

**UNIVERSIDAD HISPANOAMERICANA**

**INGENIERÍA INFORMÁTICA**

**TESINA PARA OPTAR EL GRADO DE  
BACHILLERATO EN LA CARRERA DE  
INGENIERÍA INFORMÁTICA**

**TÍTULO DEL PROYECTO DE GRADUACIÓN  
PROPUESTA DE MEJORA DEL SISTEMA DE  
ASEGURAMIENTO Y DIAGNÓSTICO DE  
INFRAESTRUCTURA EN LA EMPRESA AMDOCS  
COSTA RICA CONFORME A LAS MEJORES  
PRÁCTICAS EN EL MERCADO EN SAN JOSÉ,  
DURANTE EL SEGUNDO CUATRIMESTRE DEL  
2017**

**Sustentante  
Johan Quesada Romero**

**TUTOR  
Roberto Santamaría Sandoval**

**SEGUNDO CUATRIMESTRE, 2017**

## Índice de contenido

DECLARACIÓN JURADA .....	xiii
CARTA DE APROBACIÓN DEL TUTOR .....	xiv
CARTA DE APROBACIÓN DEL LECTOR .....	xv
CARTA DE APROBACIÓN DEL FILÓLOGO .....	xvi
DEDICATORIA.....	xvii
AGRADECIMIENTO.....	xviii
ABREVIATURAS.....	xix
RESUMEN .....	xxi
CAPÍTULO I: PROBLEMA DEL PROYECTO .....	23
1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO.....	24
1.1.1 Marco de Referencia Empresarial y Contextual .....	24
1.1.2 Justificación del Proyecto .....	26
1.2 Definición del Problema .....	29
1.2.1 La idea del problema .....	29
1.2.2 La pregunta del problema:.....	31
1.3 Objetivo General y Objetivos Específicos .....	31
1.3.1 Objetivo General.....	31
1.3.2 Objetivos específicos:.....	31
1.4 Alcances y Limitaciones.....	32

1.4.1	Alcances .....	32
1.4.2	Limitaciones.....	33
CAPÍTULO II: MARCO TEÓRICO .....		18
2.1	Conceptos Básicos de Infraestructura de TI .....	19
2.1.1	Elementos de Infraestructura de TI .....	19
2.1.2	Elementos lógicos en Infraestructura de TI .....	21
2.2	Modelos de Gestión de Infraestructura y Mejores Prácticas .....	25
2.2.1	ITIL v3.....	25
2.2.2	COBIT 5.....	40
2.2.3	ISO 20000-1 .....	43
CAPÍTULO III: MARCO METODOLÓGICO .....		47
3.1	Tipo y enfoque de la investigación .....	48
3.1.1	Tipo de Investigación.....	48
3.1.2	Enfoque .....	48
3.2	Fuentes y sujetos de Información .....	49
3.2.1	Fuentes de Información .....	49
3.2.2	Sujetos de Información .....	51
3.2.3	Técnicas y Herramientas .....	51
3.3	Variables de Investigación .....	52
3.4	Diseño de la Investigación .....	54

CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL.....	55
4.1 Diagnóstico Operativo .....	56
4.1.1 Modelos de trabajo actuales.....	56
4.1.2 Licenciamiento de Infraestructura.....	57
4.1.3 Proceso de monitoreo.....	57
4.1.4 Ítems de monitoreo.....	59
4.1.5 Proceso de elaboración y manejo de alertas de monitoreo .....	59
4.2 Diagnóstico Técnico.....	61
4.2.1 Infraestructura .....	61
4.3 Brechas entre el sistema actual y el propuesto.....	69
CAPÍTULO V: PROPUESTA DE PROYECTO.....	71
5.1 Diseño del sistema de aseguramiento y diagnóstico de infraestructura.....	72
5.1.1 Requerimientos del sistema .....	72
5.1.2 Modelado de casos de uso.....	83
5.1.3 Arquitectura del Sistema.....	102
5.1.4 Estructuración de la base de datos .....	104
5.2 Prototipo del sistema.....	107
5.2.1 Definición de módulos .....	107
5.2.2 Funcionalidades del sistema .....	132
5.3 Plan Piloto del sistema.....	137

5.3.1	Plan de implementación .....	137
5.3.2	Pruebas del sistema .....	138
5.3.3	Resultados de las pruebas del sistema .....	151
CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES.....		163
1.	CONCLUSIONES .....	164
2.	RECOMENDACIONES.....	166
Bibliografía .....		168
APÉNDICES Y ANEXOS .....		171
1.	APÉNDICE 1: CUESTIONARIO .....	172

## Índice de tablas

Tabla 1. Servidores nivel físico .....	30
Tabla 2. Servidores nivel virtual. ....	30
Tabla 3. Actividades, Métodos y Técnicas de Nivel de Servicio.....	27
Tabla 4. Fuentes Primarias .....	50
Tabla 5. Sujetos de Información.....	51
Tabla 6. Variables de Investigación .....	53
Tabla 7. Licenciamiento de Productos. ....	57
Tabla 8. Ítems de monitoreo.....	59
Tabla 9. Distribución de servidores virtuales.....	66
Tabla 10. Comparación entre sistema actual y propuesta. ....	70
Tabla 11. Requerimiento de Administración de alertas.....	73
Tabla 12. Requerimiento de Configuración de monitoreo .....	74
Tabla 13. Requerimiento de Configuración de servidores.....	75
Tabla 14. Requerimiento de Configuración de aplicación. ....	76
Tabla 15. Requerimiento de Configuración de errores.....	77
Tabla 16. Requerimiento de Configuración de tareas. ....	78
Tabla 17. Requerimiento de Configuración de procesos.....	79
Tabla 18. Requerimiento de Configuración de acceso de red.....	80
Tabla 19. Requerimiento de Configuración de almacenamiento.....	81
Tabla 20. Requerimiento de Configuración de estado de monitoreo. ....	82
Tabla 21. Caso de uso de administrar alertas.....	84
Tabla 22. Caso de uso de configurar monitoreo - tipo de aplicación.....	85

Tabla 23. Caso de uso de configurar monitoreo - tipo de alerta.....	86
Tabla 24. Caso de uso de configurar monitoreo - grupo de correo electrónico.....	87
Tabla 25. Caso de uso de configurar monitoreo - correos electrónicos. ....	88
Tabla 26. Caso de uso de configurar monitoreo - grupo de SMS. ....	89
Tabla 27. Caso de uso de configurar monitoreo - números de SMS.....	90
Tabla 28. Caso de uso de configurar servidores.....	91
Tabla 29. Caso de uso de configurar aplicaciones.....	92
Tabla 30. Caso de uso de configurar errores - directorio y archivo.....	93
Tabla 31. Caso de uso de configurar errores - código de error.....	94
Tabla 32. Caso de uso de configurar errores - parámetro de descarte.....	95
Tabla 33. Caso de uso de configurar tareas - tipo de tarea. ....	96
Tabla 34. Caso de uso de configurar tareas. ....	97
Tabla 35. Caso de uso de configurar procesos.....	98
Tabla 36. Caso de uso de configurar acceso de red.....	99
Tabla 37. Caso de uso de configurar almacenamiento. ....	100
Tabla 38. Caso de uso de configurar estado del monitoreo.....	101
Tabla 39. Requisitos técnicos. ....	103
Tabla 40. Descripción de tablas en base de datos.....	105
Tabla 41. Sub módulo de configuración de aplicación de servicio.....	107
Tabla 42. Parámetros de configuración para monitoreo del servidor de aplicación. ...	112
Tabla 43. Configuración de Errores.....	115
Tabla 44. Parámetros del módulo de configuración de procesos.....	123
Tabla 45. Parámetros de configuración de alertas.....	127

Tabla 46. Estructura de archivos del sistema.....	133
Tabla 47. Caso de Prueba para agregar tipo de aplicación. ....	139
Tabla 48. Caso de Prueba para agregar tipo de alerta. ....	139
Tabla 49. Caso de Prueba para agregar grupo de correo.....	140
Tabla 50. Caso de Prueba para agregar correo electrónico.....	140
Tabla 51. Caso de Prueba para agregar grupo de SMS. ....	141
Tabla 52. Caso de Prueba para agregar número de SMS. ....	141
Tabla 53. Caso de Prueba para agregar servidor. ....	142
Tabla 54. Caso de Prueba para agregar aplicaciones. ....	143
Tabla 55. Caso de Prueba para agregar archivos y directorios de errores. ....	144
Tabla 56. Caso de Prueba para agregar código de error.....	144
Tabla 57. Caso de Prueba para agregar parámetro de descarte. ....	145
Tabla 58. Caso de Prueba para agregar tipo de tarea. ....	146
Tabla 59. Caso de Prueba para agregar una tarea.....	146
Tabla 60. Caso de Prueba para agregar un proceso. ....	147
Tabla 61. Caso de Prueba para agregar dispositivo de red .....	147
Tabla 62. Caso de Prueba para agregar ruta de almacenamiento.....	148
Tabla 63. Caso de Prueba para agregar estado de monitoreo. ....	148
Tabla 64. Caso de Prueba para agregar alerta. ....	149
Tabla 65. Caso de Prueba para eliminar entrada en el sistema.....	150
Tabla 66. Caso de Prueba para validación de espacios. ....	150
Tabla 67. Caso de Prueba para envío notificaciones .....	151

## Índice de figuras

Figura 1. Organigrama de la institución.....	25
Figura 2. Fases y Procesos basado en ITIL Versión 3.....	26
Figura 3. Aspectos de la Gestión de la Disponibilidad .....	29
Figura 4. Ejemplo de modelo lógico de configuración.....	33
Figura 5. El proceso de gestión de eventos. ....	35
Figura 6. Diagrama del proceso de Gestión de Incidencias. ....	37
Figura 7. Proceso de Gestión de Problemas.....	39
Figura 8. Principios de COBIT 5.....	40
Figura 9. Catalizadores Corporativos COBIT 5 .....	41
Figura 10. Categorías de los Catalizadores COBIT 5 .....	42
Figura 11. Gestión de Servicios .....	44
Figura 12. Diseño del proyecto de graduación .....	54
Figura 13. Proceso del sistema de aseguramiento y diagnóstico .....	58
Figura 14. Elaboración de una alerta en el sistema actual.....	60
Figura 15. Diseño de módulos de la plataforma del servicio de aprovisionamiento. ....	63
Figura 16. Diseño de módulos la plataforma de servicios de inventario.....	64
Figura 17. Diagrama de Infraestructura Física .....	65
Figura 18. Diagrama de Infraestructura Virtual de Aprovisionamiento. ....	67
Figura 19. Diagrama de Infraestructura Virtual de Inventario.....	68
Figura 20. Casos de uso de la propuesta del sistema.....	83
Figura 21. Arquitectura del Sistema. ....	103
Figura 22. Modelado de Base de datos.....	106

Figura 23. Su módulo de configuración del sistema de monitoreo.....	108
Figura 24. Sub módulo de configuración de tipo de alerta. ....	108
Figura 25. Sub módulo de configuración de correo electrónico. ....	109
Figura 26. Sub módulo de configuración de lista de correo. ....	110
Figura 27. Sub módulo de configuración de grupo SMS.....	110
Figura 28. Sub módulo de configuración de lista de SMS.....	111
Figura 29. Módulo de configuración de servidor de aplicación.....	112
Figura 30. Sub módulo para visualizar eventos en servidores de aplicación. ....	113
Figura 31. Módulo de configuración de aplicación empresarial.....	114
Figura 32. Sub módulo para visualizar eventos en aplicaciones empresariales. ....	114
Figura 33. Módulo de configuración de errores.....	115
Figura 34. Sub módulo de configuración de archivo y directorio de errores.....	116
Figura 35. Sub módulo de configuración para descartar errores. ....	117
Figura 36. Sub módulo para visualizar errores encontrados.....	118
Figura 37. Sub módulo de configuración de tipo de tarea.....	119
Figura 38. Sub módulo de configuración de la tarea.....	120
Figura 39. Sub módulo para visualizar los eventos de las tareas. ....	121
Figura 40. Módulo de configuración de acceso a la red.....	122
Figura 41. Sub módulo para visualizar los eventos de acceso en la red.....	122
Figura 42. Módulo de configuración de procesos.....	123
Figura 43. Sub módulo para visualizar los eventos de los procesos.....	124
Figura 44. Módulo de configuración de almacenamiento.....	125
Figura 45. Sub módulo para visualizar eventos de almacenamiento. ....	126

Figura 46. Módulo de configuración de alertas. ....	128
Figura 47. Módulo para configurar el estado de las alertas.....	129
Figura 48. Sub módulo para configurar estado de las alertas.....	130
Figura 49. Módulo de pantalla principal e incidentes en la última hora. ....	131
Figura 50. Enlace de acceso a servidores. ....	133
Figura 51. Funcionamiento del sistema a través de la interfaz web. ....	135
Figura 52. Ejecución del sistema. ....	136
Figura 53. Resultado caso de prueba CP1. ....	151
Figura 54. Resultado caso de prueba CP2. ....	152
Figura 55. Resultado caso de prueba CP3. ....	152
Figura 56. Resultado caso de prueba CP4. ....	153
Figura 57. Resultado caso de prueba CP5. ....	153
Figura 58. Resultado caso de prueba CP6. ....	153
Figura 59. Resultado caso de prueba CP7. ....	154
Figura 60. Resultado caso de prueba CP7. ....	155
Figura 61. Resultado caso de prueba CP9. ....	155
Figura 62. Resultado caso de prueba CP10. ....	156
Figura 63. Resultado caso de prueba CP11. ....	156
Figura 64. Resultado caso de prueba CP12. ....	157
Figura 65. Resultado caso de prueba CP13. ....	157
Figura 66. Resultado caso de prueba CP14. ....	157
Figura 67. Resultado caso de prueba CP15. ....	158
Figura 68. Resultado caso de prueba CP16. ....	158


Figura 69. Resultado caso de prueba CP17. ....	159
Figura 70. Resultado caso de prueba CP18. ....	159
Figura 71. Resultado caso de prueba CP19. ....	160
Figura 72. Resultado caso de prueba CP20 validación de lista. ....	160
Figura 73. Resultado caso de prueba CP20 validación de espacio. ....	161
Figura 74. Resultado caso de prueba CP21 alerta por correo electrónico.....	161
Figura 75. Resultado caso de prueba CP21 alerta por SMS.....	162

# DECLARACIÓN JURADA

## DECLARACIÓN JURADA

Yo Johan Steven Quesada Romero, mayor de edad, portador de la cédula de identidad número 1 1323 0870 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de bachiller, juro solemnemente que mi trabajo de investigación titulado: Propuesta de mejora del sistema de aseguramiento y diagnóstico de Infraestructura en la empresa Andaca Costa Rica conforme a las mejores prácticas en el mercado en San José durante el segundo cuatrimestre del 2017, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; artículo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 6 días del mes de Noviembre del año dos mil diecisiete.



Firma del estudiante

Cédula: 1 1323 0870

# CARTA DE APROBACIÓN DEL TUTOR

## CARTA DEL TUTOR

San José, 3 de noviembre de 2017

**Ing. Yenory Rojas Hernández**  
**Bachillerato Ingeniería Informática**  
**Universidad Hispanoamericana**

Estimado señor:

El estudiante Johan Steven Quesada Romero, cédula de identidad número 1-1323-0870, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado PROPUESTA DE MEJORA DEL SISTEMA DE ASEGURAMIENTO Y DIAGNÓSTICO DE INFRAESTRUCTURA EN LA EMPRESA AMDOCS COSTA RICA CONFORME A LAS MEJORES PRÁCTICAS EN EL MERCADO EN SAN JOSÉ, DURANTE EL SEGUNDO CUATRIMESTRE DEL 2017, el cual ha elaborado para optar por el grado académico de Bachillerato.


En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	9
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20
c)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	28
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	19
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	19
	TOTAL		95

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,



**José Roberto Santamaría Sandoval**  
**Cédula identidad N 1-1178-0664**  
**Carné Colegio Profesional N IE-15830.**

# CARTA DE APROBACIÓN DEL LECTOR

## CARTA DE LECTOR

San José, 7 de Diciembre del 2017

**Ing. Yenory Rojas Hernández PhD.**  
**Ingeniería en Informática**  
**Universidad Hispanoamericana**

Estimada señora

El estudiante Johan Quesada Romero, cédula de identidad 1-1323-0870, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "PROPUESTA DE MEJORA DEL SISTEMA DE ASEGURAMIENTO Y DIAGNÓSTICO DE INFRAESTRUCTURA EN LA EMPRESA AMDOCS COSTA RICA CONFORME A LAS MEJORES PRÁCTICAS EN EL MERCADO EN SAN JOSÉ, DURANTE EL SEGUNDO CUATRIMESTRE DEL 2017", el cual ha elaborado para obtener su grado de Bachillerato en Ingeniería Informática.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.



---

Lic. Pedro I. Leiva Chinchilla.  
1-1394-0453

# CARTA DE APROBACIÓN DEL FILÓLOGO

San Rafael de Heredia, 07 de diciembre de 2017

Señores

Universidad Hispanamericana

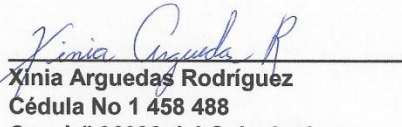
Estimados señores:

En mi calidad de filóloga, hago constar que he revisado la Tesina elaborada por el estudiante Johan Quesada Romero, para optar por el grado académico de Bachillerato en Ingeniería Informática, bajo el título:

**“PROPUESTA DE MEJORA DEL SISTEMA DE ASEGURAMIENTO Y DIAGNÓSTICO DE INFRAESTRUCTURA EN LA EMPRESA AMDOCS COSTA RICA CONFORME A LAS MEJORES PRÁCTICAS EN EL MERCADO EN SAN JOSÉ, DURANTE EL SEGUNDO CUATRIMESTRE DEL 2017”.**

La revisión se hizo en la parte morfosintáctica, forma, estilo, redacción, puntuación y ortografía; por lo cual este trabajo está listo en tales aspectos para ser presentado ante la Universidad.

Atentamente,

  
Xinia Arguedas Rodríguez  
Cédula No 1 458 488  
Carné # 06032 del Colegio de  
Licenciados y Profesores en Letras,  
Filosofía, Ciencias y Artes

Xinia Arguedas Rodríguez  
Filóloga  
Teléfono 22 37 61 66  
San Rafael de Heredia

## **DEDICATORIA**

### **A mi madre Julia.**

Por haberme brindado su apoyo incondicional en todo momento, sus consejos, valores que me han permitido ser una persona de bien.

### **A mi padre Miguel**

Por su gran ejemplo de perseverancia y esfuerzo para siempre vencer los obstáculos por más difíciles que sean.

### **A mis familiares**

A mi hermano Héctor porque me ha mostrado los diferentes caminos a seguir en la vida; a mi hermana Elizabeth que siempre ha sido un gran ejemplo académico y a mi hermano David que me hace querer ser un buen ejemplo para él en el futuro.

## **AGRADECIMIENTO**

De primero darle gracias a Dios por la salud, la sabiduría y paciencia que me ha brindado para lograr este objetivo, a mi tutor Roberto Santamaría por guiarme en la elaboración de este proyecto, a mis compañeras Tamara Salazar y Tamara Cambronero por el mutuo apoyo durante todo este proceso, a la empresa Amdocs Costa Rica por darme la oportunidad de realizar el proyecto y finalmente a la Universidad Hispanoamericana por todo el aprendizaje otorgado en estos años de estudio.

## ABREVIATURAS

**AIX:** Sistema operativo UNIX propietario de IBM (Advanced Interactive Executive).

**ORACLE:** Compañía especializada en el desarrollo de soluciones de nube y locales.

**WebSphere:** Familia de productos de software privado de IBM, se refiere a uno de sus productos específicos: WebSphere Application Server (WAS).

**SHELL:** Intérprete de órdenes o intérprete de comandos es el programa informático que provee una interfaz de usuario para acceder a los servicios del sistema operativo.

**BSS:** Sistemas de soporte empresarial.

**OSS:** Sistemas de soporte operacional.

**COBIT:** Objetivos de Control para Información y Tecnologías Relacionadas (Control Objectives for Information and related Technology).

**ISACA:** Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association).

**TI:** Tecnología de la Información.

**HTLM:** Lenguaje de Marcado para Hipertextos (HyperText Markup Language).

**ITIL:** Biblioteca de Infraestructura de Tecnologías de Información.

**UNIX:** Sistema operativo, es decir, constituye una colección de programas que ejecutan otros programas en una computadora.

**BSD:** Berkeley Software Distribution, sistema operativo derivado de Unix que nace a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.

**OSF:** Open Software Foundation (OSF) organización fundada en 1988 para crear un estándar abierto para la implementación del sistema operativo Unix

**AT&T:** Compañía estadounidense de telecomunicaciones

**SLA:** Un Service Level Agreement (SLA) es un contrato que describe el nivel de servicio que un cliente espera de su proveedor

**ISO/IEC:** Estándar para la seguridad de la información (International Organization for Standardization).

**SSH:** Protocolo y programa que sirve para acceder servidores privados a través de una puerta trasera.

**SMS:** Servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos, conocidos como mensajes de texto (Short Message Service).

**Kernel:** Es un software que constituye una parte fundamental del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

## RESUMEN

El siguiente documento explicará brevemente la propuesta del proyecto de graduación para la escuela de Ingeniería Informática de la Universidad Hispanoamericana, donde se presentarán los detalles del proyecto denominado Propuesta de mejora del sistema de Aseguramiento y Diagnóstico de Infraestructura en la empresa Amdocs Costa Rica conforme a las mejores prácticas en el mercado en San José, durante el segundo cuatrimestre del 2017.

En la actualidad la empresa Amdocs se encarga de implementar procesos e interfaces a nivel de telecomunicaciones relacionado con aprovisionamiento e inventario de servicios para sus clientes. Lo anterior se refiere, al desarrollo de integraciones entre plataformas heterogéneas, tanto internas como externas a la organización.

Jan van Bon et al (2008, p.30) define que, “Los activos de infraestructura existen en la forma de niveles definidos por sus relaciones con otros activos a los que dan soporte”, Amdocs se compone de 30 servidores en AIX, entre los cuales el servicio se encuentra instalado con bases de datos ORACLE y WebSphere que es una plataforma modular basada en estándares abiertos soportados por la industria. Puede conectar sus activos ya existentes a WebSphere a través de interfaces confiables y perdurables; también puede seguir ampliando su entorno a medida que las necesidades aumentan (IBM developerWorks, s.f.). Siendo una infraestructura interna de la empresa para el soporte de los servicios.

Dicha plataforma ha crecido en el lapso de 6 años, por cuanto la cantidad de servicios brindados por la empresa, así como su portafolio y catálogo de clientes también ha aumentado. Para realizar el monitoreo de los equipos de infraestructura se realiza por medio de scripts los cuales han sido configurados en cada uno de los servidores donde se ofrece los servicios, estos se encuentran diseñados en UNIX SHELL.

La administración para llevar a cabo el monitoreo de la infraestructura se ha tornado muy compleja, ocasionando que cuando se desea realizar un cambio se efectúe en cada uno de los servidores sin tener un control adecuado, por lo cual se plantea la necesidad de desarrollar un proyecto enfocado al ordenamiento y gestión, así como diagnóstico de la infraestructura de la empresa Amdocs Costa Rica.

## **CAPÍTULO I: PROBLEMA DEL PROYECTO**

## 1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

### 1.1.1 Marco de Referencia Empresarial y Contextual

Nombre de la empresa: Amdocs.

Año de fundación: 1982

**Estrategia:**

**Misión:**

Actuar como un negocio responsable con un equipo talentoso, comprometido y diverso de empleados.

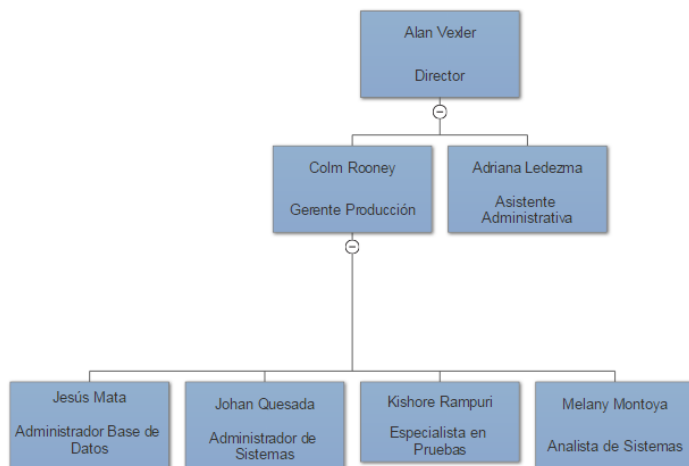
Servir como un proveedor líder de innovación sostenible en productos y servicios.

Realizar negocios con clientes globales y socios fundados en la confianza, la integridad y un compromiso mutuo con la responsabilidad ambiental y social en nuestras operaciones y comunidades.

**Visión:** Un mundo conectado de personas con poder y comunidades inclusivas, que permite el desarrollo sostenible.

## Organización: Amdocs Costa Rica

Figura 1. Organigrama de la institución



(Elaboración propia, 2017)

**Negocio al que se dedica:** Desarrollo de software y proveedor de servicios. Su solución de experiencia al cliente abarca sistemas de soporte empresarial (BSS), sistemas de soporte operacional (OSS), control de red y optimización para líneas múltiples empresariales, incluyendo redes inalámbricas, banda ancha, cable y servicios de satélite.

**Historia de la organización:** Amdocs OSS apoyará un proyecto de modernización a gran escala que permitirá un lanzamiento rápido y de bajo costo de nuevos servicios de telefonía móvil, residencial y comercial y de banda ancha.

Amdocs, proveedor líder de sistemas de experiencia del cliente, respaldará los requisitos de sistemas operativos de apoyo (OSS) de un proveedor de servicios telecomunicaciones en Costa Rica.

Esta empresa implementará los productos Amdocs CES - Cramer OSS 7.5 para soportar todas las necesidades de OSS, incluyendo planeación, inventario y

descubrimiento, provisión y activación, revisión de problemas, cumplimiento de servicio y análisis de impacto de servicio. El conjunto de productos OSS de Amdocs reemplazará a los sistemas heredados de la red existentes para sus redes inalámbricas y de cable. Este soporte generará servicios de manera más rápida y rentable.

### **1.1.2 Justificación del Proyecto**

Amdocs es un proveedor líder de software y servicios para las empresas de comunicaciones y medios más exitosos del mundo. A medida que los clientes se reinventan, esta compañía le ayuda a su transformación digital y de red a través de soluciones innovadoras, experiencia de entrega y operaciones inteligentes.

La empresa tiene una cultura de innovación. Están comprometidos a promover la innovación tanto sus clientes como en toda la organización.

Con base en lo que establece Amdocs (2017). “Es una organización de diseño que ofrece un amplio programa de innovación entre empresas que fomenta nuevas formas de pensar y conduce la excelencia para sus clientes, empleados y socios”.

El fortalecer la imagen de la empresa, brindando mejores niveles del servicio es imprescindible, de acuerdo con Jan van Bon et al. (2008, p.15) “un servicio es un medio para entregar valor a los clientes, facilitando los resultados que los clientes quieren conseguir sin asumir costes o riesgos específicos”, por lo tanto, una mejor administración permitirá reducir tiempos de ejecución en el aseguramiento del sistema y continuar con los niveles de calidad de servicio que se ha ido brindando.

La propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura de acuerdo a las mejores prácticas en el mercado, es una oportunidad de negocio, la

cual resulta de suma importancia ya que al contar con un sistema estandarizado se lograría reducir los tiempos de configuración y administración de los parámetros utilizados para los diferentes tipos de monitoreo con sus respectivas alertas, además de facilitar el uso a través de una interfaz simple sin la necesidad de tener capacidades específicas en programación pues estas se desarrollan a lo largo de los años. Según Jan van Bon et al (2008, p.28). “La extensión y profundización de experiencias adquiridas con distintos tipos de clientes, mercados, contratos y servicios facilita el desarrollo de capacidades propias”.

El optimizar el sistema de aseguramiento permitirá a la empresa ganar ventaja competitiva, de acuerdo a lo especificado en COBIT 5 ISACA (2012, p.57) “La valoración de la capacidad de la infraestructura actual de TI y de los recursos humanos de cara a soportar los requerimientos futuros del negocio y la consideración de futuros desarrollos tecnológicos que podría proporcionar una ventaja competitiva y/u optimizar costes”. Esto facilita que la empresa aproveche al máximo su información y los beneficios, de esta forma capitalizan las oportunidades de negocio.

El beneficio con la creación de un repositorio de eventos, que de acuerdo con Jan van Bon et al (2008, p.75) se puede definir como “Cualquier suceso detectable o discernible que tiene importancia para la gestión de la infraestructura de TI o para la entrega de un servicio de TI, así como para la evaluación del impacto que podría causar una desviación sobre los servicios”, permitirá a la empresa realizar un diagnóstico de los equipos que presentan problemas frecuentemente, de esta manera se podrá identificar la causa raíz que ocasiona el fallo para así solucionarlo y garantizar estabilidad en todos los equipos

que conforman la infraestructura. De acuerdo a Jan van Bon et al (2008) “la funcionalidad es lo que el cliente recibe, mientras que la garantía reside en cómo se proporciona”.

Por lo que finalmente, el implementar buenas prácticas en el modelo de aseguramiento para la infraestructura de Amdocs ayudará a la empresa a satisfacer los objetivos del negocio según lo estipula COBIT 5, donde la información necesita cumplir con los siguientes requerimientos de negocio:

- Efectividad: La información es eficaz si satisface las necesidades del consumidor de la información.
- Eficiencia: La información se obtiene y utiliza de manera fácil, es decir, consume pocos recursos, esfuerzo físico, esfuerzo cognitivo, tiempo y dinero.
- Confidencialidad: Esta corresponde a la meta de acceso restringido a la información de calidad.
- Integridad: La información está completa y libre de errores.
- Disponibilidad: Es una de las metas de la calidad de la información que están bajo los encabezados de accesibilidad y seguridad.
- Cumplimiento: Se refiere a cumplir con aquellas leyes, regulaciones y acuerdos contractuales, a los que están sujetos los procesos del negocio.
- Fiabilidad: La información es verdadera y creíble.
- Conformidad: La información debe ajustarse a unas especificaciones está cubierta por cualquiera de las metas de calidad de la información.

ISACA (2012, p.63)

## **1.2 Definición del Problema**

### **1.2.1 La idea del problema**

El proyecto se llevará a cabo en la empresa Amdocs Costa Rica con el fin de proponer la mejora del sistema de aseguramiento y diagnóstico de infraestructura, haciendo uso de mejores prácticas en el mercado, debido al nivel de complejidad que posee el sistema en este momento para crear, modificar y borrar los diferentes tipos de monitoreo y alertas pues el sistema no está estandarizado, no cuenta con una interfaz gráfica y tampoco con un registro histórico apropiado de incidentes reportados por los diferentes equipos.

