo el proceso finaliza con un estudio de administración del riesgo, que se encarga de reconocer la existencia de amenazas que puedan poner en peligro el éxito del PETI.

Metodología de Elaboración del PETI

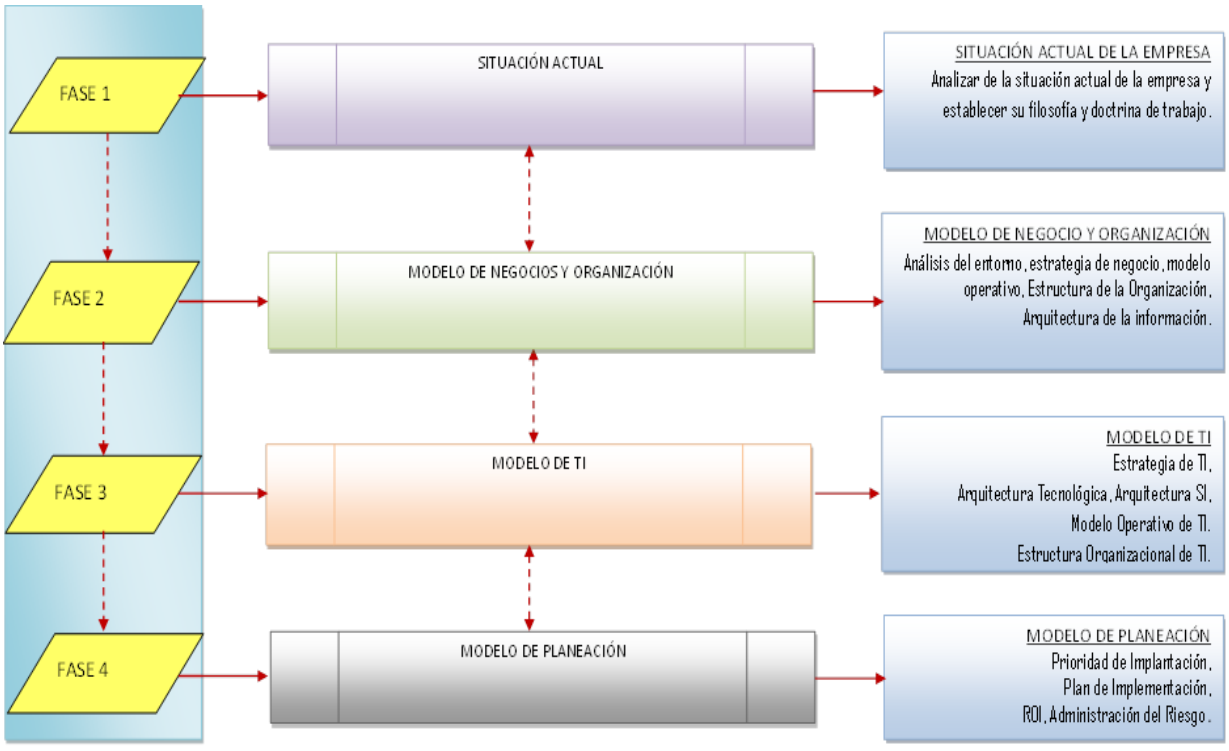


Fig. S1 Metodología de Elaboración del PETI.
Fuente: Elaboración propia

La información que debe proporcionar el Comité de Gerencia para la elaboración del PETI es la siguiente:

- FODA del Negocio
- Misión
- Visión
- Objetivos
- Organización
- Modelo Operativo del Negocio
- Estrategias Locales y Regionales

El Plan de Implementación del PETI contiene las iniciativas y proyectos de infraestructura y servicios de TI en el que se detallan los recursos tecnológicos y no tecnológicos que se necesiten para llevarlos a cabo, así como la fecha de ejecución planificada.

Para la elaboración del Plan de Implementación del PETI se utilizan las estrategias de TI alineadas a los objetivos del negocio y el Plan de Capacidades.

El PETI contiene lo siguiente:

- Análisis de Situación Actual de TI.
- FODA de TI.
- Modelo de TI.
- Matriz de Objetivos Estratégicos de la Empresa Vs. Objetivos de TI.
- Objetivo del Área de Sistemas y Portafolio de Proyectos.
- Plan de Capacidades.
- Matriz de procesos de negocio vs. Sistemas.
- Plan de Inversiones / Gastos de Tecnología.
- Plan Estratégico de Seguridad Tecnologías de Información (PESTI).
- Listado de Proveedores.
- Plan de Implementación de TI.

El Modelo de TI debe contener lo siguiente:

- Misión de TI.
- Visión de TI.
- Estructura Organizacional de TI.
- Infraestructura de TI y comunicaciones alineada al negocio.
- Funciones y responsabilidades, roles y procesos de TI.
- Objetivos de TI.
- Estrategias de TI.