Actualmente la empresa posee una amplia gama de equipo a nivel de infraestructura, debido a la cantidad de servidores físicos y virtuales requeridos para cada una de las aplicaciones del negocio y distribuidos en clúster para proporcionar un mejor rendimiento y mayor disponibilidad. Según Jan van Bon et al (2008, p.38) “La disponibilidad es el aspecto más importante en la prestación de servicios a un cliente, ya que garantiza que el cliente podrá hacer uso de los servicios en las condiciones acordadas”.

Los servicios que se brindan están relacionados con Aprovisionamiento e Inventario en telecomunicaciones y el total de servidores a nivel de producción se encuentran distribuidos de la siguiente manera:

Tabla 1. Servidores nivel físico

<b>CANTIDAD DE SERVIDORES A NIVEL FÍSICO</b>		
Aprovisionamiento	Inventario	Base de Datos
18	3	4

(Elaboración propia, 2017)

Tabla 2. Servidores nivel virtual

<b>CANTIDAD DE SERVIDORES VIRTUALES</b>	
Aprovisionamiento	Inventario
85	12

(Elaboración propia, 2017)

El sistema actual funciona correctamente y cumple las necesidades de aseguramiento, pero para ello se hace a través de scripts de sistema operativo configurados en SHELL, luego se crean tareas programas en cada uno de los servidores de la infraestructura para poder llevar a cabo el monitoreo.

El problema radica en el tiempo que se debe invertir a la hora de crear o modificar un parámetro en el sistema de aseguramiento, puesto que se realiza en cada uno de los servidores dentro de la infraestructura, tomando en cuenta que puede tomar entre 30 a 60 minutos por servidor, dependiendo de la complejidad del parámetro que se desea monitorear y se necesita de personal con conocimiento en SHELL para realizarlo y la empresa solo cuenta con un administrador de sistemas a nivel de infraestructura en este momento, ocasionando el riesgo de no cumplir con las métricas establecidas a nivel de contrato relacionado con la calidad de servicio, el cual indica que cada incidente debe ser atendido en un tiempo de 3 horas para todos los equipos y servicios.

El modelo de mantenimiento existente funciona únicamente de forma reactiva, careciendo de un registro de incidentes reiterativos en los equipos.

### **1.2.2 La pregunta del problema:**

¿De qué manera se puede proponer una mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica conforme a las mejores prácticas en el mercado, en San José durante el segundo cuatrimestre del 2017?

## **1.3 Objetivo General y Objetivos Específicos**

### **1.3.1 Objetivo General**

Proponer una mejora del sistema de aseguramiento y diagnóstico para la infraestructura en la empresa Amdocs Costa Rica conforme a las mejores prácticas en el mercado, mediante un modelo estandarizado para la reducción del nivel de complejidad del sistema actual.

### **1.3.2 Objetivos específicos:**

- Diagnosticar la situación actual del aseguramiento y diagnóstico de la infraestructura para la determinación de brechas conforme a las recomendaciones y tendencias del mercado.
- Establecer el diseño del sistema bajo un modelo estandarizado de gestión en cumplimiento de los requerimientos del negocio.

- Crear un prototipo del sistema conforme al diseño y requerimientos establecidos mediante la aplicación de metodologías de desarrollo del mercado.
- Implementar un plan piloto para el prototipo del sistema relacionado con la obtención de resultados, así como su comparación con respecto a la operación actual de la empresa.

## **1.4 Alcances y Limitaciones**

### **1.4.1 Alcances**

Para la elaboración de este proyecto se pretende proponer una mejora del sistema de aseguramiento y diagnóstico para permitir un monitoreo adecuado y de forma centralizada de la infraestructura.

- Se diagnosticará la situación actual del aseguramiento y diagnóstico de la infraestructura del ambiente de Producción de la empresa Amdocs Costa Rica, analizando el método actual que se dispone para realizar dicha tarea.
- Se establecerá un diseño bajo un modelo estandarizado que cumplan los requerimientos del negocio, el cual facilite la administración del sistema y garantice continuar con una buena calidad de servicio.
- Se creará un prototipo del sistema conforme al diseño y requerimientos que han sido establecidos mediante metodologías del mercado.
- Se implementará un plan piloto para el prototipo del sistema con el fin de obtener resultados y así poder compararlos con el sistema actual, y de esta forma aumentar el potencial del rendimiento, Jan van Bon et al (2008, p.43) especifica

que “se debe visualizar y definir de manera que todas las decisiones estén orientadas a la creación de valor para el cliente”.

#### **1.4.2 Limitaciones**

- La propuesta del sistema está sujeto a ser ejecutado exclusivamente sobre sistemas operativos en UNIX y Linux, con bases de datos ORACLE.
- El diseño del sistema será realizado exclusivamente bajo una plataforma Web en Java y HTML, además será ejecutado sobre un servidor Apache Tomcat.
- El proyecto es una propuesta de mejora para el actual sistema de aseguramiento y diagnóstico de la empresa, así que se procederá a crear un prototipo, pero será la empresa quien tome la decisión de llegar a implementarlo en un futuro.
- La auditoría es aplicada por la empresa, por lo cual no entra dentro de los temas de desarrollo.
- Las restricción de salida de información relacionada con estructura, código de programación y base de datos por parte de Amdocs Costa Rica, respecto a su naturaleza de la información que es estrictamente delicada en el área de seguridad debido al servicio que ofrece a sus clientes.

## **CAPÍTULO II: MARCO TEÓRICO**

## **2.1 Conceptos Básicos de Infraestructura de TI**

En este capítulo se definirán los conceptos de la estructura tecnológica y buenas prácticas basados en metodologías como ITIL V3, COBIT.

La búsqueda del procesamiento de la información de una manera rápida, eficaz y confiable ha hecho que las empresas inviertan más en tecnología y en mejorar su estrategia de servicios.

### **2.1.1 Elementos de Infraestructura de TI**

#### **2.1.1.1 Sistema Operativo UNIX**

Según establecen Luna, A y Sanz, P (2011, p.5) “UNIX es un sistema operativo tradicionalmente usado en minicomputadoras y workstations en la comunidad académica, así como en grandes instalaciones empresariales.”

Actualmente varias empresas han creado su propia versión de UNIX, las cuales fueron implementadas en el mercado, a continuación, se mostrará una lista de ellas basado en la descripción de Luna, A y Sanz, P (2011, p.6):

1. SCO. – Santa Cruz Operation: Calificado como excéntrico y su mayor aporte proviene de AT&T.
2. SunOS, Solaris: Desarrollados por Sun Microsystems el cual en la actualidad pertenece a Oracle.
3. HP-UX: Es el UNIX de Hewlett-Packard, cuenta con características propias y depende del hardware.

4. IRIX: Es la versión de Silicon Graphics. Sus versiones anteriores partieron de BSD, pero han ido evolucionando hacia los estándares de AT&T.
5. AIX: Es el UNIX de IBM. Se considera el único en su especie de forma administrativa, fue diseñado para ordenadores RISC-6000 que se extendieron hasta punto de haber vendido 500000 unidades en 1997.
6. DEC: Utiliza el estándar OSF/1, que está basado en un estándar Mach desarrollado en Carnegie-Mellon University. Se parece a BSD desde el punto administrativo y posee muchos rasgos de AT&T.

El sistema operativo en el que se encuentra la infraestructura de Amdocs Costa Rica es UNIX, por esta razón la propuesta de mejora para el sistema de aseguramiento y diagnóstico de la infraestructura será propuesto bajo esta plataforma.

#### **2.1.1.2 Bases de Datos**

De acuerdo con Hueso, L (2014, p.22). “Una base de datos es un conjunto de datos almacenados entre los que existen relaciones lógicas y ha sido diseñada para satisfacer los requerimientos de información de una empresa u organización”.

La base de datos será una parte vital para la propuesta del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica ya que ahí es donde se almacenarán todos los datos relacionados con la configuración, creación, modificación, eliminación e historial de alertas del sistema.

## **2.1.2 Elementos lógicos en Infraestructura de TI**

### **2.1.2.1 AIX**

Es una versión de UNIX que ha sido desarrollado por la compañía IBM.

El mundo empresarial actual debe basarse en una infraestructura que sea segura, altamente disponible y capaz de adaptarse rápidamente a las cambiantes necesidades del negocio. AIX proporciona estas funcionalidades y más con el rendimiento, fiabilidad y la seguridad que exigen sus datos de misión crítica.

IBM (s.f.)

La propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica será configurada bajo esta plataforma ya que toda la infraestructura cuenta con este sistema operativo.

### **2.1.2.2 Shell**

Los ordenadores utilizados por el sistema solo comprenden unos y ceros llamado sistema binario, el cual es difícil de utilizar para los humanos a la hora de desarrollar un programa.

Por lo que según indican Luna, A y Sanz, P (2011, p.11). “Para evitar el grave problema que sería la necesidad de dominar el lenguaje binario se creó un programa llamado Shell que se encarga de recoger diferentes comandos tecleados y pasarlos al Kernel de manera que este haga algo concreto”, es decir, la Shell es un intérprete de comandos entre el Kernel y la persona que lo utiliza.

El método que recurrirá para la recolección de datos por medio de forma estandarizada para la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica será por medio de scripts programados en Shell.

### **2.1.2.3 Lenguaje Java**

Un lenguaje de programación multiplataforma el cual es versátil para la implementación en diferentes sistemas operativos, según establece la empresa Oracle lo siguiente:

Java es un lenguaje de programación y una plataforma informática comercializada por primera vez en 1995 por Sun Microsystems. Hay muchas aplicaciones y sitios web que no funcionarán a menos que tenga Java instalado y cada día se crean más. Java es rápido, seguro y fiable. Desde portátiles hasta centros de datos, desde consolas para juegos hasta súper computadoras, desde teléfonos móviles hasta Internet, Java está en todas partes.

(Oracle Corporation, s.f).

La propuesta de mejora del sistema de aseguramiento y diagnóstico de Infraestructura en la empresa Amdocs Costa Rica utilizará Java Servlet, el cual son pequeños programas que se ejecutarán en el contexto de un navegador web, que de acuerdo con Ordax, J y Aranzazu, P. (2012, p.71).”Los Java Servlets eran un tipo de componente Java EE que se empaquetaba en un módulo web (WAR) y se desplegaba y ejecutaba en el contenedor web de un Servidor de Aplicaciones Java EE.”

#### **2.1.2.4 Lenguaje HTML**

Es un lenguaje de programación web, Terán, J. (2010, p.15) establece que “es el tercer componente sobre el cual se basa el servicio Web. Este lenguaje facilita mediante el uso de etiquetas, -marcas o tags-, la inclusión, en los documentos publicados, de texto, tablas, imágenes, audio, vídeo, enlaces a otros recursos”.

La propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica utilizará este lenguaje de programación para realizar la interacción con el usuario final, donde podrá realizar configuración a través de asistentes, además podrá visualizar las diferentes configuraciones e incidentes listados en tablas.

#### **2.1.2.5 Servidor Web Tomcat**

Tomcat es un software de código abierto para la implementación de tecnologías Java Servlet, JavaServer Pages, Java Expression Language y Java WebSocket, según establece Apache (s.f.). “El software de Apache Tomcat se desarrolla en un entorno abierto y participativo y pretende ser una colaboración de los mejores desarrolladores de todo el mundo”.

La propuesta de mejora del sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs Costa Rica utilizará el servidor Tomcat debido a que puede ser ejecutado múltiples sistemas operativos lo cual facilita su uso, además al ser un sistema de código abierto no recurre en costos de licencia y posee una amplia documentación relacionado al soporte técnico.

### **2.1.2.6 WebSphere Application Server**

La empresa líder mundial en servicios IBM establece que WebSphere es una plataforma que brinda seguridad y flexibilidad a la infraestructura según detalla lo siguiente:

IBM WebSphere Application Server proporciona un rango de entornos de ejecución Java EE 7 seguros y flexibles, disponibles en local o en cualquier cloud público, privado o híbrido. Tanto si su objetivo es reducir costes, como desbloquear nuevo valor de su inversión en aplicaciones o acelerar la comercialización, WebSphere tiene la opción adecuada para cada necesidad de negocio. (IBM, s.f.).

La empresa Amdocs utiliza WebSphere Application Server en su infraestructura para ejecutar las diferentes aplicaciones con las que cuenta dentro de su plataforma, por esta razón se debe desarrollar la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica para ser compatible con esta tecnología.

## **2.2 Modelos de Gestión de Infraestructura y Mejores Prácticas**

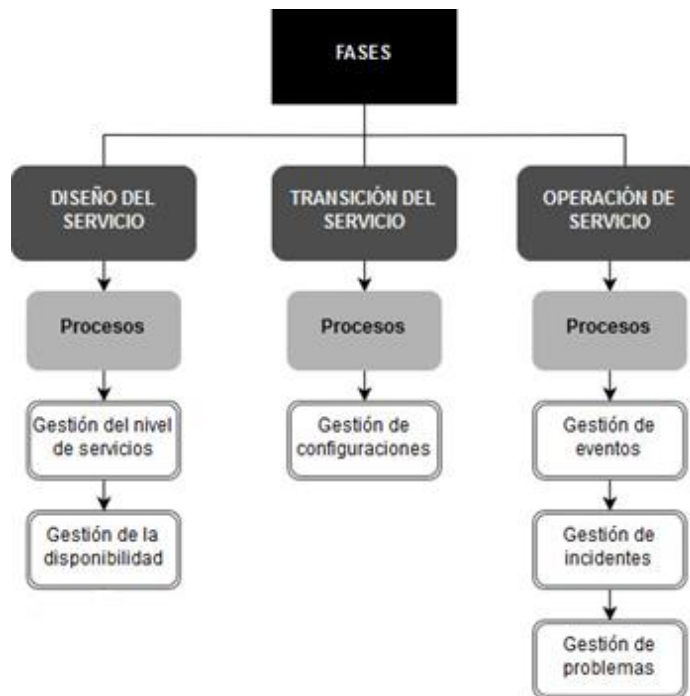
### **2.2.1 ITIL v3**

ITIL es un conjunto de buenas prácticas que ha sido implementado en varias empresas para el manejo adecuado de TI.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de la organización. Jan van Bon et al (2008, p.7).

La propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica será desarrollada basado en las siguientes fases de ITIL versión 3. En la figura 2 se mostrarán cada uno de los procesos involucrados en dichas fases.

Figura 2. Fases y Procesos basado en ITIL Versión 3



(Elaboración propia, 2017)

### 2.2.1.1 Fase de Diseño de Servicio

La implementación en el diseño de servicio establecido por ITIL v3 establece la forma en la cual se puede brindar un mejor manejo a los servicios del negocio y cuenta con tres tipos de Gestiones denominadas Gestión del nivel de servicios, Gestión de la disponibilidad y Gestión de la continuidad del servicio.

Para realizar la propuesta de mejora del sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs Costa Rica se necesitará estandarizar el manejo de los servicios que se brindan. Esta fase cuenta con los siguientes objetivos como parte de su metodología:

- Contribuir a los objetivos del negocio.

- Contribuir a ahorrar tiempo y dinero.
- Minimizar o prevenir riesgos.
- Contribuir a satisfacer las necesidades presentes y futuras del mercado.
- Evaluar y mejorar la eficacia y la eficiencia de los servicios de TI.
- Apoyar el desarrollo de políticas y estándares para servicios de TI.
- Contribuir a mejorar la calidad de los servicios de TI.

Jan van Bon et al. (2008, p.21).

### 2.2.1.2 Gestión del Nivel de Servicio

A continuación, en la tabla 3, se detallará cada una de las actividades, métodos y técnicas que han sido especificados en ITIL versión 3, que serán necesarias para realizar la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica con base en Jan van Bon et al (2008, p.71).

Tabla 3. Actividades, Métodos y Técnicas de Nivel de Servicio

<b>Monitorización del rendimiento con respecto al SLA</b>	Tiene que ser posible medir todo lo que esté incluido en el SLA, ya que de lo contrario podrían surgir disputas y posibles pérdidas de confianza.
<b>Aumento de satisfacción del cliente</b>	Se debería tener en cuenta la satisfacción del cliente el servicio entregado.
<b>Revisión y ajuste de acuerdos de apoyo</b>	El proveedor de servicios de TI depende de cierta medida de sus propios servicios técnicos internos. Por esta razón es preciso acuerdos subyacentes con departamentos internos.
<b>Revisión y mejora de servicios</b>	Se debe mantener consultas periódicas con el cliente con el fin de evaluar los servicios e identificar posibles en la provisión de servicios, centrándose siempre en las mejoras que puedan ser más beneficiosas para el negocio.

Fuente: Elaboración propia, 2017

### 2.2.1.3 Gestión de la Disponibilidad

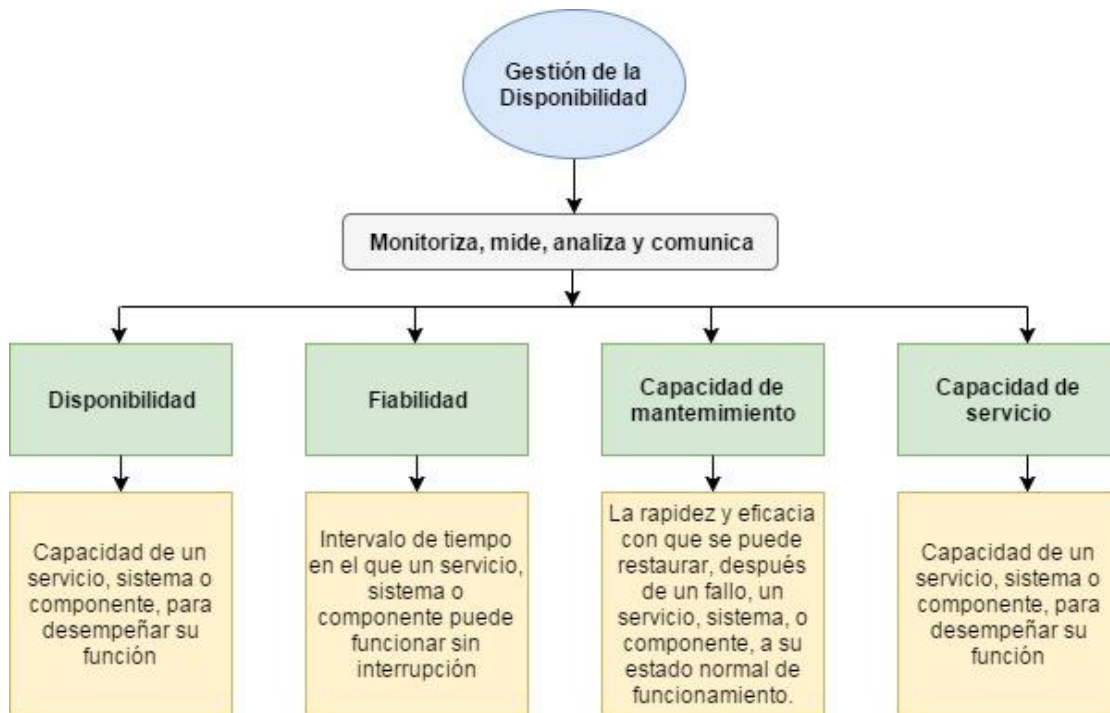
La Gestión de la Disponibilidad cubre en gran medida varios factores que incluyen, diseño, implementación, medición y disponibilidad de servicios de TI, lo siguiente son las principales actividades de este proceso se utilizarán para realizar la propuesta de mejora del sistema de aseguramiento y diagnóstico de Infraestructura en la empresa Amdocs Costa Rica:

- Determinar el impacto de los fallos de los componentes.
- Definir los objetivos particulares de disponibilidad, fiabilidad y capacidad de mantenimiento de los componentes de TI.
- Monitorizar y analizar componentes de TI.
- Establecer medidas e informes de disponibilidad, fiabilidad y capacidad de mantenimiento, que reflejen las perspectivas del usuario de negocio y de la organización de TI de soporte.

Jan van Bon et al (2008, p.84)

La finalidad de estas actividades es proporcionar una visión de disponibilidad en la infraestructura, en el cual se pueda garantizar el servicio que se le brinda al cliente, según indica Jan van Bon et al (2008, p.85) por medio de monitorización, medición, análisis y comunicación de cada uno de los siguientes aspectos en la figura 3.

Figura 3. Aspectos de la Gestión de la Disponibilidad



Fuente: Elaboración propia, 2017

#### **2.2.1.4 Fase de Transición del Servicio**

En esta fase se involucra la planificación y coordinación de procesos que se utilizarán en la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica, para llevar a cabo distintas tareas, ya sean labores de implementación, desarrollo o soporte, debe involucrar a todas las personas interesadas.

La transición del Servicio incluye la gestión y coordinación de los procesos, sistemas y funciones necesarios para la construcción, prueba y despliegue de una “versión” en producción, así como para la definición del servicio según las especificaciones del cliente y las partes interesadas. Jan van Bon et al (2008, p.33).

Esta fase produce un gran impacto a la operación del cliente, de acuerdo con Jan van Bon et al (2008, p.33). “Una Transición del Servicio es eficaz y eficiente si, dentro de las limitaciones, produce todo lo que requiere la empresa en términos de dinero y otros medios necesarios”.

#### **2.2.1.5 Gestión de la Configuración y Activos del Servicio**

La Gestión de la Configuración propone un modelo lógico de la infraestructura de TI donde relaciona los servicios con los diferentes componentes que son necesarios para proveer tales servicios.

Según Jan van Bon et al (2008, p.72). "El objetivo es definir componentes de servicio e infraestructura y mantener registros precisos de la configuración."

Lo que busca este proceso es garantizar que en la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura de la empresa Amdocs todos los componentes que son parte de un producto o servicio se encuentren identificados y que

además se mantengan actualizados, así como todos aquellos activos ajenos a TI que por alguna razón particular se vean afectados o sean requeridos para brindar el servicio.

De acuerdo con Jan van Bon et al (2008, p.72). "La Gestión de la Configuración y Activos del Servicio aumenta la visibilidad y el rendimiento del servicio, la versión o el entorno." Entre las mejoras se encuentra lo siguiente:

- Mejor previsión y planificación de cambios.
- Cambios y entregas que podrán ser valorados, planificados y provisionados satisfactoriamente.
- Incidencias y problemas que podrán ser resueltos dentro de los objetivos estipulados de nivel de servicio.
- Mejor adhesión a estándares, obligaciones legales y regulaciones.
- Capacidad para identificar los costes asociados a un servicio.

Jan van Bon et al (2008, p.73).

Los pasos a seguir para realizar la implementación serían los siguientes:

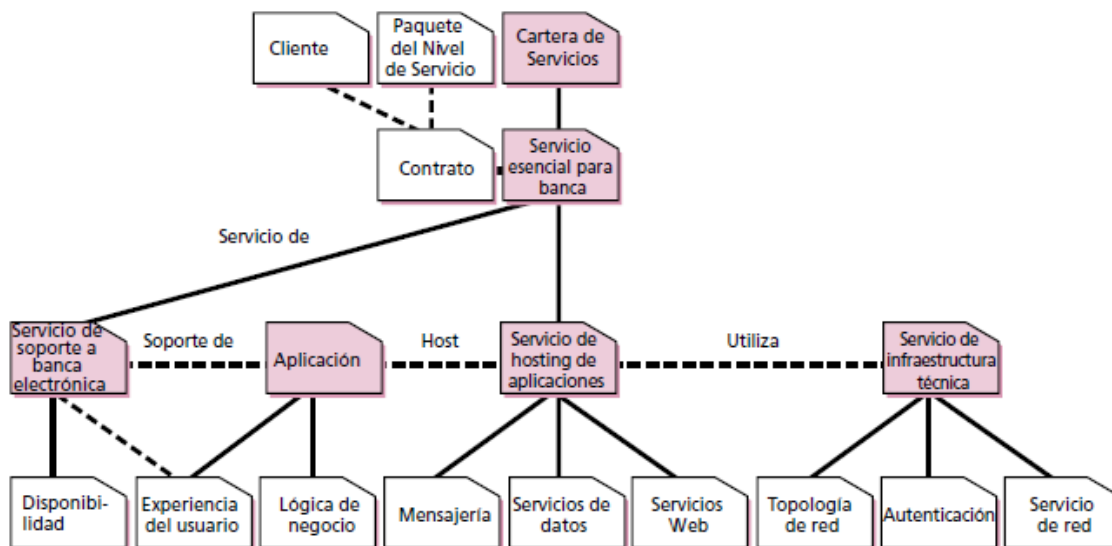
1. **Políticas:** Desarrollar y mantener políticas con las que se establezcan los objetivos, el alcance, los principios y los factores críticos de éxito respecto a lo que se quiere lograr con el proceso.
2. **Puntos de partida:** Los elementos para el desarrollo y control de activos, como:
  - a. Necesidad de garantizar los acuerdos contemplados en el SLA.
  - b. Especificaciones para servicios con alto grado de disponibilidad, fiabilidad y rentabilidad.

- c. Especificaciones para criterios de rendimiento.
  - d. Transición desde mantenimientos proactivo hasta control proactivo.
  - e. Obligación de contar con información adecuada de activos y configuración para los interesados.
3. **Conceptos básicos:** Establecer relaciones entre elementos de configuración permite crear un modelo lógico de los servicios, los activos y la infraestructura, como:
- a. Análisis de impacto para los cambios propuestos.
  - b. Investigación de la causa de incidencias y problemas.
  - c. Planificación y diseño de cambios, actualizaciones de software e innovación tecnológica.
  - d. Planificación de paquetes de versiones y despliegues.
  - e. Optimización en el uso de activos y en costes.

Jan van Bon et al (2008, p.73)

La figura 4 muestra la implementación del modelo lógico de configuración.

Figura 4. Ejemplo de modelo lógico de configuración



(Jan van Bon et al. 2008, p. 73)

### 2.2.1.6 Fase de la Operación del Servicio

Esta fase se halla orientada a la coordinación de actividades y procesos para entregar los servicios de una manera adecuada para la propuesta de mejora del sistema de aseguramiento y diagnóstico de la empresa Amdocs, se debe establecer un orden de prioridades para entrar en operación al soporte de un servicio de acuerdo al número de actividades y su impacto, entre otras.

La Operación del Servicio tiene como objetivos la coordinación y ejecución de las actividades y procesos necesarios para entregar y gestionar servicios para usuarios y clientes con el nivel especificado. La Operación del Servicio también tiene la responsabilidad de gestionar la tecnología necesaria para la prestación y el soporte de los servicios. Jan van Bon et al (2008, p.21).

### 2.2.1.7 Gestión de Eventos

Una de las medidas primordiales para realizar la propuesta de mejora del sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs, es proporcionar verificación, aseguramiento, control y seguimiento a la infraestructura por medio de notificación de eventos.

Para garantizar la eficacia de la Operación del Servicio, una organización debe ser consciente del estado de su infraestructura y poder detectar desviaciones respecto a la operación normal o prevista. Se requieren unos buenos sistemas de monitorización y control. Jan van Bon et al (2008, p.75).

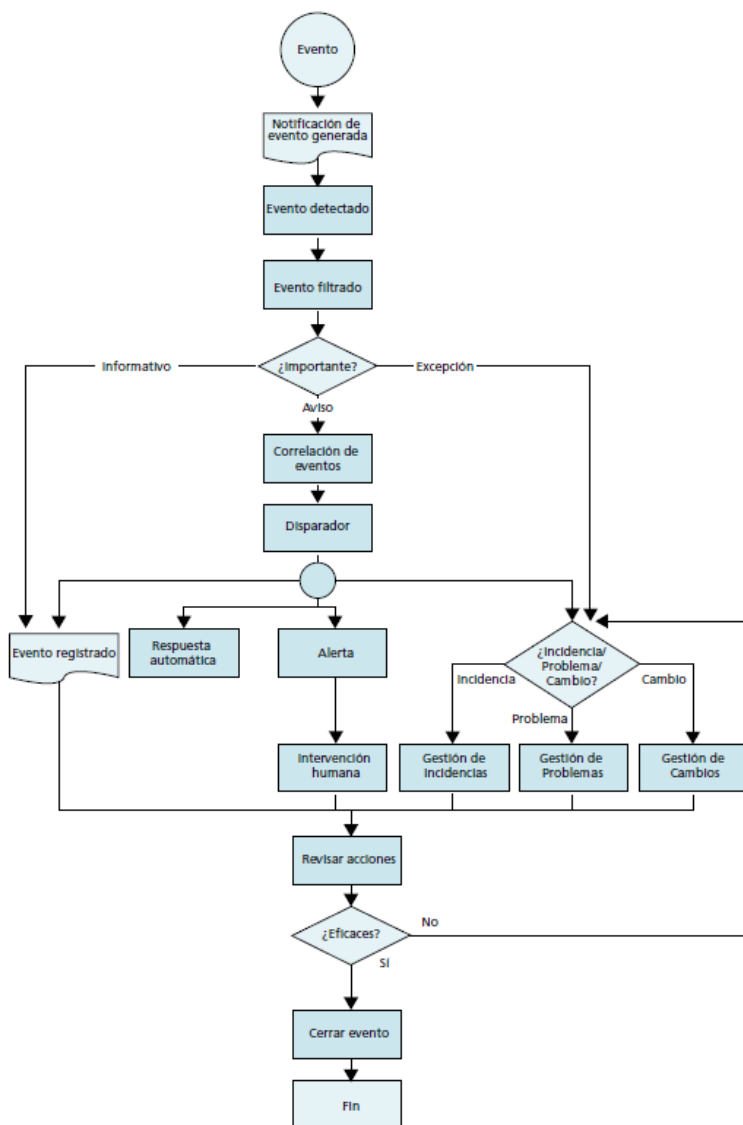
El beneficio que proporciona la Gestión de Eventos suele tener un valor añadido al negocio, como los siguientes:

- La gestión de eventos proporciona mecanismos para la rápida detección de incidencias.
- La gestión de eventos permite la monitorización por excepción de ciertos tipos de actividades automatizadas.
- Si está integrada en otros procesos de Gestión de Servicio, la gestión de eventos puede detectar excepciones o cambios de estado; hace que la persona o el equipo adecuado puede responder más rápidamente, lo que mejora el rendimiento del proceso.
- La gestión de eventos ofrece una base para operaciones automatizadas, lo que aumenta la eficacia y libera costosos recursos humanos para dedicarlos a trabajos más innovadores.

Jan van Bon et al (2008, p.75).

La figura 5 muestra el flujo del proceso de gestión de eventos.

Figura 5. El proceso de gestión de eventos



Fuente: Jan van Bon et al, 2008, p. 77

### 2.2.1.8 Gestión de Incidencias

Este proceso cubrirá en la propuesta de mejora del sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs todo lo relacionado con las incidencias reportadas, por ejemplo: fallos, preguntas o consultas que los usuarios

plantean o personal técnico o incluso detectadas de forma automática por medio de la herramienta de monitoreo.

La Gestión de incidencias causa efectos visibles para el negocio el cual hace más fácil demostrar su valor que en otros campos, se deben tomar en cuenta los siguientes aspectos:

- **Límites de tiempo:** Se debe definir límites de tiempo para todas las fases y emplearlos como objetivos acuerdos de nivel operativo.
- **Modelos de incidencias:** Es una manera de determinar los pasos necesarios para ejecutar correctamente un proceso de acuerdo a estándares.
- **Incidencias graves:** Requieren un procedimiento distinto, con plazos más cortos y mayor nivel de urgencia.

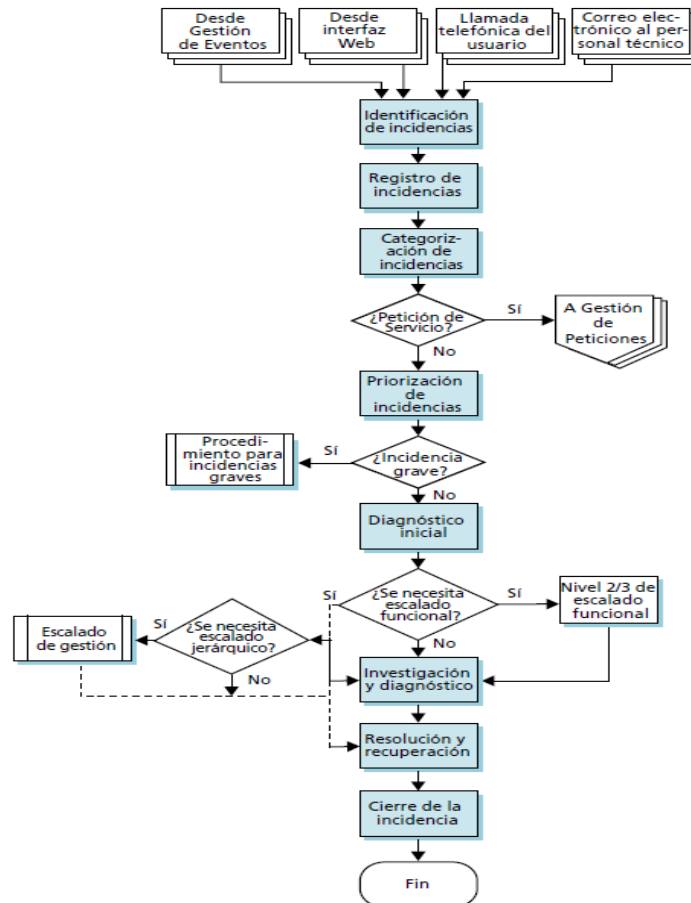
Jan van Bon et al (2008, p.83)

Por consiguiente, el proceso de Gestión de Incidencias deberá seguir los siguientes pasos:

1. Identificación.
2. Registro.
3. Clasificación.
4. Priorización.
5. Diagnóstico.
6. Escalado.
7. Investigación y diagnóstico.
8. Resolución y recuperación.
9. Cierre.

La figura 6 muestra el flujo del proceso de la Gestión de Incidencias.

Figura 6. Diagrama del proceso de Gestión de Incidencias



Fuente: Jan van Bon et al (2008, p. 83)

Para gestionar un control adecuado de las incidencias en la infraestructura se deberán realizar las siguientes tareas:

- Detectar incidencias lo más pronto posible.
- Convencer a todo el personal de que se deben registrar todas las incidencias.
- Disponibilidad de información sobre problemas y errores conocidos para que el personal de Gestión de Incidencias pueda aprender de incidentes anteriores.

- Integración en el Sistema de Gestión de la Configuración para determinar la relación entre elementos de configuración.
- Integración en el proceso de Gestión del Nivel de Servicio para que la Gestión de Incidencias pueda determinar el impacto y prioridades de los incidentes.

Jan van Bon et al (2008, p. 84).

#### **2.2.1.9 Gestión de Problemas**

Finalmente, para llevar a cabo la verificación, aseguramiento, control y seguimiento de la propuesta de mejora del sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs, será necesario realizar una adecuada Gestión de Problemas ya que este proceso se encarga de dar el correcto seguimiento a la raíz que provoca un incidente quien se ha estado generando de forma constante y así poder solventar el problema de manera definitiva.

Jan van Bon et al (2008, p.94) determina; "la gestión de problemas incluye todas las actividades necesarias para diagnosticar la causa subyacente de incidencias y encontrar una solución a esos problemas. También debe garantizar que la solución se implementa con los procedimientos de control correcto."

La Gestión de Problemas deberá llevar a cabo los siguientes métodos para así tener un mejor control del servicio:

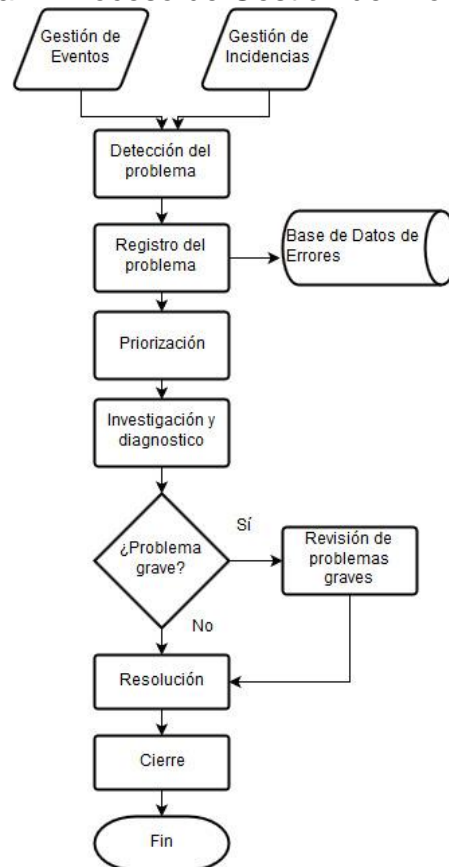
- Identificar una causa desconocida para una o más incidencias conlleva a realizar un registro del problema.
- El grupo técnico analiza la incidencia y descubre que existe un problema.

- Se realiza un seguimiento automático del error en la aplicación o la infraestructura, lo que hace que herramientas de alertas o eventos creen automáticamente un registro de incidencia que indica la necesidad de registrar un problema.
- El suministrador informa de un problema que hay que resolver.
- Se realiza un análisis de incidencias como parte de la gestión correctiva de problemas.

Jan van Bon et al (2008, p.97)

La figura 7 muestra el flujo de como el sistema cubrirá el proceso de Gestión de Problemas.

Figura 7. Proceso de Gestión de Problemas



Fuente: Elaboración propia, 2017

### 2.2.2 COBIT 5

COBIT 5 ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, este modelo beneficiará a la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica al mantener un equilibrio entre la realización del beneficios, el optimizar los niveles de riesgos y utilización de los recursos.

Según establece ISACA (2012, p.14). “COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales”, las cuales se muestran en la figura 8.

Figura 8. Principios de COBIT 5



Fuente: ISACA (2012, p.13)

La propuesta de aseguramiento y diagnóstica de infraestructura en la empresa Amdocs Costa Rica hará uso del principio 4 denominado Hacer posible un enfoque Holístico.

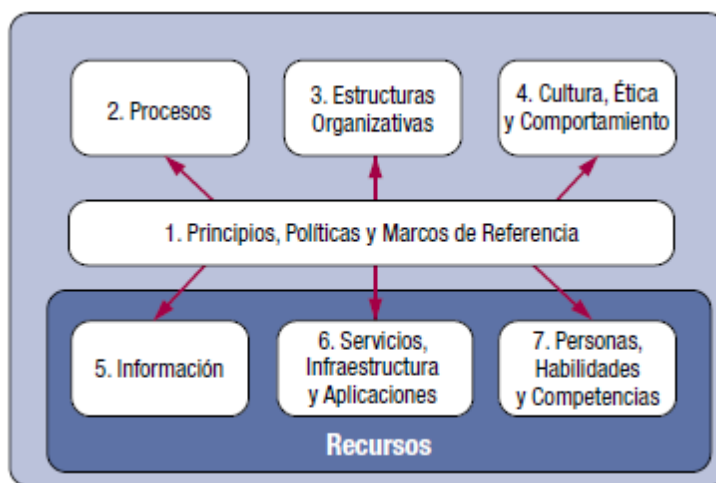
### 2.2.2.1 Principio 4: Hacer posible un enfoque Holístico

#### Catalizadores COBIT 5

Los catalizadores de acuerdo a ISACA (2012, p.27) “son factores que, individual y colectivamente, influyen sobre si algo funcionará, en este caso, el gobierno y la gestión de la empresa TI”. Los catalizadores son guiados por la cascada de metas, es decir, los objetivos de alto nivel relacionados con TI.

COBIT describe siete categorías de catalizadores los cuales se mostrarán en la figura 9.

Figura 9. Catalizadores Corporativos COBIT 5



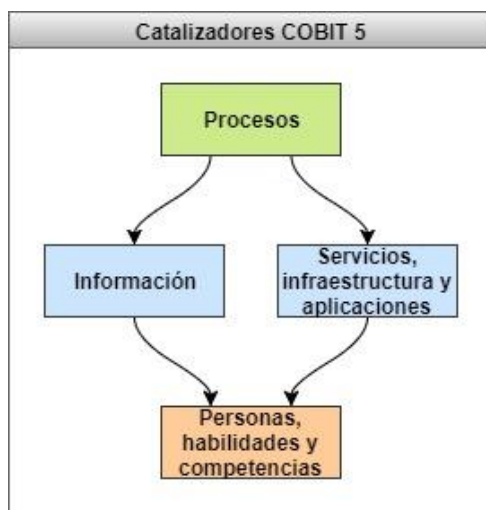
Fuente: ISACA (2012, p.27)

La propuesta de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica se basará en cuatro de las categorías especificadas en la figura anterior, que se definirán a continuación:

- **Procesos:** Describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- **Información:** impregna toda la organización e incluye toda la información producida y utilizada por la empresa.
- **Servicios, infraestructura y aplicaciones:** incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- **Personas, habilidades y competencias:** están relacionadas con la personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y acciones correctivas.

En la figura 10 se mostrarán las cuatro categorías relacionadas entre sí, para ser utilizadas en la propuesta de aseguramiento y diagnóstico de infraestructura.

Figura 10. Categorías de los Catalizadores COBIT 5



Fuente: Elaboración propia, 2017

### **2.2.3 ISO 20000-1**

De acuerdo con ISO/IEC 20000 (2005, p.3). “Esta norma promueve la adaptación de un enfoque de procesos integrados para proveer servicios de manera eficaz, con el fin de cumplir los requisitos del negocio y el cliente”.

La propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica se beneficiará al usar esta norma ya que coordinará la integración y aplicación de los procesos de gestión del servicio al proveer control continuo, incrementará la eficiencia y obtendrá oportunidades de mejora continua.

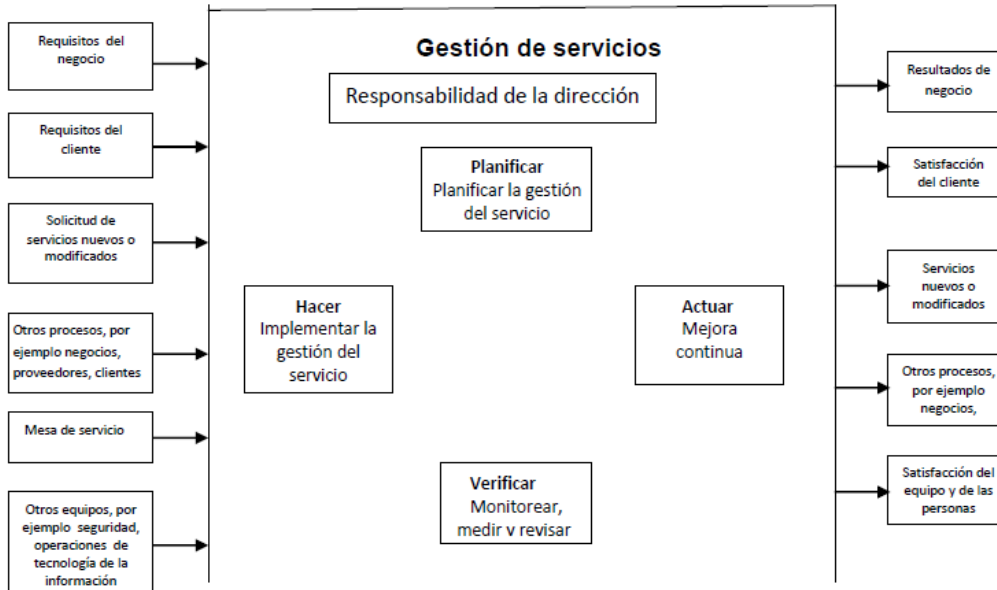
#### **2.2.3.1 Planificación e Implementación de la Gestión del Servicio**

La metodología “Planificar-Hacer-Verificar-Actuar” (PHVA) de acuerdo con ISO/IEC 20000 (2005, p.6) se puede aplicar a todos los procesos y se define de la siguiente manera:

- a) Planificar: establece los objetivos y los procesos necesarios para entregar resultados de acuerdo con los requisitos especificados por el cliente y las políticas de la organización.
- b) Hacer: Implementación de los procesos.
- c) Verificar: Monitorear y medir todos los procesos y servicios comparándolos con las políticas, objetivos y requisitos que han sido definidos y reportar los resultados.
- d) Actuar: Tomar acciones para mejora continua en el desempeño de los procesos.

En la figura 11 se muestra la Gestión de Servicios establecida por la norma.

Figura 11. Gestión de Servicios



Fuente: ISO/IEC 20000 (2005, p.6)

A continuación, se definirán los procesos y las relaciones que serán necesarias para realizar la propuesta del sistema de aseguramiento y diagnóstico de infraestructura, de acuerdo a los puntos establecidos en la figura 11.

### 2.2.3.1.1 Planificar la gestión del servicio (Planificar)

El proveedor del servicio de acuerdo con ISO/IEC 20000 (2005, p.8) debe implementar el plan de la gestión del servicio, incluyendo lo siguiente:

- Los objetivos y los requisitos que se deben alcanzar por parte de la gestión del servicio.
- Los procesos que se deben ejecutar.
- El enfoque que se debe tomar para identificar, evaluar y gestionar problemas y riesgos para el logro de los objetivos.
- Las herramientas que sean adecuadas para sustentar los procesos.

### **2.2.3.1.2 Implementar la gestión del servicio y prestar el servicio (Hacer)**

De acuerdo a lo que establece ISO/IEC 20000 (2005, p.8) se debe implementar el plan de la gestión del servicio, incluyendo los siguientes aspectos:

- Documentación, planes, procedimientos y definiciones de cada proceso o grupos de proceso.
- Identificación y gestión de los riesgos para el servicio.
- Coordinación de los procesos de la gestión del servicio.

### **2.2.3.1.3 Monitorear, Medir y Revisar (Verificar)**

El proveedor de servicio debe aplicar los métodos adecuados para monitorear según establece ISO/IEC 20000 (2005, p.9). “Estos métodos deben demostrar la capacidad de los procesos para alcanzar los resultados que fueron planificados anteriormente”, de acuerdo a lo siguiente:

- Satisfacer el plan de la gestión del servicio y los requisitos.
- Estar implementados y que se mantengan de manera eficaz.

#### **2.2.3.1.4 Mejora continua (Actuar)**

El objetivo será mejorar la eficacia y la eficiencia de la gestión y la manera en que se prestará el servicio. ISO/IEC 20000 (2005, p.10) define la mejora continua de la siguiente manera:

- a) Gestión de las mejoras: Se debe implementar un proceso para identificar, medir, informar y gestionar las actividades de mejor continua.
- b) Actividades
  - Recolectar y analizar datos para establecer la línea base.
  - Identificar, planificar e implementar mejoras.
  - Medir, informar y comunicar mejoras del servicio.
  - Garantizar que todas las acciones aprobadas se llevan a cabo y logran sus objetivos.

## **CAPÍTULO III: MARCO METODOLÓGICO**

### **3.1 Tipo y enfoque de la investigación**

El siguiente capítulo tiene como objetivo establecer el método para recopilar la información que ha sido seleccionado para la realización del proyecto.

#### **3.1.1 Tipo de Investigación**

El tipo de investigación que será utilizado para efectuar este proyecto es de naturaleza Aplicada ya que ayudará a mejorar el proceso de aseguramiento y diagnóstico de la infraestructura de la empresa, según establece Cegarra, J (2004, p.42). “La investigación Aplicada comprende el conjunto de actividades que tienen por finalidad el descubrir o aplicar conocimientos científicos nuevos, que puedan realizarse en productos y en procesos nuevos utilizables”.

#### **3.1.2 Enfoque**

La naturaleza de un proyecto o investigación se puede enfocar en dos aspectos, en cuantitativo o cualitativo, con base en lo que indica Sampieri, R (2010, p.4). “El enfoque cuantitativo usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías.” El otro aspecto que indica el autor es relacionado a nivel cualitativo en que menciona. “El enfoque cualitativo utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación.”

El enfoque que caracteriza esta investigación es cualitativo, de acuerdo a las características que esta posee, por el hecho de que la recolección de los datos no lleva una medición específica, la investigación es dirigida a través de áreas y los resultados desarrollados por eventos, conductas y observaciones.

## **3.2 Fuentes y sujetos de Información**

A continuación, se brindará una explicación de los sujetos y las fuentes de información que han sido utilizadas.

### **3.2.1 Fuentes de Información**

Según establece Sampieri (2010, p.53) las fuentes de información son el material en el cual se va a detectar, consultar y obtener la bibliografía para los propósitos del estudio. Se hará uso de diferentes fuentes primarias como secundarias las cuales se darán en detalle a continuación.

#### **3.2.1.1 Fuentes primarias**

De acuerdo con Sampieri; “Las fuentes primarias proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes.” (2010, p.53).

Las fuentes primarias que se utilizarán para llevar a cabo esta investigación son libros, criterio de expertos e informes técnicos.

- a) Libros: Aquellos relacionados con la implementación de ITIL Versión 3, COBIT 5, ISO 20000, Programación en Java y Shell, y Administración de WebSphere.
- b) Criterio de Expertos: Personas con más de 10 años de experiencia en Java, Oracle e Infraestructura.
- c) Informes técnicos: Diferentes sitios web en relación con la programación en Java, Shell, WebSphere y Oracle.

La tabla 4 muestra las fuentes primarias que serán consultadas para crear la propuesta.

Tabla 4. Fuentes Primarias

<b>Libros</b>	<b>Autor</b>	<b>Descripción</b>
Transición del Servicio Basada en ITIL V3	Jan van Bon	Estos libros ofrecen información detallada a quienes tienen la responsabilidad de tomar decisiones estratégicas sobre información, así como al grupo de personas responsables de planificar y ejecutar la entrega de los sistemas de información
Operación del Servicio Basada en ITIL V3	Arjen de Jong	
Mejora Continua del Servicio Basada en ITIL V3	Axel Kolthof	
Estrategia del Servicio Basada en ITIL V3	Mike Pieper	
Diseño del Servicio Basada en ITIL V3	Ruby Tjassing	
	Annelies van der Veen	
	Tieneke Verheijen	
Programación web en java	José Aranzazu Cassá	Métodos de programación en Shell
<b>Criterio de Expertos</b>	<b>Área de conocimiento</b>	<b>Descripción</b>
Gerente de Producción	Programación en Java e Infraestructura	Desarrollador experimentado de la empresa
Administrador de Base de datos	Base de datos	DBA de la empresa
Analista de Sistemas	Usuario experto	Usuario experto en las aplicaciones
<b>Informes técnicos</b>	<b>Fuente</b>	<b>Descripción</b>
Sitios web	IBM y Oracle	Descripción del uso de WebSphere y Oracle

Fuente: Elaboración propia, 2017

### 3.2.1.2 Fuentes secundarias

Se señala que “las fuentes secundarias son aquellas que contienen información organizada, elaborada, producto de análisis, extracción o reorganización que refiere a documentos primarios originales” (Alcalá, s.f.).

Las fuentes secundarias que se utilizarán para esta investigación serán informes de la empresa Amdocs Costa Rica, otros trabajos de investigación de la Universidad Hispanoamericana, sitios web relacionados con sistemas de monitoreo de infraestructura.

### 3.2.2 Sujetos de Información

A continuación, se detallarán los sujetos consultados para realizar la investigación, con el fin de recopilar datos importantes.

Tabla 5. Sujetos de Información

<b>Departamento</b>	<b>Puesto</b>
Informática	Gerente de Producción
Informática	Administrador de Base de Datos
Informática	Analista de Sistemas

Fuente: Elaboración propia, 2017

### 3.2.3 Técnicas y Herramientas

Las siguientes son las técnicas y herramientas que se implementarán en la investigación.

#### 3.2.3.1 Entrevista

La Real Academia Española (s.f.) define entrevista de la siguiente manera, “vista, concurrencia y conferencia de dos o más personas en lugar determinado, para tratar o resolver un negocio.”

En una investigación cualitativa es una herramienta muy importante debido a la experiencia de las personas, según menciona Sampieri (2010, p.17), al realizar

entrevistas abiertas a ingenieros muy experimentados que le transmitirían sus vivencias, problemas que enfrentaron y las soluciones implementadas.

Se realizarán entrevistas con los expertos de Amdocs Costa Rica, detalladas en la tabla 4, con el fin de obtener información relacionada sobre conocimiento y medidas.

### **3.2.3.2 Cuestionario**

Uno de los instrumentos más utilizados para realizar la recolección de datos, según establece Sampieri (2010). “Un cuestionario consiste en un conjunto de preguntas respecto de una o más variables a medir” (p.217).

Esta herramienta se utilizará para determinar el método actual de aseguramiento y diagnóstico de la infraestructura, además se conocerá la perspectiva que tiene el personal de Amdocs Costa Rica respecto a ella y de esta manera se podrá formular puntos de mejora.

## **3.3 Variables de Investigación**

A continuación, se presentarán las variables del proyecto en relación con los objetivos establecidos.

Tabla 6. Variables de Investigación

Objetivo Específico	Variables	Fuentes y Sujetos	Herramientas
Diagnosticar la situación actual del aseguramiento y diagnóstico de la infraestructura para la determinación de brechas conforme a las recomendaciones y tendencias del mercado.	Situación actual del aseguramiento y diagnóstico de la infraestructura  Recomendaciones y tendencias del mercado	Normativas ISO	Revisión de las normativas ISO
Establecer el diseño del sistema bajo un modelo estandarizado de gestión en cumplimiento de los requerimientos del negocio.	Diseño del sistema bajo modelo estandarizado	Mejores prácticas COBIT	Entrevistas a profesionales en el campo de TI  Revisión de recomendaciones COBIT
Crear un prototipo del sistema conforme al diseño y requerimientos establecidos mediante la aplicación de metodologías de desarrollo del mercado.	Prototipo del sistema	Mejores prácticas ITIL  Programación de Shell Script  Manual de Introducción al lenguaje HTML  Programación web en java	Entrevistas a profesionales en el campo de TI  Revisión de la documentación de lenguajes de programación
Implementar un plan piloto para el prototipo del sistema relacionado con la obtención de resultados, así como su comparación con respecto a la operación actual de la empresa.	Implementación de plan piloto para prototipo	Mejores prácticas ITIL	Entrevistas a profesionales en el campo de TI  Revisión de las recomendación ITIL V3

Fuente: Elaboración Propia, 2017

### 3.4 Diseño de la Investigación

El proyecto buscará proponer una mejora al sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs Costa Rica, donde se han establecido varias etapas con el fin de cumplir cada objetivo:

Figura 12. Diseño del proyecto de graduación



Fuente: Elaboración Propia, 2017

En la figura 12 se muestra las partes con las que cuenta el diseño del proyecto de graduación, que será detallado a continuación:

- **Recopilación de Datos:** Por medio de entrevistas con los diferentes expertos en el área de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica a través de cuestionarios.
- **Análisis de datos:** Con base en el estudio de las mejores prácticas de mercado se podrá establecer los requerimientos para realizar la propuesta de mejora al sistema de aseguramiento y diagnóstico de infraestructura.
- **Desarrollo de prototipo:** Haciendo uso del criterio de los expertos, normativas y mejores prácticas se desarrollará un sistema de aseguramiento y diagnóstico de infraestructura de acuerdo a los requisitos establecido.

## **CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL**

El siguiente capítulo consistirá en el diagnóstico de la situación actual con que cuenta el sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica, quien se encarga de proveer software y servicios de telecomunicaciones.

## **4.1 Diagnóstico Operativo**

### **4.1.1 Modelos de trabajo actuales**

La empresa Amdocs Costa Rica posee una gama de dispositivos como servidores físicos y virtuales, estos cuentan con distintos procesos y aplicaciones que deben ser monitoreados para proveer un buen servicio.

La interrupción del funcionamiento de un dispositivo significa en la mayoría de los casos una afectación en el servicio, puede llegar a provocar pérdidas al negocio; el sistema hace una verificación de cada uno de los dispositivos configurados, envía notificaciones a través de correo electrónico y mensajería de texto para una atención ágil y efectiva.

El personal de Amdocs Costa Rica recibe las alertas con una descripción y el error del dispositivo que está siendo afectado, luego proceden a identificar si el incidente es conocido o si está documentado para resolverlo, si este constituye un incidente no conocido o necesita de mayor análisis, se escala al especialista en el área para estudiar el problema y de ser necesario se realiza un cambio controlado para poder solventarlo.

#### 4.1.2 Licenciamiento de Infraestructura

La empresa actualmente ha adquirido diversas licencias para los diferentes componentes de su infraestructura, entre estas se encuentran tres externas y una propia que se detallará a continuación en la tabla 7.

Tabla 7. Licenciamiento de Productos

Producto	Versión	Tipo	Propietario
AIX	5.3	Sistema Operativo	IBM
WebSphere	6.1	Middleware	IBM
Oracle	10g	Base de datos	Oracle
OSS	7.5	Aprovisionamiento e Inventario	Amdocs

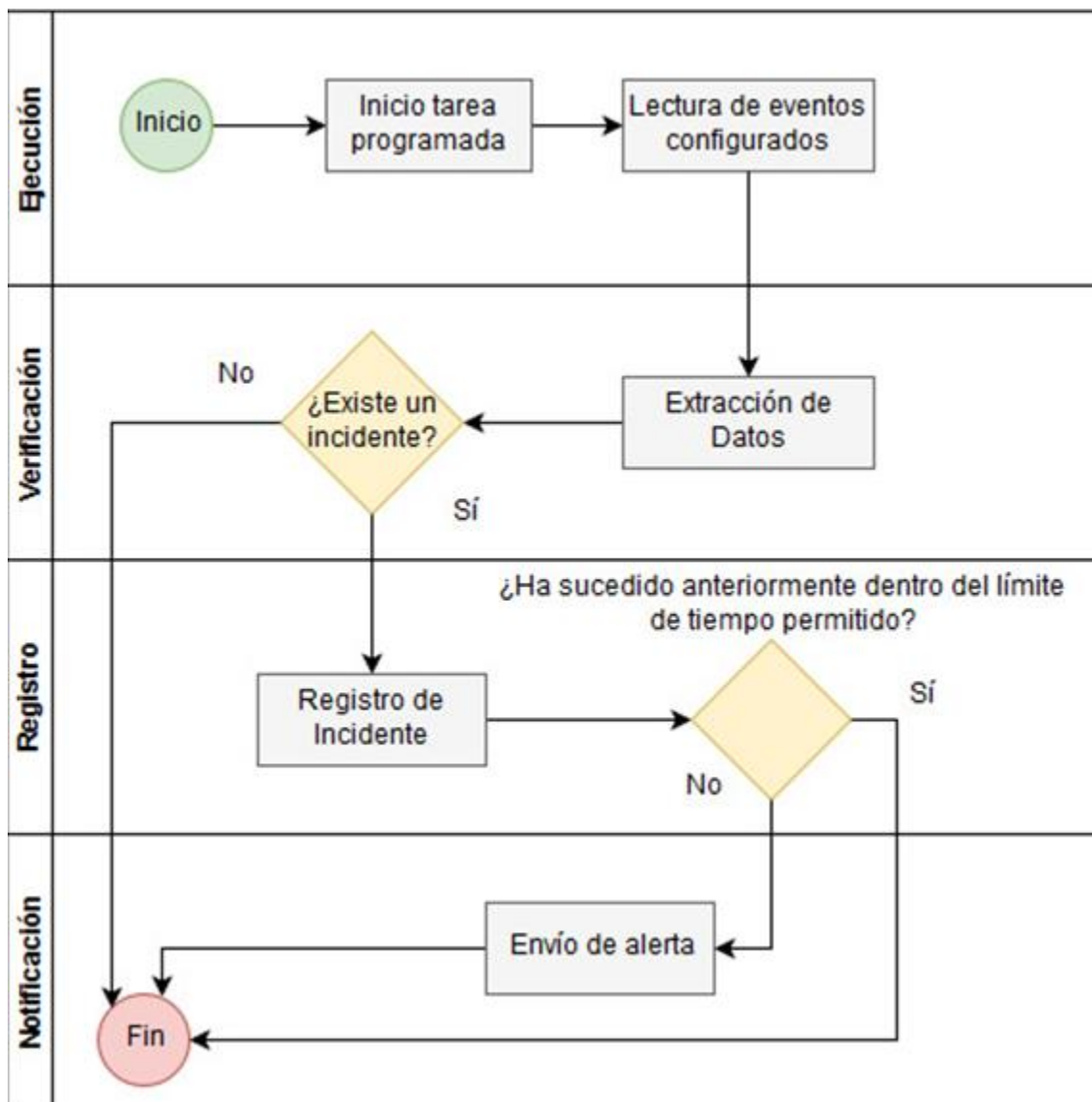
Fuente: Elaboración Propia, 2017

El sistema de aseguramiento de infraestructura actual no necesita de un licenciamiento adicional, debido a que ha sido creado por el mismo personal de Amdocs por medio de scripts de sistema operativo que extraen la información, utilizando conexiones SSH, el cual no requiere de agentes adicionales.

#### 4.1.3 Proceso de monitoreo

La figura 13 muestra el proceso utilizado por el sistema de aseguramiento de infraestructura actual de la empresa Amdocs Costa Rica, para la detección y notificación de incidentes.