En el plan de Capacidad de TI, se documenta la contribución de tecnología a los objetivos de negocio tomando como referencia el histórico de mediciones de monitoreo de infraestructura tales como:

- Monitoreo de red / internet / red interna: Medición de Performance - Consumo de ancho de banda.
- Monitoreo de Sistema Operativo: Disponibilidad de servicios por consumo de memoria, disco, procesador.

- Monitoreo de Base de datos (Performance / Espacio en disco)
- Monitoreo de disponibilidad de infraestructura (Servidores / Sistema Operativo / Base de datos).

Esta información es registrada por los administradores de las diferentes plataformas a través de los dispositivos de monitoreo de infraestructura.

Mostrando:

- La estabilidad histórica de los Servicios.
- Complejidad de prestación de servicios.
- Costos asociados (mantenimiento).
- Fortalezas / Debilidades de los servicios prestados a nivel de soporte de sistemas.

En base a lo cual el Consultor de Sistemas realiza las estimaciones de capacidad a nivel de infraestructura para el periodo en planificación.

Desarrollo del Diagrama de Flujo Elaboración y Seguimiento del Plan Estratégico de TI

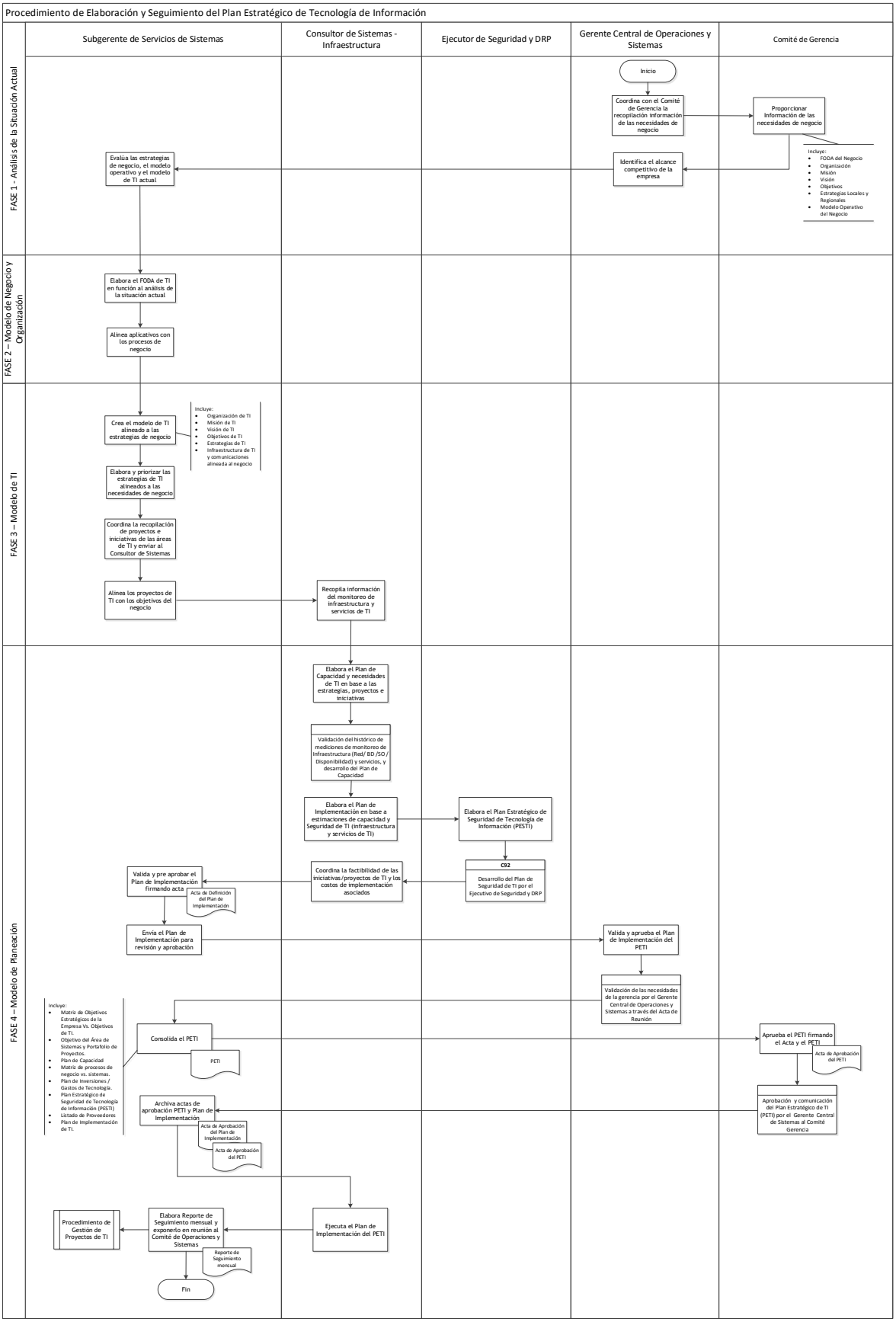


Fig. S2 Elaboración y Seguimiento del Plan Estratégico de Tecnología de Información. Fuente: Elaboración propia.