Figura 13. Proceso del sistema de aseguramiento y diagnóstico



Fuente: Elaboración Propia, 2017

El proceso del sistema de aseguramiento y diagnóstico de la infraestructura actual, consiste en varios scripts que contienen listas de ítems, las cuales van a ser parte del monitoreo, el proceso es ejecutado a través de tareas programadas en Unix, este verifica los ítems configurados en las listas y realiza la conexión a los diferentes servidores para

extraer los datos, luego se comparan los datos recopilados con los parámetros de monitoreo, si existe un incidente se registra en la base de datos, luego los scripts hacen una verificación con la cantidad de tiempo configurado que resulta necesario para enviar una alerta respecto a la última que se envió, si el incidente es nuevo o si es repetido, pero ha superado la cantidad de tiempo permitido, se envía la alerta.

#### 4.1.4 Ítems de monitoreo

El sistema de aseguramiento y diagnóstico de infraestructura actual en la empresa Amdocs Costa Rica tiene establecidos una serie de ítems que deben ser monitoreados para poder garantizar un buen servicio, donde se pueden observar el estado de los servidores tanto físicos como virtuales.

La tabla 8 especifica los diferentes ítems que han sido configurados

Tabla 8. Ítems de monitoreo

Ítem	Descripción	Notificación
Acceso de red	Verificación de la accesibilidad de los servidores físicos en la red	No accesible
Servidor de aplicación	Verificación del estado del servidor virtual	Detenido
Aplicación empresarial	Verificación del estado de la aplicación instalada	Detenida
Errores de aplicación	Verificación de errores en los logs de los servidores virtuales	Encontrados
Procesos	Verificación del estado de procesos específicos (demonios) ejecutados en los servidores físicos	Detenidos
Espacio en disco	Verificación del espacio disponible en el disco duro en servidores físicos	Alcanza límite permitido

Fuente: Elaboración Propia, 2017

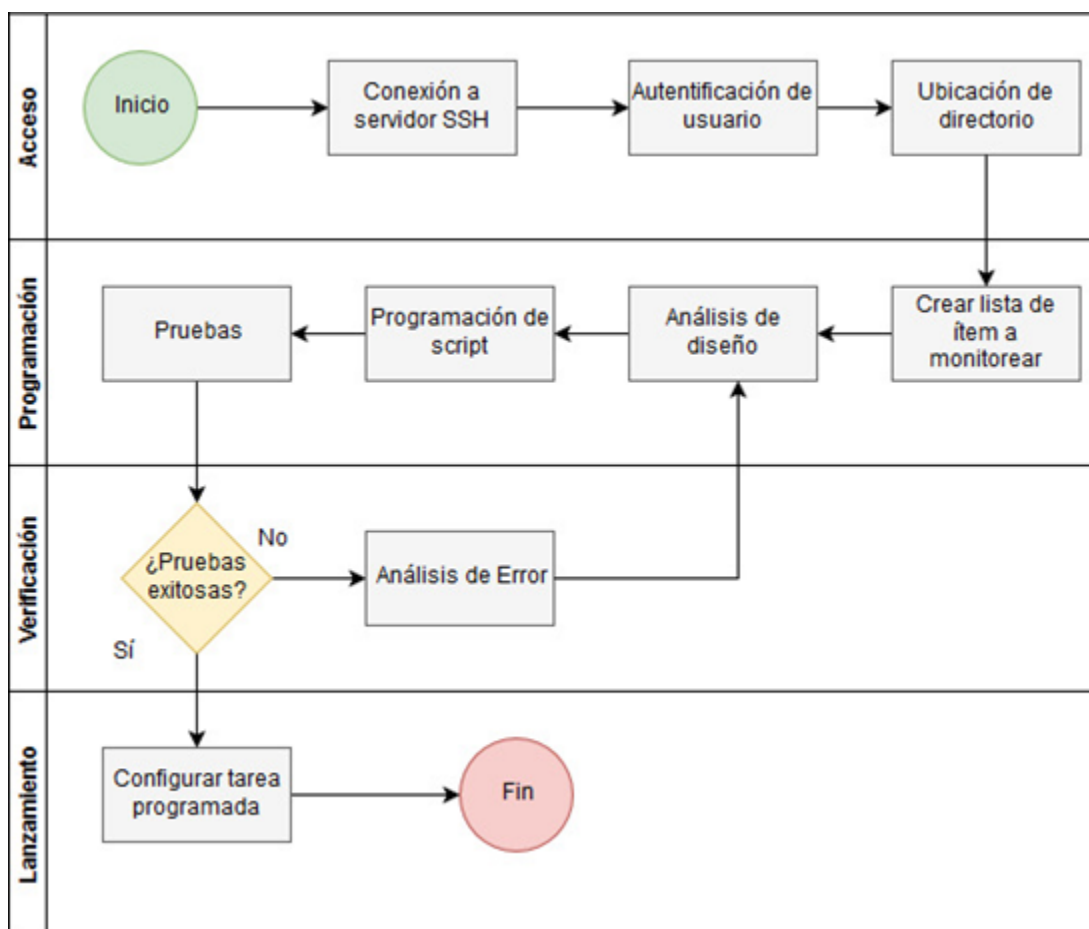
#### 4.1.5 Proceso de elaboración y manejo de alertas de monitoreo

El sistema de monitoreo actual se encuentra configurado en su totalidad con Shell scripts sin una interfaz gráfica, ubicados en diferentes directorios de acuerdo a la aplicación y al

tipo de alerta; además cada alerta cuenta con un script diferente de acuerdo a la función que se desea monitorear.

Las listas de configuración de los ítems se encuentran en archivos de texto plano ubicados en los directorios donde se almacenan los scripts, la figura 14 muestra el proceso de creación de una nueva alerta.

Figura 14. Elaboración de una alerta en el sistema actual



Fuente: Elaboración Propia, 2017

Para poder crear, modificar o eliminar una alerta del sistema de monitoreo es requisito primordial tener una cuenta con acceso de lectura y escritura a los servidores en Unix y

dependiendo del nivel de complejidad de programación de la alerta, este proceso puede tomar alrededor de 60 minutos por script.

## **4.2 Diagnóstico Técnico**

A continuación, se detallarán los diferentes elementos de infraestructura y software que componen la plataforma de Amdocs Costa Rica que están siendo monitoreados bajo el sistema actual de aseguramiento y diagnóstico.

### **4.2.1 Infraestructura**

La empresa Amdocs Costa Rica cuenta con 25 servidores físicos y 97 servidores virtuales instalados en WebSphere, todos estos detallados al inicio de este documento en las tablas 1 y 2.

#### **4.2.1.1 Servicios**

La empresa Amdocs Costa Rica se encarga de proveer servicios de aprovisionamiento para redes celulares e inventario de equipo de red, la plataforma a su vez se encuentra dividida en módulos que cuentan con una función específica.

El servicio de aprovisionamiento cuenta con un nivel más completo de procesamiento, debido a que posee diferentes módulos que interactúan entre sí para procesar una orden de servicio.

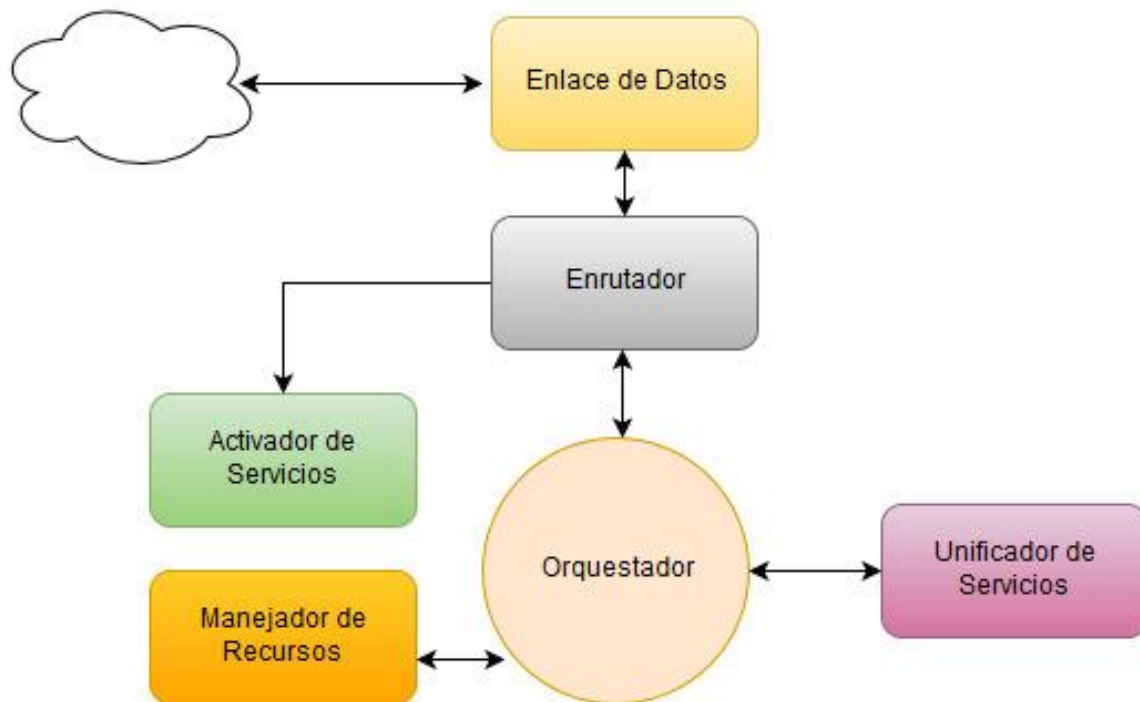
La plataforma del servicio de aprovisionamiento está compuesta por los siguientes módulos:

1. **Enlace de datos:** Se encarga de recibir las solicitudes para activar o desactivar un nuevo servicio de la red celular.

2. **Enrutador:** Su función es enviar las diferentes transacciones para que sean procesadas hacia los módulos de orquestación o activación.
3. **Orquestador:** Es el módulo más complejo, este se encarga de procesar la orden de servicio, solicitando información a los demás módulos sobre recursos o servicios disponibles y enviar la solicitud de activación o desactivación de un servicio móvil.
4. **Manejador de Recursos:** Este módulo contiene la información de los números de teléfonos disponibles que pueden ser asignados.
5. **Unificador de Servicios:** Contiene la información de los servicios que tiene asociado un número de teléfono, ya sea internet, vídeo llamada, llamadas internacionales, etc.
6. **Activador de Servicios:** Se encarga de activar o desactivar un servicio en la red celular.

La figura 15 muestra el diseño de los módulos de la plataforma del servicio de aprovisionamiento.

Figura 15. Diseño de módulos de la plataforma del servicio de aprovisionamiento

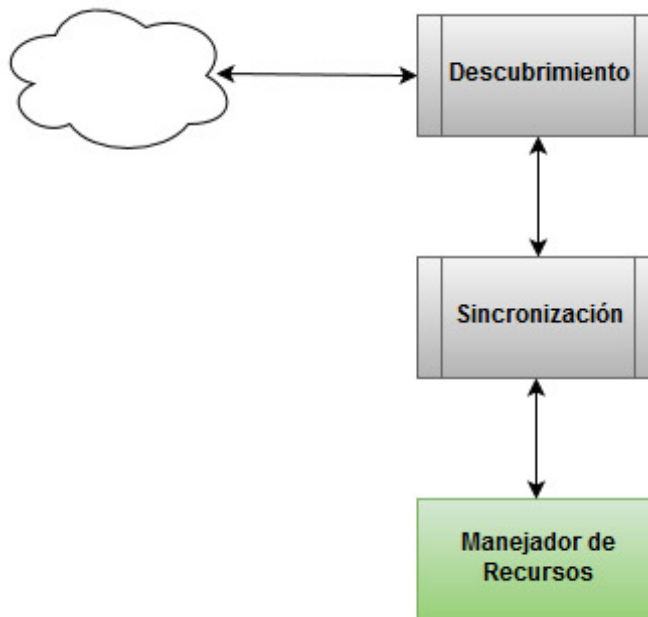


Fuente: Elaboración Propia, 2017

El servicio de inventario se encarga de ejecutar un proceso de descubrimiento de dispositivos en la red y una vez que son descubiertos, otro proceso se encarga de realizar la sincronización hacia la base de datos para que así sean visibles en la aplicación.

La figura 16 muestra el diagrama de la plataforma del servicio de inventario.

Figura 16. Diseño de módulos la plataforma de servicios de inventario



Fuente: Elaboración Propia, 2017

La plataforma del servicio de inventario se compone de los siguientes módulos:

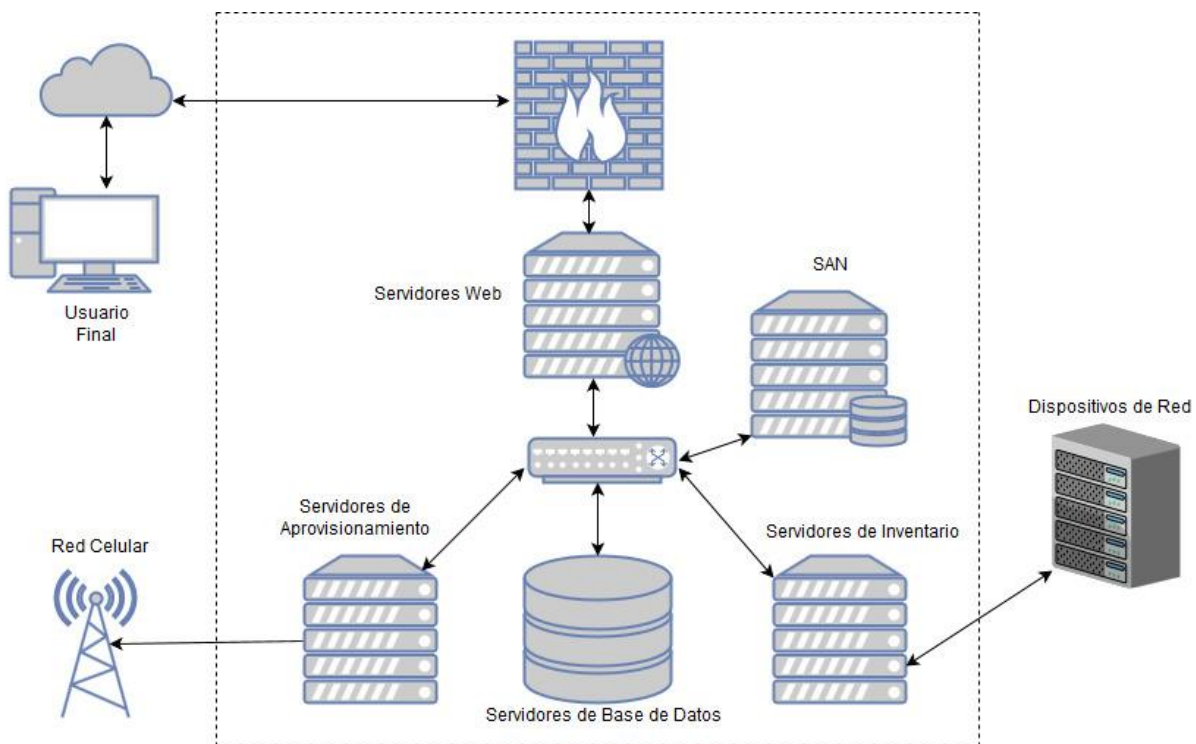
1. **Descubrimiento:** Se encarga de hacer un reconocimiento de los dispositivos que están en la red, conocer su estado y verificación de equipo nuevo.
2. **Sincronización:** Proceso que envía la información de los dispositivos encontrados en la red a una base de datos.
3. **Manejador de recursos:** Su función es administrar y configurar los dispositivos que han sido encontrados en la red.

#### 4.2.1.2 Servidores físicos

Los servidores son utilizados para proveer los servicios de aprovisionamiento, inventario y base de datos, además la empresa cuenta con servidores web para proveer el acceso a las aplicaciones y realizar un balance de cargas.

La figura 17 muestra el diagrama de la infraestructura de los servidores físicos.

Figura 17. Diagrama de Infraestructura Física



Fuente: Elaboración Propia, 2017

#### 4.2.1.3 Servidores virtuales

La arquitectura de la plataforma de servicios en la empresa Amdocs Costa Rica consta de 97 servidores virtuales instalados en WebSphere y divididos por celdas que han sido asignadas a cada módulo de acuerdo a la función que desempeña la aplicación.

La tabla 9 muestra cómo se encuentran distribuidos los servidores virtuales entre los servicios de aprovisionamiento e inventario.

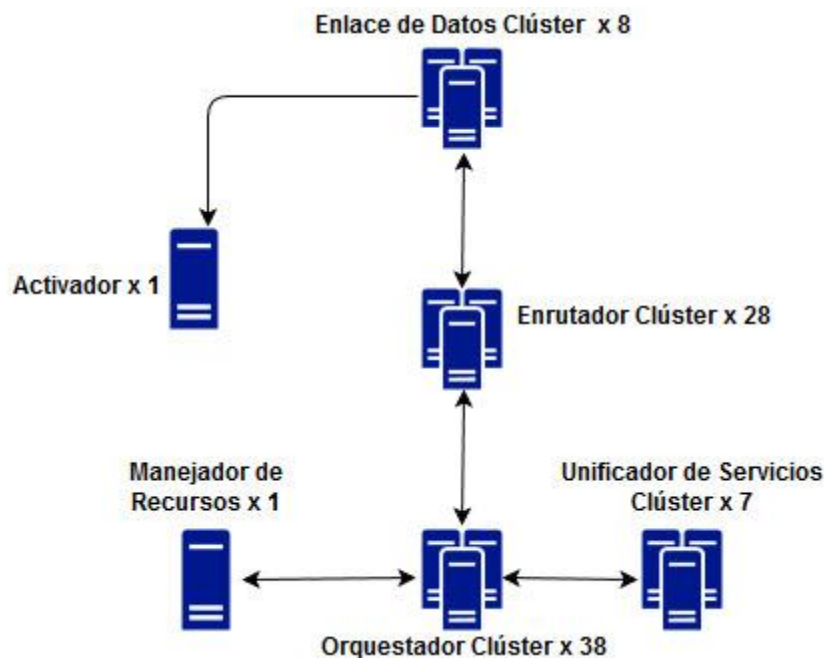
Tabla 9. Distribución de servidores virtuales

<b>Aprovisionamiento</b>		<b>Inventario</b>	
<b>Módulo</b>	<b>Cantidad</b>	<b>Módulo</b>	<b>Cantidad</b>
Enlace de datos	8	Descubrimiento	3
Enrutador	28	Sincronización	1
Orquestador	38	Manejador de Recursos	8
Unificador de Servicios	7		
Manejador de Recursos	1		
Activador	1		
Web	2		
<b>TOTAL</b>	<b>85</b>		<b>12</b>

Fuente: Elaboración Propia, 2017

La figura 18 muestra el diagrama con la distribución de los servidores virtuales de los módulos de la plataforma del servicio de aprovisionamiento:

Figura 18. Diagrama de Infraestructura Virtual de Aprovisionamiento

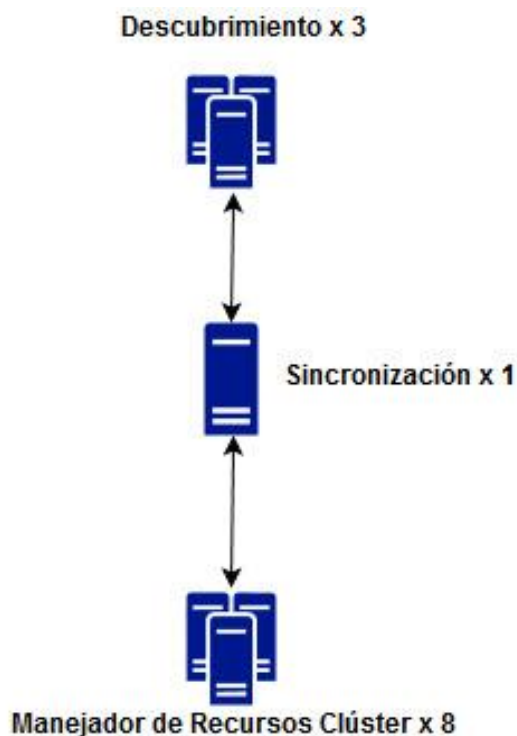


Fuente: Elaboración Propia, 2017

Los módulos están instalados en su mayoría en clúster de acuerdo a la cantidad de procesamiento que necesite la aplicación, los servidores que son autónomos manejan un flujo más bajo de trabajo y cuentan con una configuración de continuidad de negocio activo – pasivo.

La figura 19 contiene el diagrama con la distribución de los servidores virtuales de los módulos de la plataforma del servicio de inventario:

Figura 19. Diagrama de Infraestructura Virtual de Inventario



Fuente: Elaboración Propia, 2017

La plataforma del servicio de inventario solo cuenta con un módulo en clúster que es el manejador de recursos ya que cuenta con mayor procesamiento de datos, el servidor de sincronización realiza un único proceso, por esa razón solo necesita de un servidor, por último, el módulo de descubrimiento cuenta con 3 servidores autónomos que realizan tareas específicas para escanear todos los dispositivos en la red.

### **4.3 Brechas entre el sistema actual y el propuesto**

La empresa Amdocs Costa Rica cuenta con un sistema de aseguramiento de infraestructura efectivo en la actualidad, sin embargo, es creado a nivel de sistema operativo por medio de scripts, el cual requiere de conocimiento especial en programación Shell y administración en Unix, genera que la creación de una alerta lleve a tomar mucho tiempo en ser finalizada.

Las alertas funcionan de manera adecuada, cada vez que se suscita un incidente en la infraestructura el script envía una notificación a través de correos electrónicos y mensajes de texto para que el personal pueda atenderlo lo más pronto posible.

El sistema al no ser estandarizado posee una gran cantidad de scripts que se encuentran ubicados en diferentes directorios en el servidor, dificulta la modificación, debido a que se debe realizar una búsqueda del script en específico y una vez identificado se debe volver a analizar el código para verificar su funcionamiento y así modificarlo, finalmente se volverán a realizar pruebas y se confirmará que los cambios deseados fueron exitosos.

La configuración del sistema no se encuentra almacenada en un punto centralizado se efectúa a través de múltiples archivos de texto plano dentro de los directorios del servidor que son consultados por los scripts a la hora de ser ejecutados, si se desea agregar, editar o eliminar un ítem en la configuración, se debe ubicar el archivo de configuración relacionado con la alerta y proceder a la modificación.

La propuesta del proyecto que se plantea simplificará el proceso de administración de monitoreo ya que centralizará la configuración del sistema en una base de datos, dejando

de lado el uso de múltiples archivos de texto plano, además estandarizará los scripts de recolección de datos, lo cual permitirá el uso de pocos scripts ubicados en un mismo directorio para todas las diferentes alertas que serán necesarias.

El uso de una interfaz web que forma parte de la propuesta beneficiará al personal de Amdocs Costa Rica en la reducción de tiempo a la hora de crear, editar o eliminar alertas ya que no se deberá realizar la programación de un servidor en Shell Script, sino que lo hará por medio de asistentes.

Finalmente, el sistema propuesto permitirá al personal visualizar los incidentes que han ocurrido de manera sencilla sin tener que hacer uso de una herramienta adicional para consultar la base de datos.

En la tabla 10 se podrá observar un resumen de la comparación entre el sistema actual con el sistema que será propuesto.

La tabla 10 hace una comparación entre el sistema actual y lo que se espera con la propuesta.

Tabla 10. Comparación entre sistema actual y propuesta

<b>Sistema Actual</b>	<b>Propuesta</b>
Manejo del sistema por Unix Shell	Manejo del sistema por aplicación web
Múltiples scripts para recolección de datos y envío de notificaciones por alerta	Scripts de recolección de datos y envío de alertas estandarizado para todas las alertas
Configuración de sistema almacenada en archivos de texto plano	Configuración de sistema centralizada en base de datos
Proceso de elaboración y manejo de alertas a través de programación de código	Proceso de elaboración y manejo de alertas simplificado por asistentes web.

Fuente: Elaboración Propia, 2017

## **CAPÍTULO V: PROPUESTA DE PROYECTO**

A continuación, en el siguiente capítulo se presentará la propuesta de mejora para el sistema de aseguramiento y diagnóstico de infraestructura en la empresa Amdocs Costa Rica, donde se definirá el diseño del sistema, el prototipo y el piloto de implementación del mismo.

## **5.1 Diseño del sistema de aseguramiento y diagnóstico de infraestructura**

### **5.1.1 Requerimientos del sistema**

La propuesta buscará cubrir la mayor necesidad del personal de Amdocs, el cual es contar con un sistema eficiente y de fácil acceso, que cuente con una configuración y administración sencilla para la notificación de los diferentes incidentes que se pueden presentar en la infraestructura sin la necesidad de programar scripts a nivel de sistema operativo.

La empresa ha establecido una serie de requerimientos que debe cumplir la propuesta del sistema de aseguramiento y diagnóstico de infraestructura, cada uno fue establecido con base en las diferentes entrevistas realizadas con el personal.

La tabla 11 mostrará el requerimiento de administración de alertas donde se establecerá las entradas deseadas, el procedimiento a ser ejecutado con sus respectivas salidas.

Tabla 11. Requerimiento de Administración de alertas

<b>ID:</b>	R1	<b>Estado:</b> Solicitado
<b>Nombre:</b> Administración de alertas		
<b>Descripción:</b> Se requiere un mantenimiento para administrar los registros de las alertas, el sistema debe proporcionar poder agregar, modificar, eliminar cualquier registro.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Tipo de alerta.</li> <li>• Usuario de Unix.</li> <li>• Servidor.</li> <li>• Frecuencia.</li> <li>• Estado alerta por correo.</li> <li>• Grupo de correos.</li> <li>• Estado alerta por SMS</li> <li>• Grupo de SMS</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de administración, e ingresa a la opción de configuración de alertas.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> </ul>		

La tabla 12 mostrará el requerimiento de configuración de monitoreo donde se establecerán las entradas deseadas, el procedimiento a ser ejecutado con sus respectivas salidas.

Tabla 12. Requerimiento de Configuración de monitoreo

<b>ID:</b>	R2	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de monitoreo		
<b>Descripción:</b> Se requiere un mantenimiento de los datos que las alertas van a consultar para enviar las notificaciones.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Configuración de aplicaciones.</li> <li>• Configuración de tipo de alerta.</li> <li>• Configuración de grupo de correo.</li> <li>• Configuración de grupo de SMS</li> <li>• Configuración de lista de correos.</li> <li>• Configuración de lista de números SMS</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de monitoreo, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> </ul>		

Fuente: Elaboración Propia, 2017

La tabla 13 mostrará el requerimiento de configuración de servidores donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 13. Requerimiento de Configuración de servidores

<b>ID:</b>	R3	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de servidores		
<b>Descripción:</b> Se requiere un mantenimiento con los nombres de los servidores de aplicación que van a ser monitoreados, el servidor físico donde están instalados, las aplicaciones que contienen y los eventos ocurridos.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Nombre de aplicación.</li> <li>• Servidor físico.</li> <li>• Servidor de aplicación.</li> <li>• Estado del servidor de aplicación.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de servidor de aplicación, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 14 mostrará el requerimiento de configuración de aplicación donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 14. Requerimiento de Configuración de aplicación

<b>ID:</b>	R4	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de aplicación		
<b>Descripción:</b> Se requiere un mantenimiento con los nombres de las aplicaciones empresariales ligados con el componente de aplicación de la plataforma de servicios.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Nombre de componente de aplicación de servicio.</li> <li>• Nombre de aplicación empresarial.</li> <li>• Listar incidentes.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de aplicación, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 15 mostrará el requerimiento de configuración de errores donde se establecerán las entradas deseadas, el procedimiento a ser ejecutado con sus respectivas salidas.

Tabla 15. Requerimiento de Configuración de errores

<b>ID:</b>	R5	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de errores		
<b>Descripción:</b> Se requiere un mantenimiento para configurar los archivos de registros que deben ser monitoreados, además de los directorios en donde se encuentran ubicados, los errores que se desea notificar y los parámetros que deben ser descartados.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Configurar directorio y archivo.</li> <li>• Configurar error.</li> <li>• Configurar lista de descarte.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de aplicación, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 16 mostrará el requerimiento de configuración de tareas donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 16. Requerimiento de Configuración de tareas

<b>ID:</b>	R6	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de tareas		
<b>Descripción:</b> Se requiere un mantenimiento para configurar diferentes tareas que se ejecutan a través de la base de datos mediante consultas.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Configurar el tipo de tarea.</li> <li>• Configurar consulta de la tarea.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de aplicación, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 17 mostrará el requerimiento de configuración de procesos donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 17. Requerimiento de Configuración de procesos

<b>ID:</b>	R7	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de procesos		
<b>Descripción:</b> Se requiere un mantenimiento para configurar diferentes procesos específicos de sistema operativo que deben estar siendo ejecutados en los servidores.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Aplicación relacionada.</li> <li>• Nombre del proceso.</li> <li>• Cantidad.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de procesos, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 18 mostrará el requerimiento de configuración de acceso de red donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 18. Requerimiento de Configuración de acceso de red

<b>ID:</b>	R8	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de acceso de red		
<b>Descripción:</b> Se requiere un mantenimiento para configurar los nombres y las direcciones IP de los servidores que deben estar siempre accesibles en la red.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Nombre del servidor.</li> <li>• Dirección IP</li> <li>• Componente de aplicación que posee.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de acceso de red, e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 19 mostrará el requerimiento de configuración de almacenamiento donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 19. Requerimiento de Configuración de almacenamiento

<b>ID:</b>	R9	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de almacenamiento		
<b>Descripción:</b> Se requiere un mantenimiento para configurar los sistemas de archivos en los diferentes servidores para notificar cuando existe poco espacio disponible en el disco duro.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Nombre del servidor.</li> <li>• Sistema de archivo.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de almacenamiento e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> <li>• El usuario podrá listar incidentes asociados.</li> </ul>		

Fuente: Elaboración propia, 2017

La tabla 20 mostrará el requerimiento de configuración de estado de monitoreo donde se establecerán las entradas deseadas, el procedimiento por ser ejecutado con sus respectivas salidas.

Tabla 20. Requerimiento de Configuración de estado de monitoreo

<b>ID:</b>	R10	<b>Estado:</b> Solicitado
<b>Nombre:</b> Configuración de estado de monitoreo		
<b>Descripción:</b> Se requiere un mantenimiento para activar o desactivar las notificaciones del monitoreo para todos los componentes de una aplicación específica.		
<b>Entradas:</b>		
<ul style="list-style-type: none"> <li>• Nombre del componente de aplicación.</li> <li>• Estado.</li> </ul>		
<b>Procedimiento:</b>		
<ul style="list-style-type: none"> <li>• El usuario ingresa al módulo de configuración de estado de monitoreo e ingresa a la opción de configuración deseada.</li> <li>• El usuario ingresa las entradas necesarias del mantenimiento.</li> <li>• El usuario da clic en el botón guardar.</li> </ul>		
<b>Salidas:</b>		
<ul style="list-style-type: none"> <li>• Se listará en pantalla al usuario el proceso realizado.</li> </ul>		

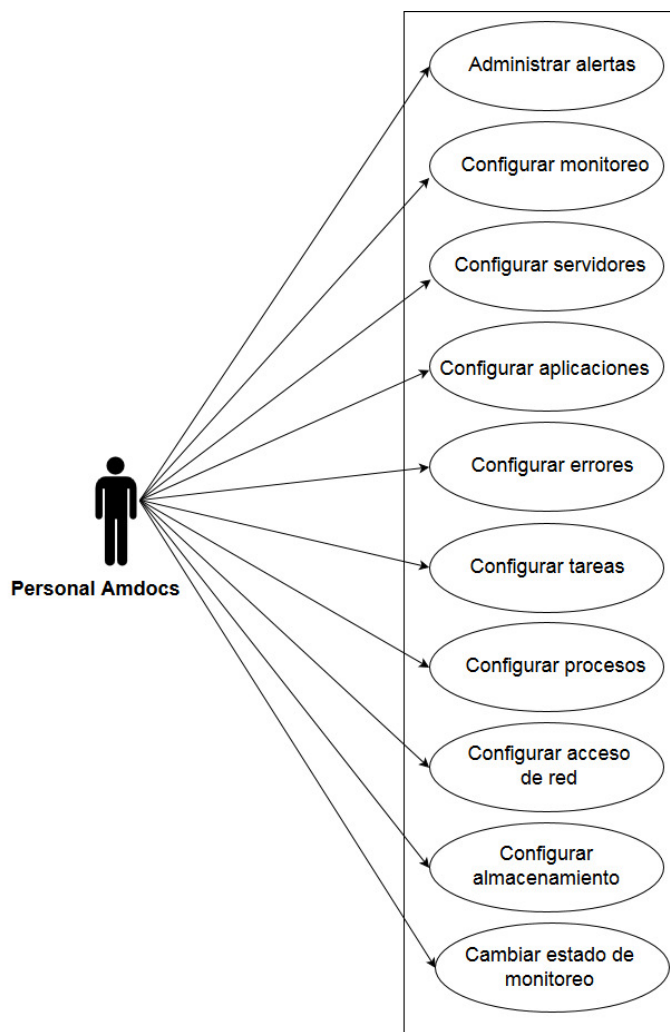
Fuente: Elaboración propia, 2017

## 5.1.2 Modelado de casos de uso

Una vez conocidos los requerimientos del sistema se procederá a profundizar en detalle un conjunto de requisitos mediante casos de uso, de acuerdo a las diferentes funciones que el sistema va a poseer.

### 5.1.2.1 Diagrama de Casos de Uso

Figura 20. Casos de uso de la propuesta del sistema



Fuente: Elaboración propia, 2017

### 5.1.2.2 Casos de Uso

La tabla 21 mostrará el caso de uso para administrar las alertas donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 21. Caso de uso de administrar alertas

Nombre:	Administrar alertas	ID	CU1
ID Requerimiento	RF1		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar las alertas que se desea recibir de la infraestructura a través de correos y SMS.		
Actores:	Personal de Amdocs		
Precondición:	1- Debe haber un tipo de aplicación configurado. 2- Debe haber un grupo de correo electrónico configurado. 3- Debe haber un grupo de SMS configurado.		
Flujo Normal:	Paso:	Acción:	
	1	Seleccionar el tipo de aplicación.	
	2	Seleccionar el tipo de alerta.	
	3	Ingresar el usuario de Unix.	
	4	Ingresar el servidor de manejo de la aplicación.	
	5	Ingresar la frecuencia de envío de notificaciones.	
	6	Seleccionar el estado de la notificación por correo electrónico.	
	7	Seleccionar el grupo de correo electrónico a ser notificado.	
	8	Seleccionar el estado de la notificación por SMS	
	9	Seleccionar el grupo de SMS a ser notificado.	
	10	Presionar botón de enviar.	
Flujo Alternativo 1:	Paso:	Acción:	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 22 mostrará el caso de uso para configurar el tipo de aplicación del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 22. Caso de uso de configurar monitoreo - tipo de aplicación

<b>Nombre:</b>	<b>Configurar monitoreo - tipo de aplicación</b>		<b>ID</b>	<b>CU2.1</b>
<b>ID Requerimiento</b>	<b>RF2</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los diferentes tipos de aplicaciones.			
Actores:	Personal de Amdocs			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar nombre del tipo aplicación.		
	2	Ingresar nombre del perfil del tipo de aplicación.		
	3	Ingresar sufijo del tipo de aplicación.		
	4	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 23 mostrará el caso de uso para configurar el tipo de alerta del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 23. Caso de uso de configurar monitoreo - tipo de alerta

<b>Nombre:</b>	<b>Configurar monitoreo - tipo de alerta</b>		<b>ID</b>	<b>CU2.2</b>
<b>ID Requerimiento</b>	<b>RF2</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los diferentes tipos de alertas.			
Actores:	Personal de Amdocs			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar descripción.		
	2	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 24 mostrará el caso de uso para configurar el grupo de correo electrónico del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 24. Caso de uso de configurar monitoreo - grupo de correo electrónico

<b>Nombre:</b>	<b>Configurar monitoreo - grupo de correo electrónico</b>		<b>ID</b>	<b>CU2.3</b>
<b>ID Requerimiento</b>	<b>RF2</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los grupos de correo electrónico que recibirán las alertas.			
Actores:	Personal de Amdocs			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar nombre del grupo de correo electrónico.		
	2	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 25 mostrará el caso de uso para configurar el correo electrónico del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 25. Caso de uso de configurar monitoreo - correos electrónicos

<b>Nombre:</b>	<b>Configurar monitoreo - correos electrónicos</b>	<b>ID</b>	<b>CU2.4</b>
<b>ID Requerimiento</b>	<b>RF2</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar los correos electrónicos y asociarlos a un grupo de correo electrónico que recibirán las alertas.		
Actores:	Personal de Amdocs		
Precondición:	Debe existir un grupo de correo electrónico.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Ingresar correo electrónico.	
	2	Seleccionar grupo de correo electrónico.	
	3	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 26 mostrará el caso de uso para configurar el grupo de SMS del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 26. Caso de uso de configurar monitoreo - grupo de SMS

<b>Nombre:</b>	<b>Configurar monitoreo - grupo de SMS</b>		<b>ID</b>	<b>CU2.5</b>
<b>ID Requerimiento</b>	<b>RF2</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los grupos de SMS que recibirán las alertas.			
Actores:	Personal de Amdocs			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar nombre del grupo de SMS.		
	2	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 27 mostrará el caso de uso para configurar el número de SMS del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 27. Caso de uso de configurar monitoreo - números de SMS

<b>Nombre:</b>	<b>Configurar monitoreo - números de SMS</b>	<b>ID</b>	<b>CU2.6</b>
<b>ID Requerimiento</b>	<b>RF2</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar los números de teléfono y asociarlos a un grupo de SMS que recibirán las alertas.		
Actores:	Personal de Amdocs		
Precondición:	Debe existir un grupo de SMS.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Ingresar número de teléfono.	
	2	Seleccionar grupo de SMS.	
	3	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 28 mostrará el caso de uso para configurar los servidores donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 28. Caso de uso de configurar servidores

<b>Nombre:</b>	<b>Configurar servidores</b>		<b>ID</b>	<b>CU3</b>
<b>ID Requerimiento</b>	<b>RF3</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los servidores que van a ser monitoreados para recibir alertas, además de activar o desactivar las alertas para un servidor de aplicación en específico.			
Actores:	Personal de Amdocs			
Precondición:	Debe existir un tipo de aplicación configurado.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Seleccionar el tipo de aplicación.		
	2	Ingresar el nombre del servidor físico.		
	3	Ingresar el nombre del servidor de aplicación (WebSphere).		
	4	Seleccionar el estado de notificación.		
	5	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 29 mostrará el caso de uso para configurar el tipo de alerta del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 29. Caso de uso de configurar aplicaciones

<b>Nombre:</b>	<b>4 - Configurar aplicaciones</b>	<b>ID</b>	<b>CU4</b>
<b>ID Requerimiento</b>	<b>RF4</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar las aplicaciones empresariales de WebSphere que deben ser monitoreadas para recibir alertas.		
Actores:	Personal de Amdocs		
Precondición:	Debe existir un tipo de aplicación configurado.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Seleccionar el tipo de aplicación.	
	2	Ingresar el nombre de la aplicación empresarial.	
	3	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 30 mostrará el caso de uso para configurar el directorio y archivo de error del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 30. Caso de uso de configurar errores - directorio y archivo

<b>Nombre:</b>	<b>Configurar errores - directorio y archivo</b>		<b>ID</b>	<b>CU5.1</b>
<b>ID Requerimiento</b>	<b>RF5</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los directorios y el archivo que debe ser monitoreado para notificar por medio de alertas los errores encontrados.			
Actores:	Personal de Amdocs			
Precondición:	Debe existir un tipo de aplicación configurado.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Seleccionar el tipo de aplicación.		
	2	Ingresar el nombre del servidor físico.		
	3	Ingresar la ruta del directorio donde se ubica el archivo.		
	4	Ingresa el nombre del archivo.		
	5	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 31 mostrará el caso de uso para configurar el código de error del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 31. Caso de uso de configurar errores - código de error

<b>Nombre:</b>	<b>Configurar errores - código de error</b>	<b>ID</b>	<b>CU5.2</b>
<b>ID Requerimiento</b>	<b>RF5</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar el código de error en conjunto con parámetros de búsqueda y el mensaje que va proporcionar la alerta.		
Actores:	Personal de Amdocs.		
Precondición:	No hay.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Ingresar código de error.	
	2	Ingresar parámetro para filtrar.	
	3	Ingresar mensaje.	
	4	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 32 mostrará el caso de uso para configurar el parámetro de descarte del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 32. Caso de uso de configurar errores - parámetro de descarte

<b>Nombre:</b>	<b>Configurar errores - parámetro de descarte</b>	<b>ID</b>	<b>CU5.3</b>
<b>ID Requerimiento</b>	<b>RF5</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar un parámetro para ser descartado en la búsqueda de errores en los archivos por medio del código de error.		
Actores:	Personal de Amdocs.		
Precondición:	No hay.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Ingresar parámetro para descartar.	
	2	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 33 mostrará el caso de uso para configurar el tipo de tarea del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 33. Caso de uso de configurar tareas - tipo de tarea

<b>Nombre:</b>	<b>Configurar tareas - tipo de tarea</b>		<b>ID</b>	<b>CU6.1</b>
<b>ID Requerimiento</b>	<b>RF6</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar la descripción del tipo de tarea que debe ser monitoreado para el envío de alertas.			
Actores:	Personal de Amdocs.			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar descripción.		
	2	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 34 mostrará el caso de uso para configurar las tareas del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 34. Caso de uso de configurar tareas

<b>Nombre:</b>	<b>Configurar tareas</b>	<b>ID</b>	<b>CU6.2</b>
<b>ID Requerimiento</b>	<b>RF6</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar la consulta de base de datos que se va a utilizar para verificar el estado de la tarea la cual debe ser monitoreada.		
Actores:	Personal de Amdocs.		
Precondición:	1- Debe haber un tipo de aplicación configurado. 2- Debe haber un tipo de tarea configurado.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Seleccionar el tipo de aplicación.	
	2	Seleccionar el tipo de tarea.	
	3	Ingresar la consulta de base de datos.	
	4	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 35 mostrará el caso de uso para configurar procesos del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 35. Caso de uso de configurar procesos

<b>Nombre:</b>	<b>Configurar procesos</b>	<b>ID</b>	<b>CU7</b>
<b>ID Requerimiento</b>	<b>RF7</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar el nombre del proceso a nivel de sistema operativo que debe ser monitoreado y la cantidad que este debe tener en ejecución.		
Actores:	Personal de Amdocs.		
Precondición:	Debe haber un tipo de aplicación configurado.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Seleccionar el tipo de aplicación.	
	2	Ingresar el nombre del proceso.	
	3	Ingresar la cantidad.	
	4	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

La tabla 36 mostrará el caso de uso para configurar el acceso de red del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 36. Caso de uso de configurar acceso de red

<b>Nombre:</b>	<b>Configurar acceso de red</b>		<b>ID</b>	<b>CU8</b>
<b>ID Requerimiento</b>	<b>RF8</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los servidores y dispositivos que deben ser accesibles en la red para así enviar alertas cuando no están disponibles.			
Actores:	Personal de Amdocs.			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar el nombre.		
	2	Ingresar la dirección IP		
	3	Ingresar la descripción.		
	4	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 37 mostrará el caso de uso para configurar el almacenamiento del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 37. Caso de uso de configurar almacenamiento

<b>Nombre:</b>	<b>Configurar almacenamiento</b>		<b>ID</b>	<b>CU9</b>
<b>ID Requerimiento</b>	<b>RF9</b>			
Autor:	Johan Quesada Romero			
Descripción:	Se encarga de ingresar, modificar o borrar los diferentes sistemas de archivos en los servidores físicos a los cuales se debe monitorear el espacio de almacenamiento disponible.			
Actores:	Personal de Amdocs.			
Precondición:	No hay.			
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Ingresar el nombre.		
	2	Ingresar la ruta del sistema de archivos.		
	3	Presionar botón de enviar.		
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>		
	1	Se valida la información.		
	2	Se muestra un mensaje de atención.		
	3	Se devuelve a pedir la información.		

Fuente: Elaboración propia, 2017

La tabla 38 mostrará el caso de uso para configurar el estado del monitoreo donde se establecerá el flujo normal y alternativo con sus respectivos pasos a seguir.

Tabla 38. Caso de uso de configurar estado del monitoreo

<b>Nombre:</b>	<b>Configurar estado del monitoreo</b>	<b>ID</b>	<b>CU10</b>
<b>ID Requerimiento</b>	<b>RF10</b>		
Autor:	Johan Quesada Romero		
Descripción:	Se encarga de ingresar, modificar o borrar el estados de todas las alertas relacionadas a una aplicación en específico para habilitar o deshabilitar las alertas por correo electrónico y SMS.		
Actores:	Personal de Amdocs.		
Precondición:	No hay.		
<b>Flujo Normal:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Ingresar aplicación.	
	2	Seleccionar el estado.	
	3	Presionar botón de enviar.	
<b>Flujo Alternativo 1:</b>	<b>Paso:</b>	<b>Acción:</b>	
	1	Se valida la información.	
	2	Se muestra un mensaje de atención.	
	3	Se devuelve a pedir la información.	

Fuente: Elaboración propia, 2017

### 5.1.3 Arquitectura del Sistema

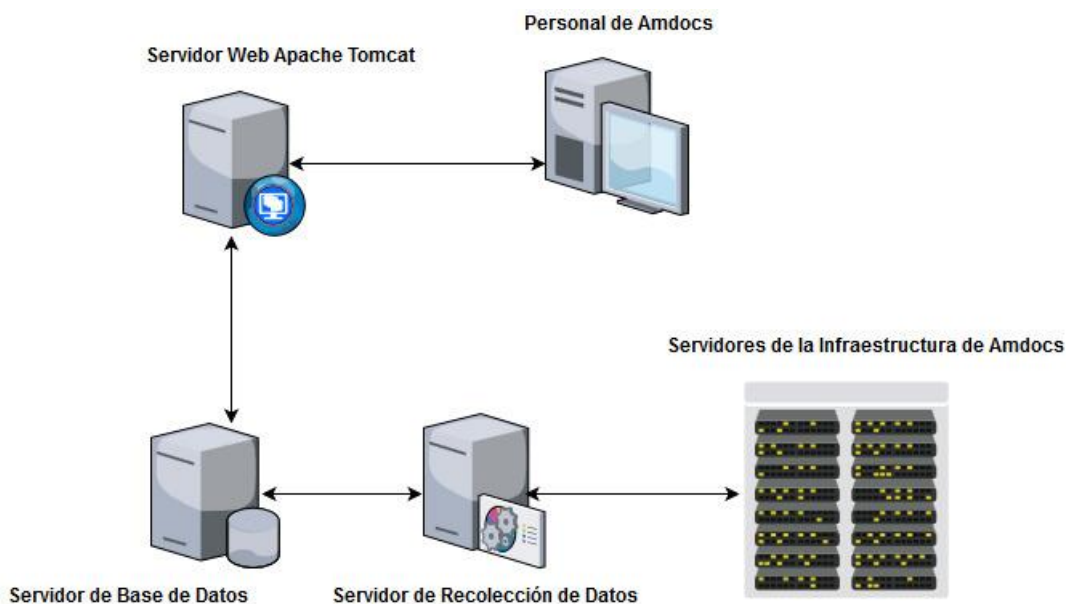
La propuesta consistirá en establecer una arquitectura centralizada para el sistema de aprovisionamiento y diagnóstico de infraestructura, con el fin de estandarizar la configuración para las distintas aplicaciones.

Los siguientes son los componentes con los que contará la arquitectura del sistema:

- 1- **Servidor de Base de Datos:** Aquí se almacenarán todas las configuraciones del sistema de monitoreo y todos los incidentes que han sido notificados, de esta forma se podrá contar con un historial.
- 2- **Servidor de Recolección de Datos:** Este servidor contendrá los scripts estandarizados para la recolección de datos de los diferentes servidores de la infraestructura de Amdocs a través de conexiones por SSH, también será responsable de ejecutar las tareas programadas con las cuales se realizará el monitoreo, el envío de notificaciones en forma de alertas y registrará cada uno de los incidentes en la base de datos.
- 3- **Servidor Web Apache Tomcat:** Este servidor va a tener instalada la aplicación que ha sido desarrollada en Java y HTML para el manejo de la interfaz gráfica del sistema de monitoreo, el personal de Amdocs podrá acceder a esta, siempre y cuando se encuentre en la red local o esté utilizando un acceso remoto por medio de una VPN.

La figura 21 contiene el diagrama de la arquitectura que utilizará el sistema propuesto:

Figura 21. Arquitectura del Sistema



Fuente: Elaboración propia, 2017

### 5.1.3.1 Requisitos técnicos

A continuación, se mostrará en la tabla 39 los requisitos técnicos que necesitará el sistema para ser ejecutado de forma eficiente:

Tabla 39. Requisitos técnicos

Requisito	Nombre	Versión
Sistema Operativo	AIX	5.3
Servidor Web	Apache Tomcat	8
Base de datos	Oracle	10g
Otros	Java	8

Fuente: Elaboración propia, 2017

La propuesta del sistema no necesitará la instalación de agentes en los equipos para poder funcionar, sin embargo, sí será necesario realizar los siguientes pasos, que son funciones nativas de UNIX:

- 1. Creación de un usuario de monitoreo:** Todos los servidores van a necesitar crear un usuario de monitoreo que será necesario para realizar las conexiones a través de SSH.
- 2. Creación de llaves públicas:** El protocolo SSH tiene la funcionalidad de crear llaves públicas entre servidores, con el objetivo de poder acceder entre ellos sin recurrir a una contraseña, esta es encriptada y se utilizará con los usuarios de monitoreo.
- 3. Instalación de cliente Oracle:** El servidor donde se instalará la aplicación necesitará un cliente Oracle para poder realizar el acceso a la base de datos configurando el archivo "tnsnames.ora".

#### **5.1.4 Estructuración de la base de datos**

El sistema propuesto contará con un total de 25 tablas en la base de datos que ha sido normalizada a la tercera forma para evitar redundancia, disminuir problemas de actualización en las tablas y proteger la integridad de los datos.

La base de datos se utilizará para registrar los incidentes que han sido notificados a través de alertas y también para almacenar la configuración del sistema de aseguramiento y diagnóstico de infraestructura.

La tabla 40 mostrará el nombre y la descripción de cada una de las tablas que serán propuestas en el nuevo sistema de monitoreo.

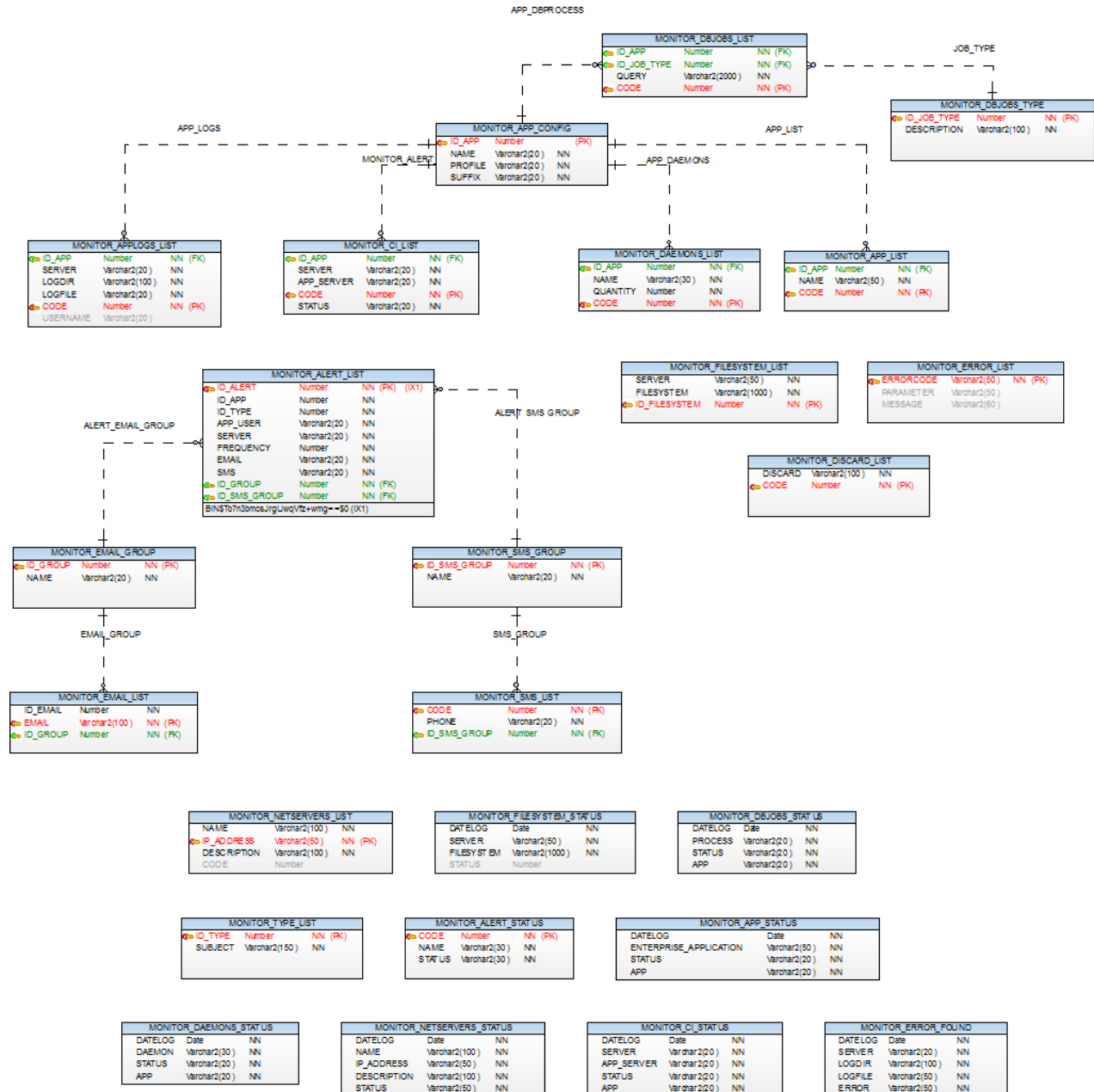
Tabla 40. Descripción de tablas en base de datos

TABLA	DESCRIPCIÓN
MONITOR_TYPE_LIST	Tabla que contiene la configuración de los tipos de alerta del monitoreo.
MONITOR_ALERT_LIST	Tabla que contiene las alertas que serán ejecutadas.
MONITOR_ALERT_STATUS	Tabla que contiene el estado de las alertas por aplicación.
MONITOR_APPLOGS_LIST	Tabla que contiene el servidor, directorio y archivo que se desea notificar errores.
MONITOR_APP_CONFIG	Tabla que contiene la configuración de la aplicación de servicio.
MONITOR_APP_LIST	Tabla que contiene configuradas las aplicaciones empresariales de WebSphere.
MONITOR_APP_STATUS	Tabla que el historial del estado de las aplicaciones empresariales de WebSphere.
MONITOR_CI_LIST	Tabla que contiene la configuración de los servidores de aplicación de WebSphere.
MONITOR_CI_STATUS	Tabla que contiene el historial del estado de los servidores de aplicación de WebSphere.
MONITOR_DAEMON_LIST	Tabla que contiene la configuración de los procesos de Unix a ser monitoreados.
MONITOR_DAEMON_STATUS	Tabla que contiene el historial del estado de los procesos de Unix.
MONITOR_DBJOBS_LIST	Tabla que contiene la consulta de las tareas que deben ser monitoreadas.
MONITOR_DBJOBS_STATUS	Tabla que contiene el historial del estado de las tareas.
MONITOR_DBJOBS_TYPE	Tabla que contiene la configuración del tipo de tareas.
MONITOR_DISCARD_LIST	Tabla que contiene la configuración de los valores que deben ser ignorados en el monitoreo de errores.
MONITOR_EMAIL_GROUP	Tabla que contiene la configuración de los grupos de correo electrónico que recibirán alertas.
MONITOR_EMAIL_LIST	Tabla que contiene los correos electrónicos asociados a un número de grupo de correo electrónico.
MONITOR_ERROR_FOUND	Tabla que contiene el historial de errores encontrados.
MONITOR_ERROR_LIST	Tabla que contiene la configuración de los errores que deben ser monitoreados.
MONITOR_FILESYSTEM_LIST	Tabla que contiene la configuración de los sistemas de archivos que deber ser monitoreados.
MONITOR_FILESYSTEM_STATUS	Tabla que contiene el historial del estado de uso en almacenamiento de los sistemas de archivos.
MONITOR_NETSERVER_LIST	Tabla que contiene la configuración de los servidores y dispositivos físicos que deben ser accesibles en la red.
MONITOR_NETSERVER_STATUS	Tabla que contiene el historial del estado de conectividad de los servidores y dispositivos físicos en la red.
MONITOR_SMS_GROUP	Tabla que contiene la configuración de los grupos de SMS que recibirán notificaciones.
MONITOR_SMS_LIST	Tabla que contiene la configuración de los números de teléfono asociados a un grupo de SMS.

Fuente: Elaboración propia, 2017

La figura 22 presentará el modelado de las tablas en la base de datos con sus respectivas relaciones y atributos.

Figura 22. Modelado de Base de datos



Fuente: Elaboración propia, 2017

## 5.2 Prototipo del sistema

### 5.2.1 Definición de módulos

El prototipo del nuevo sistema de aseguramiento y diagnóstico de infraestructura estará compuesto por 11 módulos, los cuales contarán con funciones relacionados con configuración del sistema, alertas y consulta de los registros históricos de incidentes.

A continuación, se procederá a explicar cada uno de los módulos que conforman el prototipo.

#### 5.2.1.1 Módulo de Configuración del Sistema de Monitoreo

Este módulo será dividido en seis sub módulos que permitirán configurar cada uno de los parámetros necesarios para realizar la configuración de las alertas y enviar notificaciones cada vez que un incidente se presenta en la infraestructura.

##### 5.2.1.1.1 Sub módulo de configuración de aplicación de servicio

Este sub módulo se utilizará para configurar los datos relacionados con la aplicación de servicio que podría ser afectado por un incidente en la infraestructura.

En la tabla 41 se describirán los parámetros que deberán ser configurados:

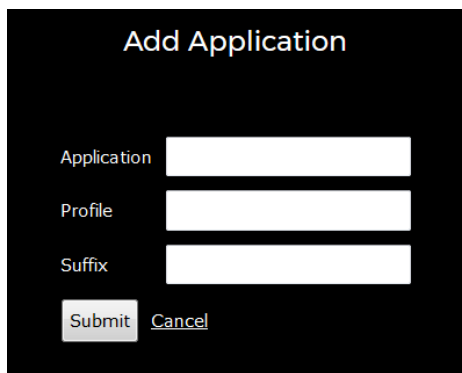
Tabla 41. Sub módulo de configuración de aplicación de servicio

Nombre	Descripción
Aplicación	Se ingresará el nombre de la aplicación de servicio.
Perfil	Se ingresará el nombre del perfil de WebSphere donde la aplicación es administrada.
Sufijo	Se ingresará el sufijo utilizado para denominar a la aplicación de servicio.

Fuente: Elaboración propia, 2017

La figura 23 se podrá visualizar el sub módulo de configuración del sistema de monitoreo en el prototipo:

Figura 23. Su módulo de configuración del sistema de monitoreo



The image shows a dark-themed user interface for adding an application. At the top, the title 'Add Application' is centered in white. Below the title, there are three white input fields stacked vertically, labeled 'Application', 'Profile', and 'Suffix' on the left. At the bottom left, there is a white 'Submit' button, and to its right is a white 'Cancel' button with a blue underline.

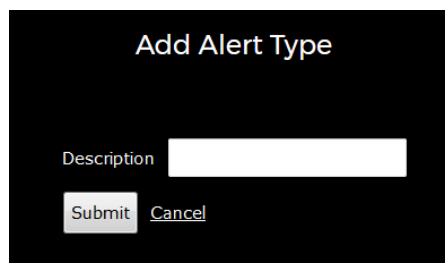
Fuente: Elaboración propia, 2017

#### 5.2.1.1.2 Sub módulo de configuración de tipo de alerta

Este sub módulo permitirá crear los diferentes tipos de alertas que serán utilizados para monitorear la infraestructura, se agregará una descripción por tipo el cual será agregado a cada una de las notificaciones.

El sistema solo necesitará una descripción como parámetro de configuración, en la figura 24 se podrá apreciar cómo se podrá visualizar este sub módulo en el sistema.

Figura 24. Sub módulo de configuración de tipo de alerta



The image shows a dark-themed user interface for adding an alert type. At the top, the title 'Add Alert Type' is centered in white. Below the title, there is a single white input field labeled 'Description' on the left. At the bottom left, there is a white 'Submit' button, and to its right is a white 'Cancel' button with a blue underline.

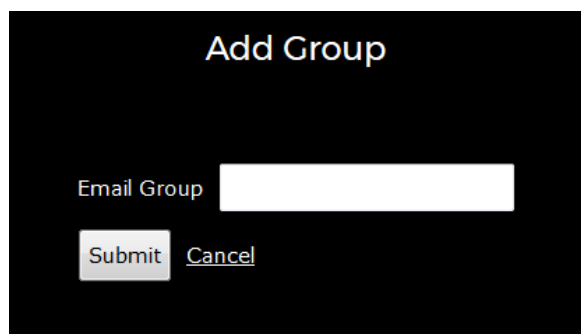
Fuente: Elaboración propia, 2017

### 5.2.1.1.3 Sub módulo de configuración de grupo de correo electrónico

Este sub módulo será utilizado para configurar distintos grupos de correo electrónico para enviar alertas a los miembros que componen dicho grupo. La idea de usar grupos de correo electrónico es garantizar que las alertas serán enviadas a personas de interés en resolver el incidente y evitar notificaciones no deseadas.

Para configurar el grupo de correo electrónico bastará con agregar un nombre de grupo que no esté en uso, la figura 25 mostrará este sub módulo en el sistema.

Figura 25. Sub módulo de configuración de correo electrónico



The image shows a dark-themed user interface for adding a new email group. At the top, the text "Add Group" is centered. Below this, the label "Email Group" is positioned to the left of a white rectangular input field. At the bottom left of the form area, there is a "Submit" button, and to its right is a "Cancel" button with a blue underline.

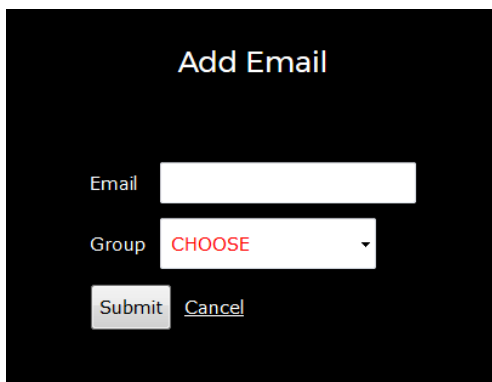
Fuente: Elaboración propia, 2017

### 5.2.1.1.4 Sub módulo de configuración de lista de correo

Este sub módulo será utilizado para agregar cada uno de los correos electrónicos de las personas interesadas a recibir una notificación, el correo estará vinculado a un grupo de correo electrónico de acuerdo al tipo de alerta que desea recibir.

Los parámetros de configuración de este sub módulo serán el correo electrónico deseado y se deberá seleccionar el grupo al que va a pertenecer como se apreciará en la figura 26.

Figura 26. Sub módulo de configuración de lista de correo



The screenshot shows a form titled "Add Email" with a black background. It contains two input fields: "Email" with a white text box, and "Group" with a dropdown menu showing "CHOOSE" in red text. Below the fields are two buttons: "Submit" and "Cancel".

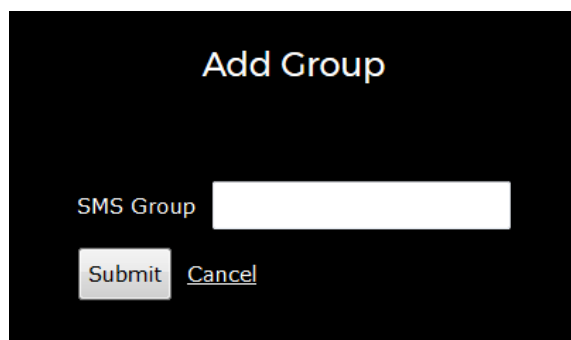
Fuente: Elaboración propia, 2017

#### 5.2.1.1.5 Sub módulo de configuración de grupo de SMS

Este módulo será utilizado para configurar varios grupos de SMS para el envío de notificaciones de incidentes a través de mensajería de texto móvil, su principal objetivo es que los miembros de dicho grupo reciban una alerta lo más pronto posible para poder solventar el incidente suscitado.

La figura 27 mostrará el único parámetro de configuración que se necesitará para crear el grupo el cual es un nombre que lo identifique y no exista en el sistema.

Figura 27. Sub módulo de configuración de grupo SMS



The screenshot shows a form titled "Add Group" with a black background. It contains one input field: "SMS Group" with a white text box. Below the field are two buttons: "Submit" and "Cancel".

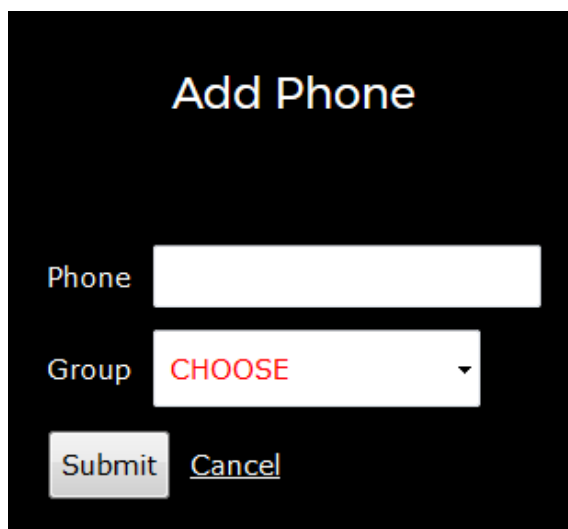
Fuente: Elaboración propia, 2017

#### 5.2.1.1.6 Sub módulo de configuración de lista de SMS

Este módulo será utilizado para crear las listas de SMS con los números de teléfono celular de las personas interesadas a recibir una notificación por mensajería de texto móvil, además se deberá seleccionar el tipo de grupo al cual será miembro de acuerdo al tipo de alerta que desea recibir.

En la figura 28 se podrá observar cómo se configurará un nuevo número de teléfono.

Figura 28. Sub módulo de configuración de lista de SMS



The image shows a dark-themed user interface for adding a phone number. At the top, the title "Add Phone" is displayed in white. Below the title, there are two input fields: a text box labeled "Phone" and a dropdown menu labeled "Group" with the word "CHOOSE" in red text. At the bottom of the form, there are two buttons: a grey "Submit" button and a white "Cancel" button with a red underline.

Fuente: Elaboración propia, 2017

### 5.2.1.2 Módulo de configuración de servidor de aplicación

El siguiente módulo estará destinado a la configuración de los servidores de aplicación utilizados por WebSphere para ejecutar distintas aplicaciones dentro de la infraestructura, en la tabla 42 se podrán observar los parámetros de configuración.

Tabla 42. Parámetros de configuración para monitoreo del servidor de aplicación

Nombre	Descripción
Aplicación	Se deberá seleccionar la aplicación de servicio.
Servidor	Se deberá ingresar el nombre del servidor físico donde se encuentra ubicado.
Servidor de aplicación	Se deberá ingresar el nombre del servidor de aplicación en WebSphere.
Estado	Se deberá seleccionar el estado de las notificaciones por alertas en caso de no querer recibirlas cuando un servidor está detenido.

Fuente: Elaboración propia, 2017

En la figura 29 se podrá observar cómo se agregará un nuevo servidor de aplicación en el sistema.

Figura 29. Módulo de configuración de servidor de aplicación

The screenshot shows a form titled "Add Application Server" with the following fields:

- Application:** A dropdown menu with the text "CHOOSE" and a downward arrow.
- Server:** A text input field.
- Application server:** A text input field.
- Status:** A dropdown menu with the text "CHOOSE" and a downward arrow.

At the bottom of the form, there are two buttons: "Submit" and "Cancel".

Fuente: Elaboración propia, 2017

### 5.2.1.2.1 Sub módulo para visualizar eventos en servidores de aplicación

Este sub módulo mostrará el histórico de eventos que han sucedido a los servidores de aplicación cada vez que un incidente se presenta, no posee parámetros de configuración.

La figura 30 mostrará la forma en que se visualizarán los eventos.

Figura 30. Sub módulo para visualizar eventos en servidores de aplicación

Configuration Item Events				
Date	Server	Application server	Status	Application
19/07/2017:15:36:28	app4	appserver04	DOWN	Enrutador
19/07/2017:15:36:28	app3	appserver03	DOWN	Enrutador
18/07/2017:14:59:23	app4	appserver04	DOWN	Enrutador
18/07/2017:14:59:23	app3	appserver03	DOWN	Enrutador

Fuente: Elaboración propia, 2017

### 5.2.1.3 Módulo de configuración de aplicación empresarial

El siguiente módulo servirá para configurar las distintas aplicaciones empresariales que posee la empresa y que se encuentran instaladas en WebSphere, este módulo permitirá monitorear si las aplicaciones se encuentran iniciadas.

El módulo necesitará de 2 parámetros de configuración donde se deberá seleccionar la aplicación de servicio e ingresar el nombre de la aplicación empresarial por monitorear.

La figura 31 mostrará la forma en que se configura una aplicación empresarial.

Figura 31. Módulo de configuración de aplicación empresarial

Fuente: Elaboración propia, 2017

#### 5.2.1.3.1 Sub módulo para visualizar eventos en aplicaciones empresariales

Este sub módulo mostrará el histórico de eventos que han sucedido a las aplicaciones empresariales cada vez que un incidente se presenta, no posee parámetros de configuración.

La figura 32 mostrará la forma en que se visualizarán los eventos.

Figura 32. Sub módulo para visualizar eventos en aplicaciones empresariales

Datelog	Enterprise_application	Status	App
09/05/2017:15:09:06	Enterprise Application	DOWN	App
09/05/2017:14:58:36	Enterprise Application	DOWN	App
05/05/2017:11:21:27	Enterprise Application	DOWN	App
03/05/2017:14:19:29	Enterprise Application	DOWN	App

Fuente: Elaboración propia, 2017

#### 5.2.1.4 Módulo de configuración de errores

El módulo permitirá agregar los errores que se presentan en los servidores donde se ejecutan las aplicaciones empresariales para así ser notificados por medio de alertas, estas se configurarán de acuerdo a los siguientes parámetros presentes en la tabla 43:

Tabla 43. Configuración de Errores

Nombre	Descripción
Código de Error	Código de error establecido por una aplicación conocida, por ejemplo código de error de Oracle o WebSphere.
Parámetro	Parámetro para será utilizado para filtrar la búsqueda y obtener un mejor resultado, no será un campo obligatorio.
Mensaje	Descripción que estará en el cuerpo de la alerta por correo electrónico acerca del error encontrado.

Fuente: Elaboración propia, 2017

En la figura 33 se podrá observar cómo se configurará un error en el sistema.

Figura 33. Módulo de configuración de errores

The image shows a web form titled "Add Error" on a black background. The form contains three input fields: "Errorcode", "Parameter", and "Message". Below the input fields are two buttons: "Submit" and "Cancel".

Fuente: Elaboración propia, 2017

#### 5.2.1.4.1 Sub módulo de configuración de archivo y directorio de errores

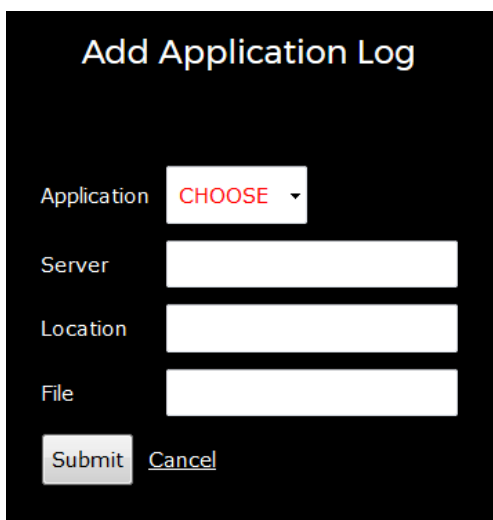
Este sub módulo permitirá configurar el nombre de los archivos y su ubicación de los cuales se desea monitorear cuando se presenta un error en el servidor para así poder ser notificado a través de una alerta.

Para realizar la configuración será necesario seguir los siguientes pasos:

- Seleccionar la aplicación a la cual se encuentra vinculado el archivo por monitorear.
- Ingresar el nombre o la dirección IP del servidor que desea monitorear.
- Ingresar la ruta de la ubicación donde se encuentra el archivo.
- Ingresar el nombre del archivo que desea ser monitoreado.

La figura 34 mostrará la forma en la cual se realizará la configuración de un archivo al cuales se desea notificar los errores encontrados.

Figura 34. Sub módulo de configuración de archivo y directorio de errores



The image shows a screenshot of a web form titled "Add Application Log". The form is set against a dark background with white text and input fields. It contains four labeled input fields: "Application" with a dropdown menu showing "CHOOSE", "Server", "Location", and "File", each with a corresponding white input box. At the bottom of the form, there are two buttons: "Submit" and "Cancel".

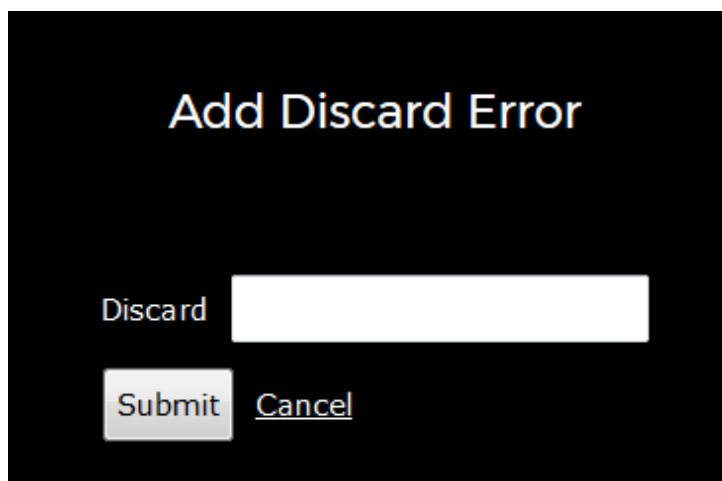
Fuente: Elaboración propia, 2017

#### 5.2.1.4.2 Sub módulo de configuración para descartar errores

La función de este sub módulo será crear una lista de parámetros que serán descartados en la búsqueda de errores para evitar falsas alertas y no alterar los errores que sí deben ser notificados, debido a que algunos componentes poseen el mismo código de error, pero una descripción distinta y suelen intervenir con el buen funcionamiento del sistema.

Para realizar la configuración solo basta con ingresar el parámetro que se desea omitir y será agregado a la lista de descarte, en la figura 35 se podrá observar la forma en que se agregará al sistema.

Figura 35. Sub módulo de configuración para descartar errores



The image shows a screenshot of a web form titled "Add Discard Error". The form has a black background with white text. It contains a label "Discard" followed by a white rectangular input field. Below the input field, there are two buttons: a grey "Submit" button and a blue "Cancel" button with a red underline.

Fuente: Elaboración propia, 2017

### 5.2.1.4.3 Sub módulo para visualizar errores encontrados

Este sub módulo permitirá al usuario visualizar un histórico de todos los errores que han sido encontrados.

En la figura 36 se podrá observar la forma en que se visualizará en pantalla los errores encontrados.

Figura 36. Sub módulo para visualizar errores encontrados

Error Found				
Date	Server	Location	File	Error
27/06/2017:16:57:40	server1	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server2	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server3	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server4	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server5	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server6	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server7	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server8	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server9	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server10	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server11	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server12	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server13	/opt/IBM/WebSphere/logs	SystemOut.log	ORA-00001
27/06/2017:16:57:40	server14	/opt/IBM/WebSphere/logs	*.txt	ORA-00001

Fuente: Elaboración propia, 2017

### 5.2.1.5 Módulo de configuración de tareas

El siguiente módulo permitirá configurar tareas específicas que serán monitoreados por medio del estado de ejecución en el que se encuentran, para esto el módulo se dividirá en 3 sub procesos que son los siguientes:

- Sub módulo de configuración de tipo de tarea.
- Sub módulo de configuración de tarea.

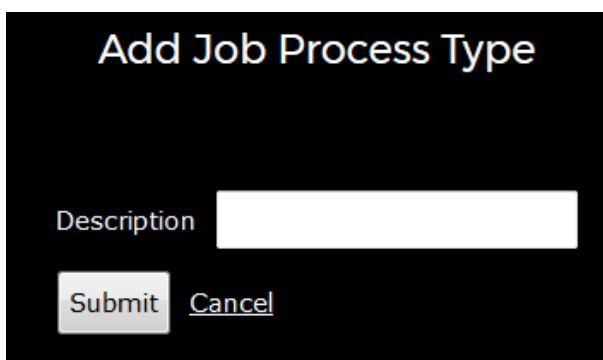
- Sub módulo de visualización de eventos de tareas.

#### 5.2.1.5.1 Sub módulo de configuración de tipo de tarea

Este sub módulo permitirá agregar un tipo de tarea que se desea monitorear, será utilizado para vincular las tareas con una descripción.

Para crear un tipo de tarea será necesario ingresar un parámetro el cual será una descripción de la misma, en la figura 37 se podrá observar la configuración.

Figura 37. Sub módulo de configuración de tipo de tarea



Fuente: Elaboración propia, 2017

#### 5.2.1.5.2 Sub módulo de configuración de tarea

Este sub módulo será utilizado para crear la consulta de base de datos que verificará el estado de la tarea que se desea monitorear, además vinculará el tipo de tarea del cual esta consiste y así podrá realizar alertas por medio de notificaciones si el estado es diferente a “iniciado”.

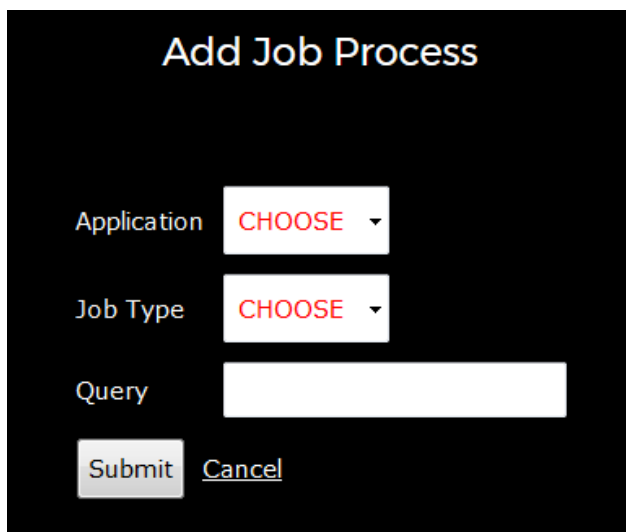
Los pasos para configurar este sub módulo serán los siguientes:

- Seleccionar la aplicación a quién pertenece la tarea.
- Seleccionar el tipo de tarea al cual se encuentra vinculado.

- Ingresar la consulta de base de datos para verificar si el estado de la tarea es iniciado.

En la figura 38 se podrá observar la forma en que se configurará la tarea en el sistema.

Figura 38. Sub módulo de configuración de la tarea



The image shows a screenshot of a web form titled "Add Job Process". The form is set against a black background. It includes three input fields: "Application" with a dropdown menu showing "CHOOSE", "Job Type" with a dropdown menu showing "CHOOSE", and "Query" with a text input field. At the bottom, there are two buttons: "Submit" and "Cancel".

Fuente: Elaboración propia, 2017

### 5.2.1.5.3 Sub módulo para visualizar los eventos de las tareas

Este sub módulo permitirá mostrar un histórico de incidentes cuando una tarea se encuentra en un estado "iniciado", esta mostrará la fecha, el nombre de la tarea, el estado en que se encuentra y la aplicación a la cual se pertenece.

En la figura 39 se podrá observar cómo se visualizarán los eventos en el sistema.

Figura 39. Sub módulo para visualizar los eventos de las tareas

Job Process Events			
Date	Process	Status	Application
19/07/2017:15:35:33	bb	BL	app1
18/07/2017:14:58:26	bb	BL	app1
28/06/2017:18:40:36	bb	BL	app1
27/06/2017:16:51:06	bb	BL	app1
27/06/2017:16:09:10	bb	BL	app2
27/06/2017:14:29:35	bb	BL	app1
26/06/2017:15:22:31	bb	BL	app2
23/06/2017:16:20:11	bb	BL	app2
23/06/2017:15:50:58	bb	BL	app2
21/06/2017:17:09:59	bb	BL	app2
21/06/2017:16:42:51	bb	BL	app3
21/06/2017:16:33:03	bb	BL	app3
09/06/2017:15:30:35	bb	BL	app3
30/05/2017:17:44:12	bb	BL	app3

Fuente: Elaboración propia, 2017

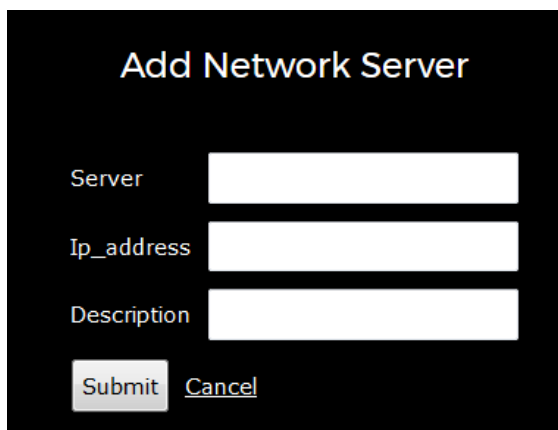
#### 5.2.1.6 Módulo de configuración de acceso a la red

El siguiente módulo permitirá agregar diferentes servidores y así monitorear su conectividad en la red, para ello será necesario ingresar lo siguientes parámetros al sistema:

- Nombre del servidor.
- Dirección IP del servidor.
- Descripción del servidor.

En la figura 40 se podrá ver como se agregar un servidor para verificar su conectividad en el sistema.

Figura 40. Módulo de configuración de acceso a la red



**Add Network Server**

Server

Ip\_address

Description

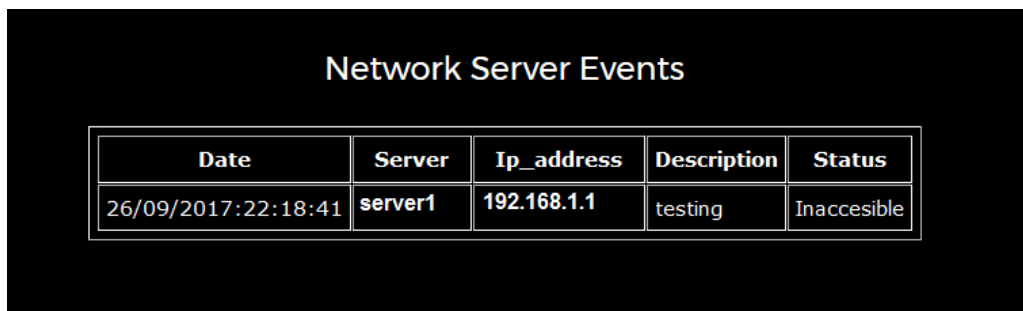
Fuente: Elaboración propia, 2017

#### 5.2.1.6.1 Sub módulo de visualizar los eventos de acceso en la red

Este sub módulo permitirá visualizar un histórico con los incidentes cuando un servidor no es accesible en la red.

La figura 41 mostrará la forma en que se podrá visualizar en el sistema.

Figura 41. Sub módulo para visualizar los eventos de acceso en la red



**Network Server Events**

Date	Server	Ip_address	Description	Status
26/09/2017:22:18:41	server1	192.168.1.1	testing	Inaccesible

Fuente: Elaboración propia, 2017

### 5.2.1.7 Módulo de configuración de procesos

La función del siguiente módulo será configurar procesos que se encuentran en el sistema operativo ligados a una aplicación específica y que deben estar en ejecución, por lo cual se deberá establecer los siguientes parámetros de la tabla 44 en la configuración del sistema de monitoreo.

Tabla 44. Parámetros del módulo de configuración de procesos

Nombre	Descripción
Aplicación	Se seleccionará la aplicación a la cual se encuentra vinculado el proceso.
Demonio	Los procesos son denominados demonios en Unix, se deberá ingresar el nombre del proceso que se desea monitorear.
Cantidad	Se deberá ingresar un número con la cantidad de procesos que deben estar en ejecución.

Fuente: Elaboración propia, 2017

La figura 42 mostrará la pantalla donde se configurará el proceso que debe ser monitoreado.

Figura 42. Módulo de configuración de procesos

The image shows a screenshot of a web-based configuration form titled "Add Daemon". The form is set against a black background with white text and input elements. It contains three main input fields: "Application" with a dropdown menu showing "CHOOSE", "Daemon" with a standard text input box, and "Quantity" with a spinner control. At the bottom of the form, there are two buttons: "Submit" and "Cancel".

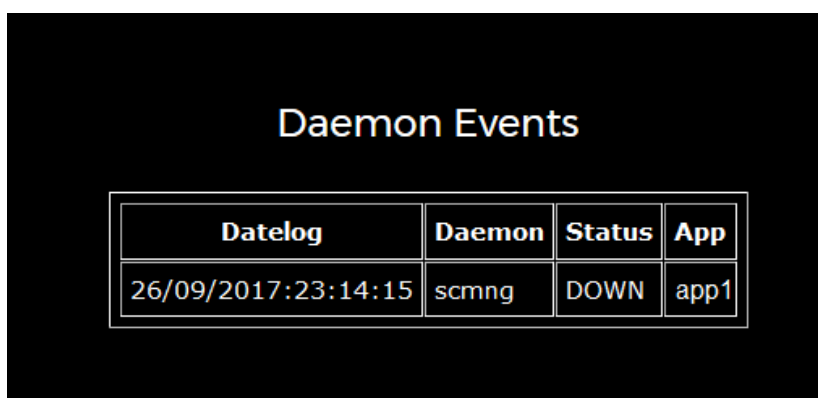
Fuente: Elaboración propia, 2017

### 5.2.1.7.1 Sub módulo para visualizar los eventos de los procesos

Este sub módulo permitirá mostrar en pantalla un histórico de los incidentes que han sido notificados cuando un proceso no está en ejecución.

La figura 43 mostrará la forma en la que se podrá observar el histórico de los procesos que han sido notificados.

Figura 43. Sub módulo para visualizar los eventos de los procesos



Datelog	Daemon	Status	App
26/09/2017:23:14:15	scmng	DOWN	app1

Fuente: Elaboración propia, 2017

### 5.2.1.8 Módulo de configuración de almacenamiento

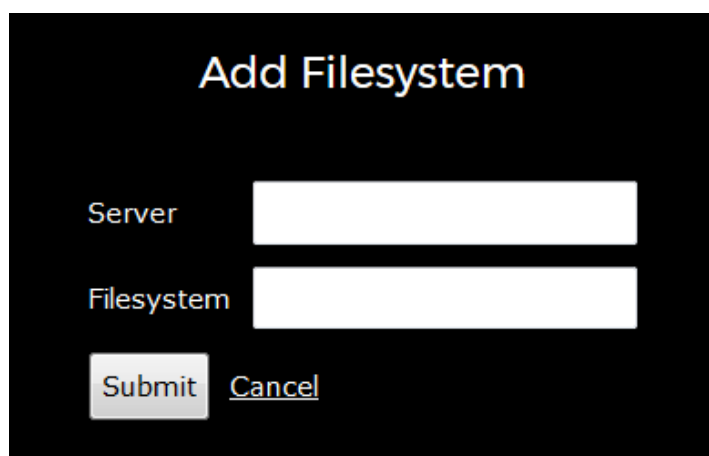
El siguiente módulo permitirá configurar los servidores y los sistemas de archivos que deben ser notificados cuando han excedido el porcentaje en el umbral de uso permitido.

Para realizar la configuración será necesario ingresar los siguientes parámetros en el sistema:

- Nombre del servidor.
- Ruta del sistema de archivos que se desea configurar.

En la figura 44 se podrá observar la pantalla en la cual se agregará una nueva configuración de almacenamiento.

Figura 44. Módulo de configuración de almacenamiento



The image shows a screenshot of a software interface titled "Add Filesystem". The interface is set against a black background with white text and elements. At the top center, the title "Add Filesystem" is displayed in a large, bold, white font. Below the title, there are two input fields. The first is labeled "Server" and the second is labeled "Filesystem", both in white text. Each label is positioned to the left of a white rectangular input box. At the bottom of the interface, there are two buttons: a solid white button labeled "Submit" and a white button with a black outline labeled "Cancel".

Fuente: Elaboración propia, 2017

#### 5.2.1.8.1 Sub módulo para visualizar eventos de almacenamiento

Este sub módulo mostrará en pantalla el histórico de incidentes notificados en relación con un sistema de archivos que ha excedido el umbral de uso.

En la figura 45 se podrá apreciar la información que se podrá visualizar en la pantalla del sistema.

Figura 45. Sub módulo para visualizar eventos de almacenamiento

### Filesystem Events

Date	Server	Filesystem	Status
19/07/2017:15:35:36	server1	/usr	91%
19/07/2017:15:12:57	server1	/usr	91%
19/07/2017:12:33:05	server1	/usr	91%
18/07/2017:14:58:28	server1	/usr	91%
04/07/2017:18:38:53	server1	/usr	90%
04/07/2017:18:34:13	server1	/usr	90%
04/07/2017:15:42:52	server2	/usr	90%
04/07/2017:15:28:04	server2	/usr	90%
04/07/2017:15:22:50	server2	/usr	90%
29/06/2017:17:06:59	server2	/usr	90%
29/06/2017:17:02:03	server3	/usr	90%
29/06/2017:16:56:42	server3	/usr	90%
29/06/2017:16:42:14	server3	/usr	90%
23/06/2017:16:21:55	server3	/usr	89%
23/06/2017:15:52:43	server3	/usr	89%

Fuente: Elaboración propia, 2017

### 5.2.1.9 Módulo de configuración de alertas

El siguiente módulo permitirá al usuario crear una lista de alertas que estarán siendo ejecutadas en el sistema, utilizando las configuraciones de los componentes que deben ser monitoreados en la infraestructura.

La tabla 45 tendrá una descripción de cada uno de los parámetros necesarios para configurar una alerta en el sistema.

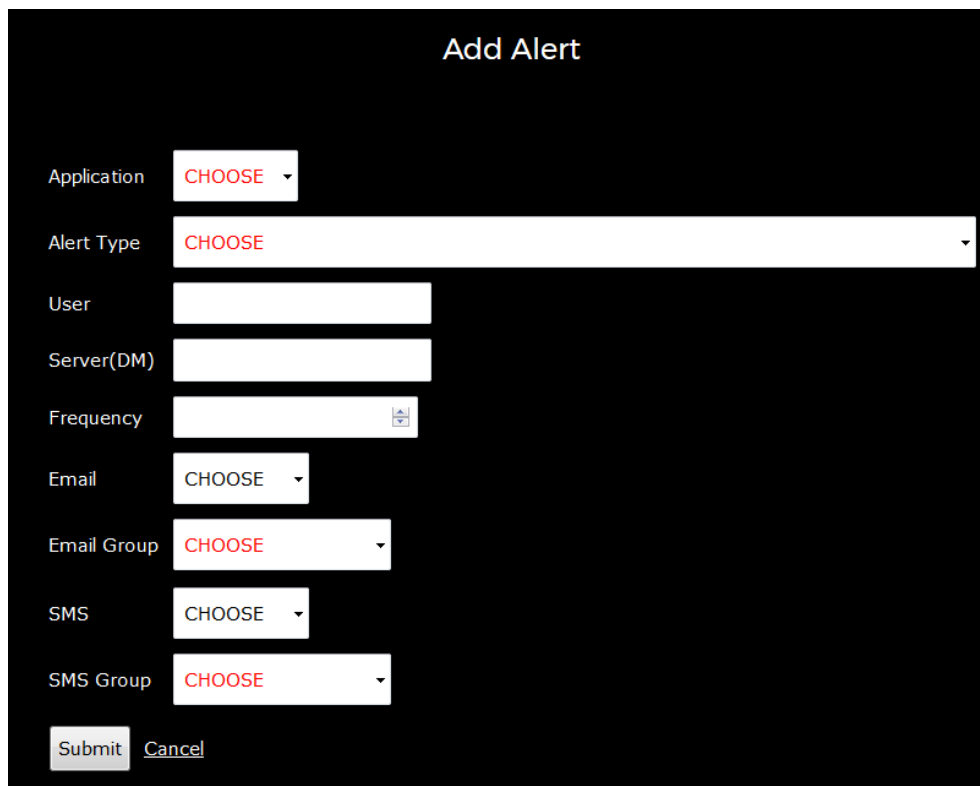
Tabla 45. Parámetros de configuración de alertas

<b>Nombre</b>	<b>Descripción</b>
Aplicación	Se seleccionará la aplicación de servicio a la cual estará asociada la alerta.
Tipo de alerta	Se seleccionará el tipo de alerta que será notificado.
Usuario	Se deberá ingresar el usuario de Unix para recolección de datos.
Servidor	Se deberá ingresar el nombre del servidor principal donde se recolectan los datos.
Frecuencia	Se deberá ingresar la frecuencia de envío de alertas cuando se presenta un mismo incidente.
Correo	Se seleccionará si se desea habilitar o deshabilitar la alerta por correo electrónico.
Grupo de correo	Se seleccionará el grupo de correo electrónico a quienes se les enviará las alertas.
SMS	Se seleccionará si se desea habilitar o deshabilitar la alerta por mensajería de texto móvil.
Grupo de SMS	Se seleccionará el grupo de SMS a quienes se les enviará las alertas por mensajería de texto móvil.

Fuente: Elaboración propia, 2017

En la figura 46 se mostrará la pantalla de configuración de una nueva alerta.

Figura 46. Módulo de configuración de alertas



The image shows a screenshot of a web application interface titled "Add Alert". The form is set against a dark background and contains the following fields:

- Application:** A dropdown menu with "CHOOSE" selected.
- Alert Type:** A wide dropdown menu with "CHOOSE" selected.
- User:** A text input field.
- Server(DM):** A text input field.
- Frequency:** A text input field with a calendar icon on the right.
- Email:** A dropdown menu with "CHOOSE" selected.
- Email Group:** A dropdown menu with "CHOOSE" selected.
- SMS:** A dropdown menu with "CHOOSE" selected.
- SMS Group:** A dropdown menu with "CHOOSE" selected.

At the bottom left of the form, there are two buttons: "Submit" and "Cancel".

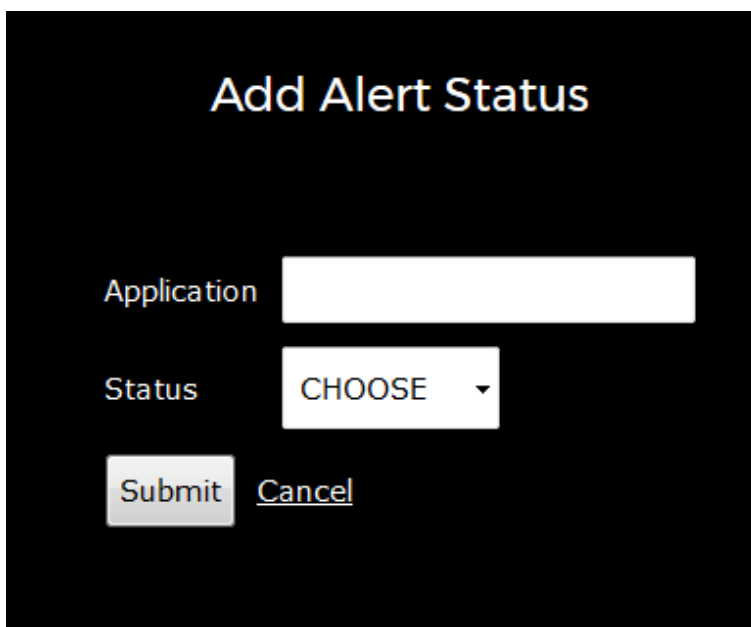
Fuente: Elaboración propia, 2017

#### 5.2.1.10 Módulo para configurar el estado de las alertas

El siguiente módulo permitirá habilitar o deshabilitar todas las alertas relacionadas con una aplicación de servicio en específico.

El módulo permitirá agregar aplicaciones para seleccionar el estado en habilitado o deshabilitado en caso de ser requerido por el usuario como se muestra en la figura 47.

Figura 47. Módulo para configurar el estado de las alertas



The image shows a web form titled "Add Alert Status" on a black background. The form includes the following elements:

- A text input field labeled "Application".
- A dropdown menu labeled "Status" with the text "CHOOSE" and a downward arrow.
- A button labeled "Submit".
- A link labeled "Cancel".

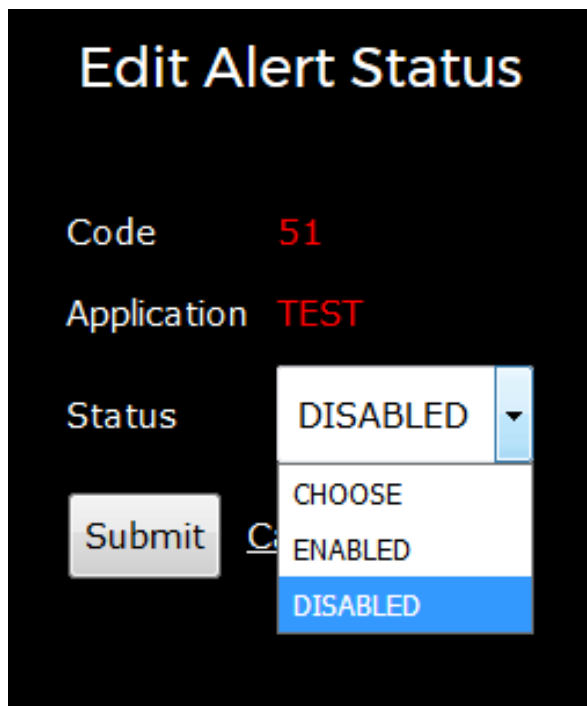
Fuente: Elaboración propia, 2017

#### 5.2.1.10.1 Sub módulo para cambiar estado de las alertas

Este sub módulo habilitará o deshabilitará las alertas que han sido configurados en caso de que se necesite detener el envío de notificaciones y la reanudación de las mismas.

Para configurar el estado de la alerta para una aplicación de servicio será solo necesario seleccionar el estado de "habilitado" o "deshabilitado" como se podrá observar en la figura 48.

Figura 48. Sub módulo para configurar estado de las alertas



**Edit Alert Status**

Code **51**

Application **TEST**

Status **DISABLED**

Submit

CHOOSE

ENABLED

DISABLED

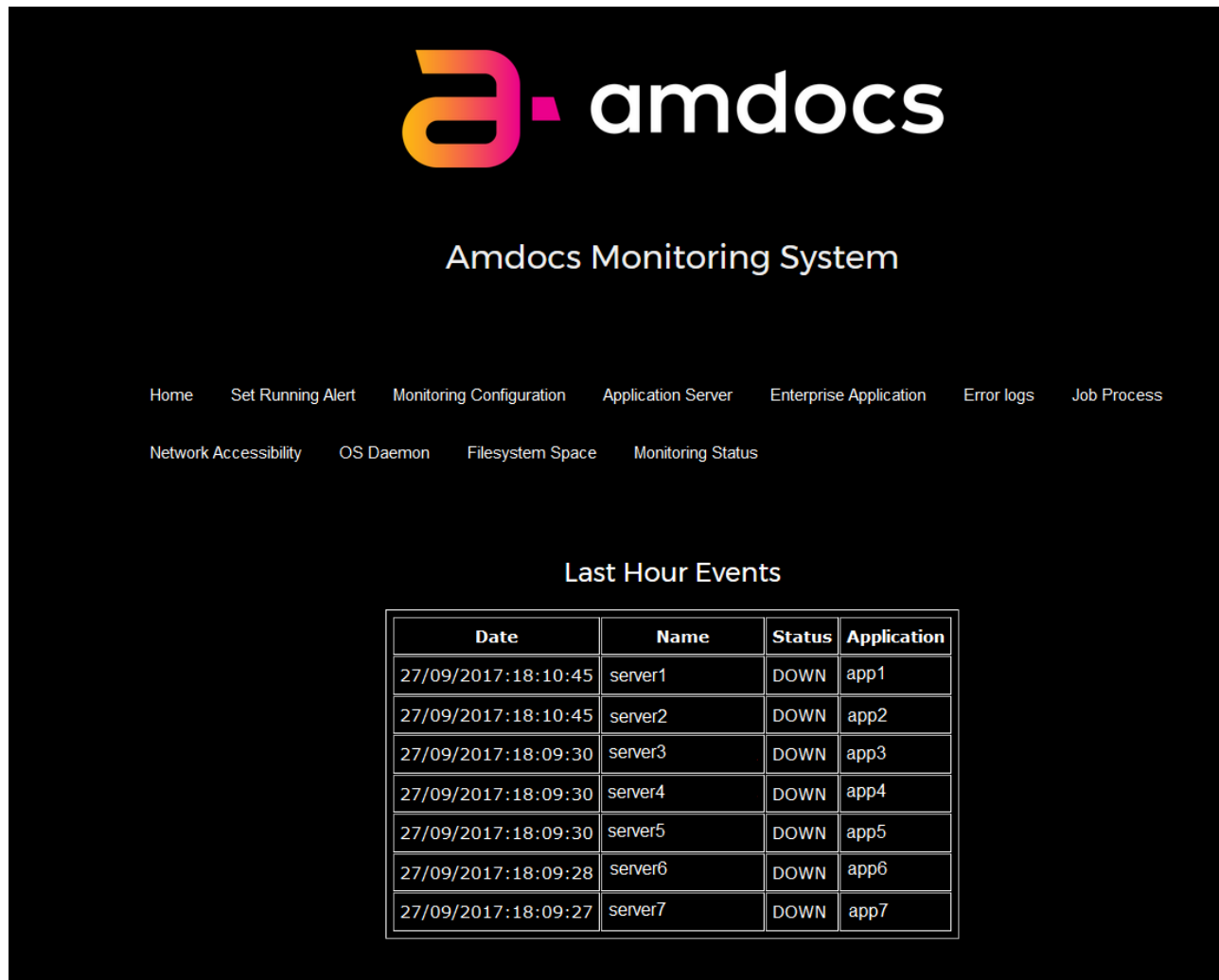
Fuente: Elaboración propia, 2017

#### 5.2.1.11 Módulo para visualizar pantalla principal e incidentes en la última hora

El siguiente módulo permitirá al usuario acceder a todos los módulos anteriores, además visualizar todos los diferentes incidentes que han sucedido en la infraestructura durante la última hora.

En la figura 49 se mostrará la forma en que se podrá observar la pantalla en el sistema.

Figura 49. Módulo de pantalla principal e incidentes en la última hora



The screenshot displays the Amdocs Monitoring System interface. At the top, the Amdocs logo is shown in a stylized orange and pink font. Below the logo, the text 'Amdocs Monitoring System' is centered. A navigation menu is located below the title, containing links for Home, Set Running Alert, Monitoring Configuration, Application Server, Enterprise Application, Error logs, Job Process, Network Accessibility, OS Daemon, Filesystem Space, and Monitoring Status. The main content area is titled 'Last Hour Events' and contains a table with the following data:

Date	Name	Status	Application
27/09/2017:18:10:45	server1	DOWN	app1
27/09/2017:18:10:45	server2	DOWN	app2
27/09/2017:18:09:30	server3	DOWN	app3
27/09/2017:18:09:30	server4	DOWN	app4
27/09/2017:18:09:30	server5	DOWN	app5
27/09/2017:18:09:28	server6	DOWN	app6
27/09/2017:18:09:27	server7	DOWN	app7

Fuente: Elaboración propia, 2017

## **5.2.2 Funcionalidades del sistema**

A continuación se presentarán las funcionalidades con las que contará el sistema para poder realizar el aseguramiento y diagnóstico de toda la infraestructura de la empresa Amdocs Costa Rica.

Dentro de las funcionalidades del sistema se podrá detallar acerca el acceso que esté realizara a los equipos de la infraestructura, el método para la recolección de datos y el registro en una base de datos.

### **5.2.2.1 Enlace de acceso a los servidores de Infraestructura**

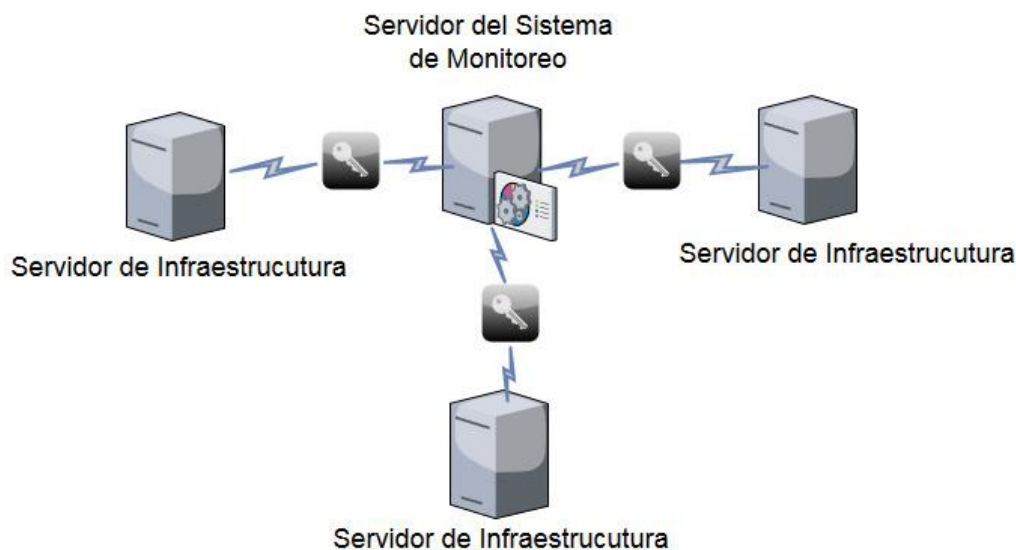
El sistema contará con un servidor principal donde se ubicarán los scripts de configuración y recolección de datos de todos los servidores que serán monitoreados en la infraestructura.

Para acceder a cada uno de los servidores que están siendo monitoreados se necesitará realizar la creación de llave públicas, éstas permitirán la conexión remota del servidor principal hacía todos los servidores sin tener que ingresar una contraseña permitiendo la creación de scripts automatizados.

La creación de llaves públicas de acuerdo a IBM (s.f.), se realiza ejecutando el siguiente comando en el servidor principal “ssh-keygen -t rsa”, este creará un archivo llamado “id\_rsa.pub” con la información del usuario, el servidor y su contraseña de manera encriptada, luego se procederá a copiar el archivo en los servidores donde se necesita acceder y agregar el contenido dentro del archivo “authorized\_keys”.

En la figura 50 se podrá observar el diagrama del enlace de acceso hacia los servidores de la infraestructura, utilizando llaves públicas RSA.

Figura 50. Enlace de acceso a servidores



Fuente: Elaboración propia, 2017

### 5.2.2.2 Estructura de archivos del sistema

El sistema será instalado sobre un sistema operativo Unix y este va contar con la siguiente estructura de archivos que serán utilizados para configuración, ejecución y registros según se detallará en la tabla 46.

Tabla 46. Estructura de archivos del sistema

Directorio	Descripción
lib	Directorio que contendrá las librerías y archivos de propiedades para la configuración del sistema a nivel de sistema operativo.
bin	Directorio que contendrá los archivos que ejecutarán para la recolección de datos, el monitoreo y el envío de alertas.
logs	Directorio que contendrá los registros de ejecución y errores del sistema.
sql	Directorio que contendrá los archivos de consultas de base de datos para la extracción e ingreso de datos.

Fuente: Elaboración propia, 2017

### **5.2.2.3 Funcionamiento del sistema a través de la interfaz web**

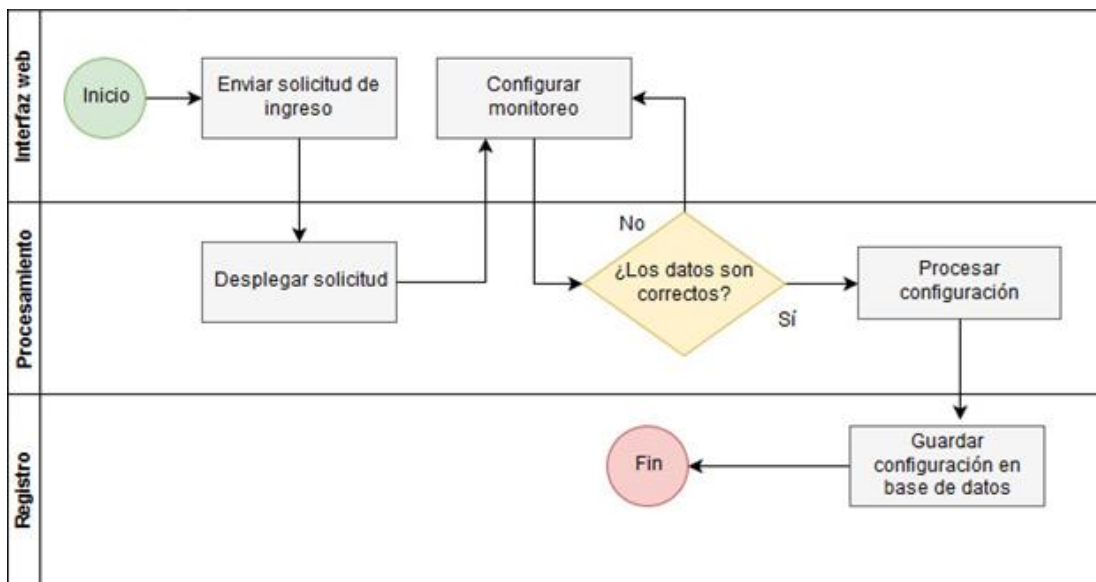
La interfaz web del sistema estará programada en Java y HTML y se encontrará en ejecución en un servidor web apache tomcat, donde se podrá realizar la configuración de las alertas por medio de los módulos para los equipos de infraestructura en la empresa.

El siguiente será el flujo de creación de alertas a través de la interfaz web del nuevo sistema aseguramiento y diagnóstico de infraestructura:

1. El usuario ingresará al sistema por medio de un navegador web.
2. El servidor web de apache tomcat recibirá la solicitud y la desplegará.
3. El usuario realizará las configuraciones.
4. El sistema verificará los datos y si no están correctos el usuario debe corregirlos.
5. El sistema procesará los datos de configuración.
6. La configuración será guardada en la base de datos.

En la figura 51 se podrá observar el flujo del sistema con los pasos anteriores.

Figura 51. Funcionamiento del sistema a través de la interfaz web



Fuente: Elaboración propia, 2017

#### 5.2.2.4 Ejecución del sistema

El nuevo sistema de aseguramiento y diagnóstico de infraestructura será ejecutado mediante una tarea programada de sistema operativo, la cual se iniciará cada 15 minutos y llamará a un script de ejecución que va a utilizar la lista de alertas configuradas en el sistema, cada una de estas alertas correrá de forma paralela.

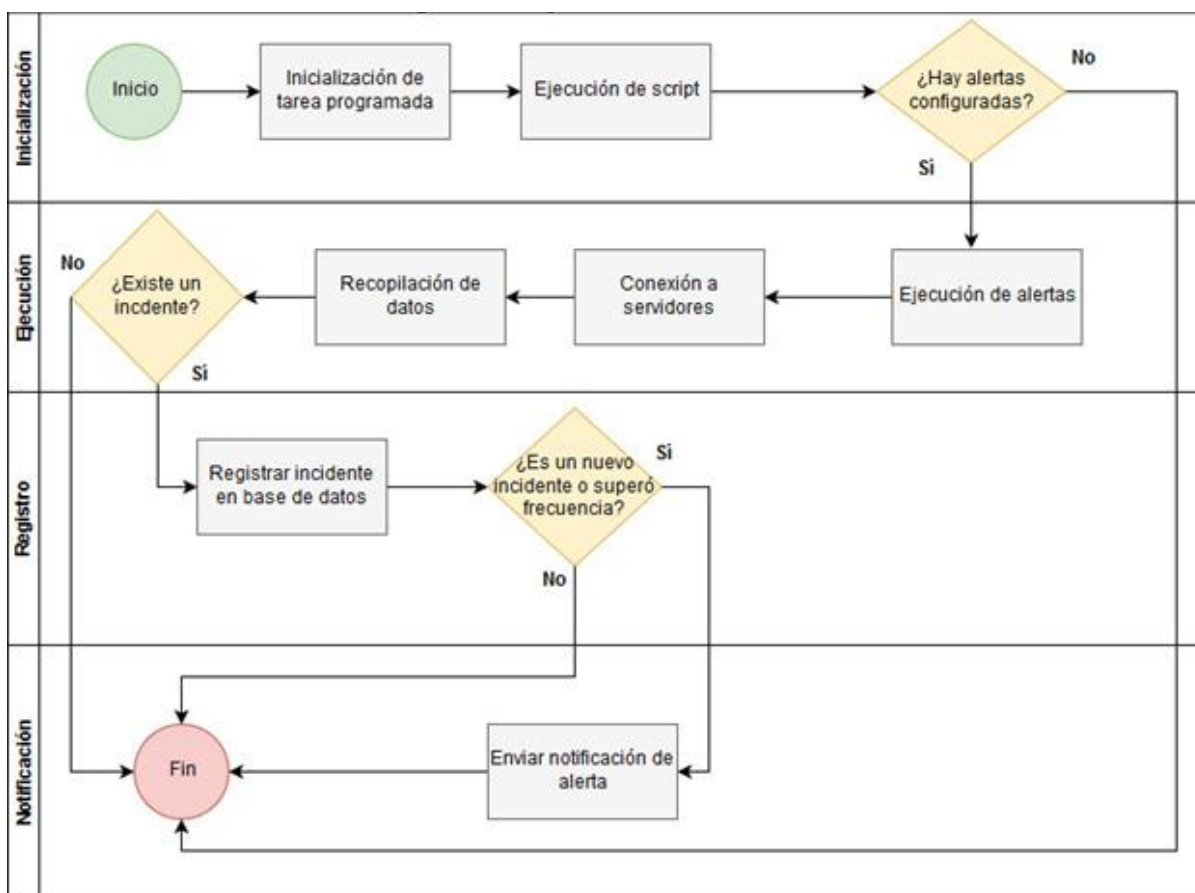
Los siguientes son los pasos que realizará el sistema para ser ejecutado.

1. Inicialá la tarea programada de sistema operativo y ejecuta el script del sistema.
2. El script verificará la lista de alertas que han sido configuradas y las ejecutará en forma paralela.
3. Se iniciará la conexión a los servidores de acuerdo al tipo de alerta y se recolectarán los datos.

4. Se verificarán los datos recopilados contra los parámetros de notificación de alertas para revisar si existe un incidente.
5. Si existe un incidente se procederá registrarlo en la base de datos.
6. Se verificará si existen alertas que han sido enviadas anteriormente y la frecuencia de envío.
7. Si el incidente no había sido notificado o ha cumplido el tiempo respecto a la frecuencia permitida se enviará una alerta por correo electrónico y SMS.

La figura 52 resumirá el flujo de ejecución del sistema.

Figura 52. Ejecución del sistema



Fuente: Elaboración propia, 2017

## **5.3 Plan Piloto del sistema**

### **5.3.1 Plan de implementación**

La implementación del nuevo sistema de aseguramiento y diagnóstico de infraestructura estará compuesta de 4 etapas que serán detalladas a continuación.

#### **5.3.1.1 Instalación de hardware y software de terceros**

Para realizar la instalación del sistema el servidor donde se ejecutará va necesitar el siguiente hardware disponible.

- Procesador Intel(R) Xeon (R) 2.93GHz
- Memoria RAM 16 GB
- Espacio en disco duro 20 GB

Además, será necesario realizar la instalación del siguiente software adicional:

- OpenSSH
- Oracle 12g
- Java 8
- Apache Tomcat8

#### **5.3.1.2 Instalación y configuración de Base de Datos**

Se deberá instalar y configurar la base de datos de acuerdo a lo establecido en el punto 5.1.4 referente a la estructura de la base de datos y validar su conectividad.

### **5.3.1.3 Configuración de archivos a nivel de sistema operativo**

Se crearán usuarios y llaves públicas entre el servidor que albergará el sistema de monitoreo y los equipos de la infraestructura, como se detalla en la sección 5.1.3.1 denominada requisitos técnicos.

Los archivos de propiedades, librerías y ejecución serán configurados de acuerdo a la sección estructura de archivos del sistema en el punto 5.2.2.2.

### **5.3.1.4 Desplegar el sistema**

Para realizar la carga del sistema será necesario iniciar el servidor web Apache Tomcat, luego ingresar a la plataforma de manejo por medio de un navegador web y cargar el archivo WAR que contendrá el nuevo sistema de aseguramiento y diagnóstico de infraestructura que se encuentra desarrollado en Java y HTML.

## **5.3.2 Pruebas del sistema**

A continuación, se procederá a crear los casos de pruebas que serán implementados en cada módulo del sistema de aseguramiento y diagnóstico de infraestructura.

Las siguientes tablas contienen la información de cada uno de los casos de pruebas que deben ser utilizados para verificar el funcionamiento del sistema y validar que cumple con los requisitos solicitados.

La tabla 47 mostrará el caso de prueba para agregar el tipo de aplicación donde se establecerá los pasos a seguir.

Tabla 47. Caso de Prueba para agregar tipo de aplicación

<b>Nombre del caso de Prueba</b>	Agregar tipo de aplicación
<b>Identificación</b>	CP1
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU2.1
<b>Pre condiciones</b>	
<b>Tipo de prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar nombre del tipo aplicación.	Usuario escribirá en pantalla un nombre del tipo de aplicación.
2- Ingresar nombre del perfil del tipo de aplicación.	Usuario escribirá en pantalla un nombre del perfil del tipo de aplicación.
3- Ingresar sufijo del tipo de aplicación.	Usuario escribirá en pantalla un sufijo del tipo de aplicación.
4- Presionar botón de enviar.	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 48 mostrará el caso de prueba para agregar el tipo de alerta donde se establecerá los pasos a seguir.

Tabla 48. Caso de Prueba para agregar tipo de alerta

<b>Nombre del caso de Prueba</b>	Agregar tipo de alerta
<b>Identificación</b>	CP2
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU2.2
<b>Pre condiciones</b>	
<b>Tipo de prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar una descripción	Usuario escribirá en pantalla una descripción de la alerta.
2- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 49 mostrará el caso de prueba para agregar el grupo de correo electrónico donde se establecerá los pasos a seguir.

Tabla 49. Caso de Prueba para agregar grupo de correo

<b>Nombre del caso de Prueba</b>	Agregar grupo de correo
<b>Identificación</b>	CP3
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU2.3
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar nombre del grupo de correo	Usuario escribirá en pantalla un nombre del grupo de correo.
2- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 50 mostrará el caso de prueba para agregar el correo electrónico donde se establecerá los pasos a seguir.

Tabla 50. Caso de Prueba para agregar correo electrónico

<b>Nombre del caso de Prueba</b>	Agregar correo electrónico
<b>Identificación</b>	CP4
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU2.4
<b>Pre condiciones</b>	Debe existir un grupo de correo electrónico.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar correo electrónico	Usuario escribirá en pantalla un correo electrónico.
2- Seleccionar grupo de correo electrónico	Usuario seleccionará un grupo de correo electrónico de la lista.
3- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 51 mostrará el caso de prueba para agregar el grupo de SMS donde se establecerá los pasos a seguir.

Tabla 51. Caso de Prueba para agregar grupo de SMS

<b>Nombre del caso de Prueba</b>	Agregar grupo de SMS
<b>Identificación</b>	CP5
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU2.5
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar nombre del grupo de SMS	Usuario escribirá en pantalla un nombre del grupo de SMS
2- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 52 mostrará el caso de prueba para agregar el número de SMS donde se establecerá los pasos a seguir.

Tabla 52. Caso de Prueba para agregar número de SMS

<b>Nombre del caso de Prueba</b>	Agregar número de SMS.
<b>Identificación</b>	CP6
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU2.6
<b>Pre condiciones</b>	Debe existir un grupo de SMS
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar número de teléfono	Usuario escribirá en pantalla un número de teléfono.
2- Seleccionar grupo de SMS	Usuario seleccionará un grupo de SMS de la lista.
3- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 53 mostrará el caso de prueba para agregar el servidor donde se establecerá los pasos a seguir.

Tabla 53. Caso de Prueba para agregar servidor

<b>Nombre del caso de Prueba</b>	Agregar servidor.
<b>Identificación</b>	CP7
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU3
<b>Pre condiciones</b>	Debe existir un tipo de aplicación.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar el tipo de aplicación	Usuario seleccionará un tipo de aplicación de la lista.
2- Ingresar el nombre del servidor físico	Usuario escribirá en pantalla el nombre del servidor físico.
3- Ingresar el nombre del servidor de aplicación (WebSphere)	Usuario escribirá en pantalla el nombre del servidor de aplicación.
4- Seleccionar el estado de notificación	El usuario seleccionará el estado en que se encontrará el servidor para el envío de notificaciones.
5- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 54 mostrará el caso de prueba para agregar aplicaciones donde se establecerá los pasos a seguir.

Tabla 54. Caso de Prueba para agregar aplicaciones

<b>Nombre del caso de Prueba</b>	Agregar aplicación.
<b>Identificación</b>	CP8
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU4
<b>Pre condiciones</b>	Debe existir un tipo de aplicación.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar el tipo de aplicación	Usuario seleccionará un tipo de aplicación de la lista.
2- Ingresar el nombre de la aplicación empresarial	Usuario escribirá en pantalla el nombre de la aplicación empresarial.
3- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 55 mostrará el caso de prueba para agregar archivos y directorios de errores donde se establecerá los pasos a seguir.

Tabla 55. Caso de Prueba para agregar archivos y directorios de errores

<b>Nombre del caso de Prueba</b>	Agregar archivos y directorios de errores.
<b>Identificación</b>	CP9
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU5.1
<b>Pre condiciones</b>	Debe existir un tipo de aplicación
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar el tipo de aplicación	Usuario seleccionará un tipo de aplicación de la lista.
2- Ingresar el nombre del servidor físico	Usuario escribirá en pantalla nombre del servidor físico.
3- Ingresar la ruta del directorio donde se ubica el archivo	Usuario escribirá en pantalla la ruta donde estará ubicado el archivo a monitorear.
4- Ingresar el nombre del archivo	Usuario escribirá en pantalla el nombre archivo.
5- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 56 mostrará el caso de prueba para agregar código de error donde se establecerá los pasos a seguir.

Tabla 56. Caso de Prueba para agregar código de error

<b>Nombre del caso de Prueba</b>	Agregar código de error
<b>Identificación</b>	CP10
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU5.2
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar código de error	Usuario escribirá en pantalla un código de error a ser monitoreado.
2- Ingresar parámetro para filtrar	Usuario escribirá en pantalla un parámetro para buscar búsqueda de ser necesario (opcional).
3- Ingresar mensaje	Usuario escribirá en pantalla un mensaje que describirá el código de error.
4- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 57 mostrará el caso de prueba para agregar parámetro de descarte donde se establecerán los pasos a seguir.

Tabla 57. Caso de Prueba para agregar parámetro de descarte

<b>Nombre del caso de Prueba</b>	Agregar parámetro de descarte
<b>Identificación</b>	CP11
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU5.3
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar parámetro para filtrar	Usuario escribirá en pantalla el parámetro que desea ser descartado.
2- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 58 mostrará el caso de prueba para agregar tipo de tarea donde se establecerán los pasos a seguir.

Tabla 58. Caso de Prueba para agregar tipo de tarea

<b>Nombre del caso de Prueba</b>	Agregar tipo de tarea
<b>Identificación</b>	CP12
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU6.1
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar descripción	Usuario escribirá en pantalla la descripción del tipo de tarea que va ser monitoreado.
2- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 59 mostrará el caso de prueba para agregar una tarea donde se establecerán los pasos a seguir.

Tabla 59. Caso de Prueba para agregar una tarea

<b>Nombre del caso de Prueba</b>	Agregar una tarea
<b>Identificación</b>	CP13
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU6.2
<b>Pre condiciones</b>	Debe existir un tipo de aplicación. Debe existir un tipo de tarea.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar el tipo de aplicación	Usuario seleccionará un tipo de aplicación de la lista.
2- Seleccionar el tipo de tarea	Usuario seleccionará un tipo de tarea de la lista.
3- Ingresar la consulta de base de datos	Usuario escribirá en pantalla la consulta de base de datos para monitorear la tarea.
4- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 60 mostrará el caso de prueba para agregar un proceso donde se establecerán los pasos a seguir.

Tabla 60. Caso de Prueba para agregar un proceso

<b>Nombre del caso de Prueba</b>	Agregar un proceso
<b>Identificación</b>	CP14
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU7
<b>Pre condiciones</b>	Debe existir un tipo de aplicación.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar el tipo de aplicación	Usuario seleccionará un tipo de aplicación de la lista.
2- Ingresar el nombre del proceso	Usuario escribirá en pantalla el nombre del proceso que debe ser monitoreado.
3- Ingresar la cantidad	Usuario escribirá en pantalla la cantidad de procesos que deben ser monitoreados.
4- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 61 mostrará el caso de prueba para agregar un dispositivo de red donde se establecerán los pasos a seguir.

Tabla 61. Caso de Prueba para agregar dispositivo de red

<b>Nombre del caso de Prueba</b>	Agregar dispositivo de red
<b>Identificación</b>	CP15
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU8
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar el nombre	Usuario escribirá en pantalla el nombre del dispositivo a monitorear accesibilidad en la red
2- Ingresar la dirección IP	Usuario seleccionará un estado de monitoreo de la lista.
3- Presionar botón de enviar.	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 62 mostrará el caso de prueba para agregar una ruta de almacenamiento donde se establecerán los pasos a seguir.

Tabla 62. Caso de Prueba para agregar ruta de almacenamiento

<b>Nombre del caso de Prueba</b>	Agregar ruta de almacenamiento
<b>Identificación</b>	CP16
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU9
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar el nombre	Usuario escribirá en pantalla el nombre del servidor donde se desea realizar el monitoreo.
2- Ingresar la ruta del sistema de archivos	Usuario escribirá en pantalla la ruta del sistema de archivos donde se desea monitorear el espacio.
3- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 63 mostrará el caso de prueba para agregar un estado de monitoreo donde se establecerán los pasos a seguir.

Tabla 63. Caso de Prueba para agregar estado de monitoreo

<b>Nombre del caso de Prueba</b>	Agregar estado de monitoreo
<b>Identificación</b>	CP17
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU10
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Ingresar aplicación	Usuario escribirá en pantalla el nombre de la aplicación.
2- Seleccionar el estado	Usuario escribirá en pantalla la ruta del sistema de archivos donde se desea monitorear el espacio.
3- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 64 mostrará el caso de prueba para agregar una alerta donde se establecerán los pasos a seguir.

Tabla 64. Caso de Prueba para agregar alerta

<b>Nombre del caso de Prueba</b>	Agregar alerta
<b>Identificación</b>	CP18
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	CU1
<b>Pre condiciones</b>	Debe haber un tipo de aplicación Debe haber un grupo de correo electrónico. Debe haber un grupo de SMS.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar el tipo de aplicación	Usuario seleccionará un tipo de aplicación de la lista.
2- Seleccionar el tipo de alerta	Usuario seleccionará un tipo de alerta de la lista.
3- Ingresar el usuario de Unix	Usuario escribirá en pantalla el usuario que se utilizará para recopilar información.
4- Ingresar el servidor de manejo de la aplicación	Usuario escribirá en pantalla el servidor que se utilizará para recopilar información.
5- Ingresar la frecuencia de envío de notificaciones	Usuario escribirá en pantalla la frecuencia en minutos con la cual se enviarán las alertas.
6- Seleccionar el estado de notificación por correo electrónico	Usuario seleccionará de la lista la opción habilitar o deshabilitar la notificación.
7- Seleccionar el grupo de correo	Usuario seleccionará de la lista el grupo de correo electrónico a ser notificado.
8- Seleccionar el estado de notificación por SMS	Usuario seleccionará de la lista la opción habilitar o deshabilitar la notificación.
9- Seleccionar el grupo de SMS	Usuario seleccionará de la lista el grupo de SMS a ser notificado.
10- Presionar botón de enviar	Sistema agregará los valores en la base de datos y mostrará todos los resultados agregados.

Fuente: Elaboración propia, 2017

La tabla 65 mostrará el caso de prueba para eliminar una entrada en el sistema donde se establecerán los pasos a seguir.

Tabla 65. Caso de Prueba para eliminar entrada en el sistema

<b>Nombre del caso de Prueba</b>	Eliminar entrada en el sistema
<b>Identificación</b>	CP19
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	
<b>Pre condiciones</b>	Existir entradas agregadas.
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar módulo	Usuario seleccionará un módulo en el sistema.
2- Dar clic en borrar	Usuario dará clic sobre borrar.
3- Confirmar borrado	El sistema preguntará si está seguro que desea borrar, luego el usuario presionará OK.

Fuente: Elaboración propia, 2017

La tabla 66 mostrará el caso de prueba para validar espacios donde se establecerán los pasos a seguir.

Tabla 66. Caso de Prueba para validación de espacios

<b>Nombre del caso de Prueba</b>	Validación de espacios
<b>Identificación</b>	CP20
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	
<b>Pre condiciones</b>	
<b>Tipo de Prueba</b>	Manual
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Seleccionar módulo.	Usuario seleccionará un módulo en el sistema.
2- Dar clic en agregar o editar	Usuario dará clic sobre agregar o editar.
3- Presionar botón de enviar	Si los espacios se encuentran vacíos o no seleccionados el sistema lanzará un mensaje de favor seleccionar este ítem o llenar este espacio.

Fuente: Elaboración propia, 2017

La tabla 67 mostrará el caso de prueba para enviar notificaciones donde se establecerán los pasos a seguir.

Tabla 67. Caso de Prueba para envío notificaciones

<b>Nombre del caso de Prueba</b>	Envío de notificaciones
<b>Identificación</b>	CP21
<b>Autor</b>	Johan Quesada Romero
<b>ID Caso de Uso</b>	
<b>Pre condiciones</b>	Debe existir una alerta agregada en el sistema.
<b>Tipo de Prueba</b>	Automático
<b>Plan de Prueba</b>	
<b>Pasos:</b>	<b>Resultado esperado</b>
1- Inicio de tarea programada	El sistema iniciar la recopilación de datos a través de tareas programadas.
2- Comparar parámetros de notificación	El sistema compara los datos recopilados con los parámetros a ser notificados.
3- Enviar notificación	Se recibirá un correo electrónico y un mensaje de texto (SMS) con una alerta.

Fuente: Elaboración propia, 2017

### 5.3.3 Resultados de las pruebas del sistema

A continuación, se presentarán los resultados obtenidos de los diferentes casos de pruebas realizados en el punto anterior.

- 1- Para el caso de prueba CP1 se agregaron diferentes tipos de aplicaciones como se puede observar en la figura 53.

Figura 53. Resultado caso de prueba CP1

Application	Profile	Suffix	Edit	Delete
all	all	all	Edit	Delete
orquestador	ORQProfile	ORQ	Edit	Delete
enrutador	ENRProfile	ENR	Edit	Delete
unificador	UNIProfile	UNI	Edit	Delete
inventario	INVProfile	INV	Edit	Delete
activador	ACTProfile	ACT	Edit	Delete
recursos	RECProfile	REC	Edit	Delete

Fuente: Elaboración propia, 2017

- 2- Para el caso de prueba CP2 se agregaron diferentes tipos de alertas como se podrá observar en la figura 54.

Figura 54. Resultado caso de prueba CP2

Description	Edit	Delete
Ambiente:Produccion - Alerta: La Aplicacion Empresarial esta detenida	<a href="#">Edit</a>	<a href="#">Delete</a>
Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	<a href="#">Edit</a>	<a href="#">Delete</a>
Ambiente:Produccion - Alerta: Demonio se encuentra detenido en el servidor	<a href="#">Edit</a>	<a href="#">Delete</a>
Ambiente:Produccion - Alerta: Se ha producido un error en el servidor de aplicacion	<a href="#">Edit</a>	<a href="#">Delete</a>
Ambiente:Produccion - Alerta: El proceso en base de datos esta detenido	<a href="#">Edit</a>	<a href="#">Delete</a>
Ambiente:Produccion - Alerta: Servidor no es accesible	<a href="#">Edit</a>	<a href="#">Delete</a>
Ambiente:Produccion - Alerta: Filesystem ha excedido el umbral de uso	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

- 3- Para el caso de prueba CP3 se agregaron diferentes grupos de correo como se podrá observar en la figura 55.

Figura 55. Resultado caso de prueba CP3

Email Group	Edit	Delete
AMDOCS	<a href="#">Edit</a>	<a href="#">Delete</a>
CLIENTE	<a href="#">Edit</a>	<a href="#">Delete</a>
AMDOCS-CLIENTE	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

- 4- Para el caso de prueba CP4 se agregaron diferentes correos electrónicos como se podrá observar en la figura 56.

Figura 56. Resultado caso de prueba CP4

Email	Group	Edit	Delete
johanquesada@gmail.com	CLIENTE	<a href="#">Edit</a>	<a href="#">Delete</a>
johanq@amdocs.com	AMDOCS	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

- 5- Para el caso de prueba CP5 se agregaron diferentes grupos de SMS como se podrá observar en la figura 57.

Figura 57. Resultado caso de prueba CP5

SMS Group	Edit	Delete
AMDOCS	<a href="#">Edit</a>	<a href="#">Delete</a>
CLIENTE	<a href="#">Edit</a>	<a href="#">Delete</a>
AMDOCS-CLIENTE	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

- 6- Para el caso de prueba CP6 se agregaron diferentes números de teléfono como se podrá observar en la figura 58.

Figura 58. Resultado caso de prueba CP6

Phone	Group	Edit	Delete
81111111	AMDOCS	<a href="#">Edit</a>	<a href="#">Delete</a>
68222222	CLIENTE	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

7- Para el caso de prueba CP7 se agregaron diferentes servidores como se podrá observar en la figura 59.

Figura 59. Resultado caso de prueba CP7

Application	Server	Application Server	Status	Edit	Delete
orquestrador	appserver1	orqserver01	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
orquestrador	appserver1	orqserver02	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
orquestrador	appserver2	orqserver03	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
orquestrador	appserver2	orqserver04	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver1	enrserver01	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver1	enrserver02	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver2	enrserver03	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver2	enrserver04	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver1	uniserver01	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver1	uniserver02	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver2	uniserver03	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver2	uniserver04	ENABLED	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

8- Para el caso de prueba CP8 se agregaron diferentes servidores como se podrá observar en la figura 60.

Figura 60. Resultado caso de prueba CP7

Application	Enterprise Application	Edit	Delete
orquestador	orqdomain	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	enrdomain	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	data-source	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	framework	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	homepage	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	wizards	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

9- Para el caso de prueba CP9 se agregaron diferentes archivos y directorios de errores como se podrá observar en la figura 61.

Figura 61. Resultado caso de prueba CP9

Application	Server	Location	File	Edit	Delete
orquestador	appserver1	/opt/ibm/websphere/ORQProfile/logs/orqserver01	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
orquestador	appserver2	/opt/ibm/websphere/ORQProfile/logs/orqserver02	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
orquestador	appserver3	/opt/ibm/websphere/ORQProfile/logs/orqserver03	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver1	/opt/ibm/websphere/ENRProfile/logs/enrserver01	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver2	/opt/ibm/websphere/ENRProfile/logs/enrserver02	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
enrutador	appserver3	/opt/ibm/websphere/ENRProfile/logs/enrserver03	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver1	/opt/ibm/websphere/UNIPProfile/logs/uniserver01	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver2	/opt/ibm/websphere/UNIPProfile/logs/uniserver02	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>
unificador	appserver3	/opt/ibm/websphere/UNIPProfile/logs/uniserver03	SystemOut.log	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

10- Para el caso de prueba CP10 se agregaron diferentes códigos de error como se podrá observar en la figura 62.

Figura 62. Resultado caso de prueba CP10

Errorcode	Parameter	Message	Edit	Delete
ORA-1691		Unable to extend lobsegment	<a href="#">Edit</a>	<a href="#">Delete</a>
J2CA00	E:	Error de WebSphere encontrado con codigo J2CA00	<a href="#">Edit</a>	<a href="#">Delete</a>
com.clarify.cbo.CboError	Internal	Internal Clarify Error	<a href="#">Edit</a>	<a href="#">Delete</a>
ADMG0003E	failed	cells/orqNetwork/clusters/ORQ_CLUSTER/sib-engines.xml	<a href="#">Edit</a>	<a href="#">Delete</a>
OutOfMemory		El servidor podría estar atascado	<a href="#">Edit</a>	<a href="#">Delete</a>
thread(s)		Existen muchos procesos colgados en el servidor	<a href="#">Edit</a>	<a href="#">Delete</a>
WLTC	E:	Se encontraron codigos de error de WebSphere	<a href="#">Edit</a>	<a href="#">Delete</a>
HMGR	E:	Error de WebSphere encontrado con codigo HMGR	<a href="#">Edit</a>	<a href="#">Delete</a>
CWS	E:	Error de WebSphere encontrado con codigo CWS	<a href="#">Edit</a>	<a href="#">Delete</a>
WTRC	E:	Error de WebSphere encontrado con codigo WTRC	<a href="#">Edit</a>	<a href="#">Delete</a>
DCSV1112W	heartbeats	Failed to respond to periodic heartbeats	<a href="#">Edit</a>	<a href="#">Delete</a>
CORBA.NO_IMPLEMENT		uniNetwork/clusters/UNI_CLUSTER	<a href="#">Edit</a>	<a href="#">Delete</a>
DCSV0004W		Did not receive adequate CPU time slice	<a href="#">Edit</a>	<a href="#">Delete</a>
ORA-01654		Unable to extend index in tablespace	<a href="#">Edit</a>	<a href="#">Delete</a>
ORA-00001	SA.SYS_C0065266	Unique constraint violated	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

11- Para el caso de prueba CP11 se agregaron diferentes parámetros de descarte como se podrá observar en la figura 63.

Figura 63. Resultado caso de prueba CP11

Discard	Edit	Delete
Queryset	<a href="#">Edit</a>	<a href="#">Delete</a>
CWSIU0002I	<a href="#">Edit</a>	<a href="#">Delete</a>
HMGR0228I	<a href="#">Edit</a>	<a href="#">Delete</a>
HMGR0218I	<a href="#">Edit</a>	<a href="#">Delete</a>
CWSIT0029I	<a href="#">Edit</a>	<a href="#">Delete</a>
HMGR0045W	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

12- Para el caso de prueba CP12 se agregó un tipo de tarea como se podrá observar en la figura 64.

Figura 64. Resultado caso de prueba CP12

Description	Edit	Delete
Agente	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

13- Para el caso de prueba CP13 se agregó una tarea como se podrá observar en la figura 65.

Figura 65. Resultado caso de prueba CP13

Application	Job Type	Query	Edit	Delete
activador	Agente	set head off set verify off set feedback offset head offset pages 0set pagesize 0spool '&1'select replace(phd_id   ','  port_sts_cd,'OP','STARTED') from phd_port_info@ACTINSTANCE where phd_id not in ('eir','evm1','h1r1','in') group by phd_id, port_sts_cd order by phd_id, port_sts_cd;spool offexit;	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

14- Para el caso de prueba CP14 se agregaron diferentes procesos como se podrá observar en la figura 66.

Figura 66. Resultado caso de prueba CP14

Application	Daemon	Quantity	Edit	Delete
orquestador	processwork	1	<a href="#">Edit</a>	<a href="#">Delete</a>
activador	manageprocess	28	<a href="#">Edit</a>	<a href="#">Delete</a>
activador	splitprocess	42	<a href="#">Edit</a>	<a href="#">Delete</a>
inventario	syncprocess	2	<a href="#">Edit</a>	<a href="#">Delete</a>
inventario	requestprocess	2	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

15- Para el caso de prueba CP15 se agregaron diferentes dispositivos de red como se podrá observar en la figura 67.

Figura 67. Resultado caso de prueba CP15

Server	Ip_address	Description	Edit	Delete
appserver1	192.168.1.11	aprovisionador	<a href="#">Edit</a>	<a href="#">Delete</a>
appserver2	192.168.1.12	aprovisionador	<a href="#">Edit</a>	<a href="#">Delete</a>
appserver3	192.168.1.13	aprovisionador	<a href="#">Edit</a>	<a href="#">Delete</a>
appserver4	192.168.1.14	aprovisionador	<a href="#">Edit</a>	<a href="#">Delete</a>
appserver5	192.168.1.15	aprovisionador	<a href="#">Edit</a>	<a href="#">Delete</a>
actserver1	192.168.1.21	activador	<a href="#">Edit</a>	<a href="#">Delete</a>
invserver1	192.168.1.31	inventario	<a href="#">Edit</a>	<a href="#">Delete</a>
dbserver1	192.168.1.41	base de datos	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

16- Para el caso de prueba CP16 se agregaron diferentes rutas de almacenamiento como se podrá observar en la figura 68.

Figura 68. Resultado caso de prueba CP16

Server	Filesystem	Edit	Delete
icepmig1	/	<a href="#">Edit</a>	<a href="#">Delete</a>
icepmig1	/usr	<a href="#">Edit</a>	<a href="#">Delete</a>
icepmig1	/var	<a href="#">Edit</a>	<a href="#">Delete</a>
icepmig1	/tmp	<a href="#">Edit</a>	<a href="#">Delete</a>
icepmig1	/home	<a href="#">Edit</a>	<a href="#">Delete</a>
icepmig1	/oravl01/oracle	<a href="#">Edit</a>	<a href="#">Delete</a>

Fuente: Elaboración propia, 2017

17- Para el caso de prueba CP17 se agregaron estados de monitoreo como se podrá observar en la figura 69.

Figura 69. Resultado caso de prueba CP17

Application	Status	Edit	Delete
unificador	ENABLED	Edit	Delete
enlace datos	ENABLED	Edit	Delete
orquestador	ENABLED	Edit	Delete
activador	ENABLED	Edit	Delete
recursos	ENABLED	Edit	Delete
inventario	ENABLED	Edit	Delete
enrutador	ENABLED	Edit	Delete
sincronizador	ENABLED	Edit	Delete

Fuente: Elaboración propia, 2017

18- Para el caso de prueba CP18 se agregaron diferentes alertas como se podrá observar en la figura 70.

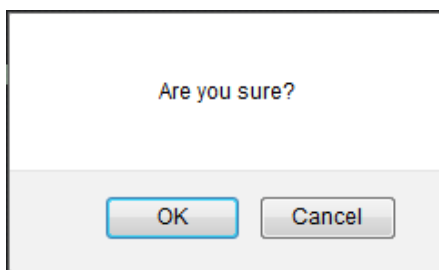
Figura 70. Resultado caso de prueba CP18

Application	Alert Type	User	Server	Frequency	Email	Email Group	SMS	SMS Group	Edit	Delete
orquestador	Ambiente:Produccion - Alerta: La Aplicacion Empresarial esta detenida	orquser1	appserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
orquestador	Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	orquser1	appserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
enrutador	Ambiente:Produccion - Alerta: La Aplicacion Empresarial esta detenida	enruser1	appserver2	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
enrutador	Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	enruser1	appserver2	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
inventario	Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	invuser1	invserver1	60 min(s)	ENABLED	CLIENTE	ENABLED	CLIENTE	Edit	Delete
unificador	Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	uniuser1	unisever1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
activador	Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	actuser1	actserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
recursos	Ambiente:Produccion - Alerta: Servidor de Aplicacion esta detenido	resuser1	resserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
activador	Ambiente:Produccion - Alerta: Demonio se encuentra detenido en el servidor	actuser1	actserver1	60 min(s)	ENABLED	CLIENTE	ENABLED	CLIENTE	Edit	Delete
orquestador	Ambiente:Produccion - Alerta: Demonio se encuentra detenido en el servidor	orquser1	appserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
recursos	Ambiente:Produccion - Alerta: Demonio se encuentra detenido en el servidor	resuser1	resserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
all	Ambiente:Produccion - Alerta: Se ha producido un error en el servidor de aplicacion	all	all	60 min(s)	ENABLED	CLIENTE	ENABLED	AMDOCS	Edit	Delete
activador	Ambiente:Produccion - Alerta: El proceso en base de datos esta detenido	actuser1	actserver1	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
all	Ambiente:Produccion - Alerta: Servidor no es accesible	all	all	60 min(s)	ENABLED	AMDOCS	ENABLED	AMDOCS	Edit	Delete
all	Ambiente:Produccion - Alerta: Filesystem ha excedido el umbral de uso	all	all	2 min(s)	ENABLED	CLIENTE	ENABLED	CLIENTE	Edit	Delete

Fuente: Elaboración propia, 2017

19- Para el caso de prueba CP19 se eliminó una entrada en los diferentes y se obtuvo la ventana de confirmación como se podrá observar en la figura 71.

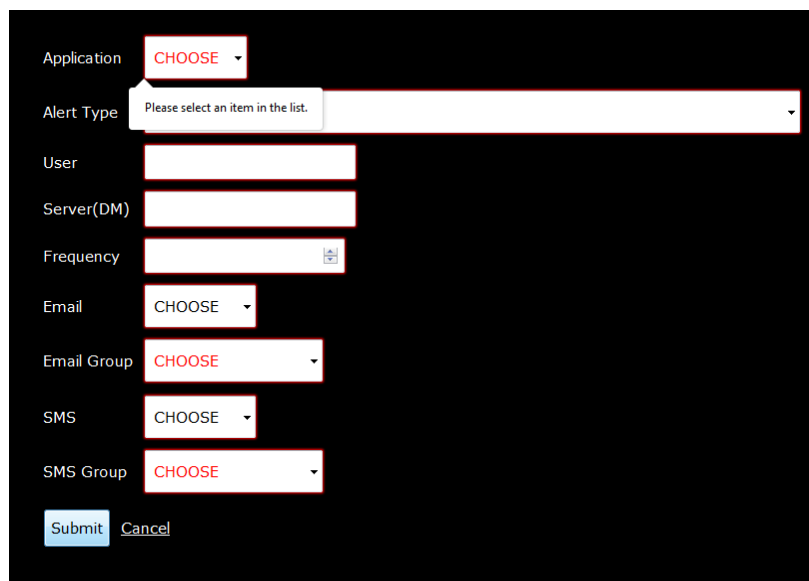
Figura 71. Resultado caso de prueba CP19



Fuente: Elaboración propia, 2017

20- Para el caso de prueba CP20 se validaron los espacios vacíos para cada entrada en los diferentes y se obtuvo un mensaje de validación como se podrá observar en las figuras 72 y 73.

Figura 72. Resultado caso de prueba CP20 validación de lista

A screenshot of a web form with a black background. The form contains several input fields and dropdown menus. The fields are: "Application" (dropdown menu with "CHOOSE" selected), "Alert Type" (dropdown menu with a validation message "Please select an item in the list."), "User" (text input field), "Server(DM)" (text input field), "Frequency" (text input field with a spinner), "Email" (dropdown menu with "CHOOSE" selected), "Email Group" (dropdown menu with "CHOOSE" selected), "SMS" (dropdown menu with "CHOOSE" selected), and "SMS Group" (dropdown menu with "CHOOSE" selected). At the bottom left, there are two buttons: "Submit" and "Cancel".

Fuente: Elaboración propia, 2017

Figura 73. Resultado caso de prueba CP20 validación de espacio

Application: orquestador

Alert Type: Ambiente:Produccion - Alerta: La Aplicacion Empresarial esta detenida

User: [Empty text box]

Server(DM): Please fill out this field.

Frequency: [Empty text box]

Email: CHOOSE

Email Group: CHOOSE

SMS: CHOOSE

SMS Group: CHOOSE

Submit Cancel

Fuente: Elaboración propia, 2017

21- Para el caso de prueba CP21 se validó la recepción de alertas por medio de correo electrónico y SMS como se podrá observar en las figura 74 y 75.

Figura 74. Resultado caso de prueba CP21 alerta por correo electrónico

**Ambiente:Produccion - Alerta: Filesystem ha excedido el umbral de uso**

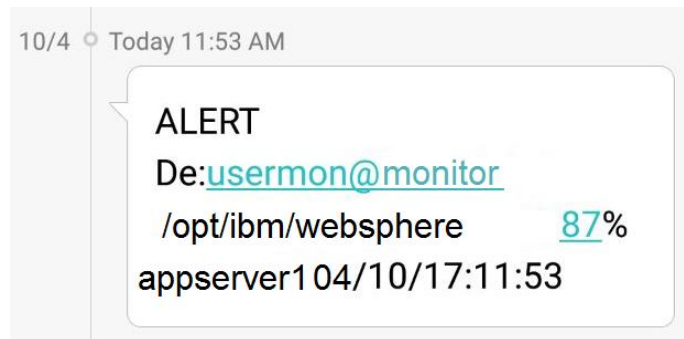
To Johan Quesada

Area de Soporte: AIX - Aplicacion  
 Fecha: Wed Oct 4 11:53:34 CST 2017  
 Ambiente: Produccion  
 Servidor: appserver1  
 Filesystem: /opt/ibm/websphere

Alerta: El filesystem ha excedido el umbral de uso en 87%

Fuente: Elaboración propia, 2017

Figura 75. Resultado caso de prueba CP21 alerta por SMS



Fuente: Elaboración propia, 2017

## **CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES**

## 1. CONCLUSIONES

Este proyecto tuvo como objetivo principal proponer una mejora al sistema de aseguramiento y diagnóstico de la infraestructura en la empresa Amdocs Costa Rica, para seguir las recomendaciones conforme a las mejores prácticas del mercado. Los resultados obtenidos proporcionan información de importancia, que se espera genere valor en el manejo del sistema de monitoreo y en el proceso de creación y modificación de alertas.

Del análisis de la información y la propuesta realizada, se plantean las siguientes conclusiones:

La empresa Amdocs Costa Rica actualmente posee un sistema de aseguramiento y diagnóstico de la infraestructura que no cumple con las recomendaciones del mercado, esto se debe a que no cuenta con la información en un punto centralizado, debido a que fue desarrollado para cubrir las necesidades que el negocio presentaba en ese momento.

Además, el sistema actual no presenta un modelo estandarizado relacionado con el desarrollo de las alertas, todas estas son programadas en SHELL a nivel de sistema operativo y cada una de ellas se crea de manera independiente con sus respectivos archivos de configuración, esto hace que el proceso de creación y modificación se vuelva complicado debido a que existe un script diferente para cada una de las alertas configuradas y al no poseer una interfaz gráfica su administración se torna compleja para el personal de la empresa y como consecuencia se debe invertir en muchas horas de trabajo adicional.

También, se determinó que el proceso actual donde el sistema realiza la recolección de datos y el envío de notificaciones se está realizando de forma efectiva, pero necesita de una reorganización en los scripts para que puedan seguir un mismo modelo de uso y sean más sencillos de ubicar.

Adicionalmente, se identificó que el proceso de ejecución del sistema actual se puede ver afectado por congestionamientos que ocasionen cuellos de botella ya que este se realiza por medio de tareas programadas, donde múltiples scripts se inician al mismo tiempo debido a que cada alerta tiene un script por separado, ello puede generar retrasos en el envío de notificaciones en situaciones cuando se presenten varios incidentes a la vez en la infraestructura.

Finalmente, se concluye que la implementación de la propuesta sumará valor al proceso de monitoreo debido a que va disminuir la complejidad en el manejo del sistema.

## 2. RECOMENDACIONES

Dentro de las recomendaciones que se pueden brindar a la empresa Amdocs Costa Rica en cuanto a la propuesta de mejora del sistema de aseguramiento y diagnóstico de infraestructura en este proyecto están:

Se recomienda a la empresa implementar la propuesta con el fin de poder contar con un sistema estandarizado que sea flexible, eficiente y confiable de acuerdo a las mejores prácticas del mercado y así cubrir las necesidades del negocio, permitirá organizar de manera adecuada los scripts del sistema, haciéndolos fácil de ubicar ya que estarán en un sitio centralizado y serán sencillos de configurar porque contarán con un mismo modelo independientemente del tipo de aplicación que se desee monitorear. Además, el personal se verá beneficiado en la utilización de la interfaz gráfica porque les permitirá invertir más tiempo en el soporte y entrega de servicios según establece ITIL, COBIT e ISO.

La implementación de la propuesta beneficiará a la optimización en el proceso de ejecución del sistema ya que este no contará con un script por alerta, sino con un solo script de ejecución con llamadas a librerías que siguen un modelo estándar para todos los tipos de alertas existentes, lo que permitirá un mayor control en el envío de notificaciones.

Por otra parte, se recomienda antes de iniciar con la implementación involucrar a los miembros que conforman el equipo técnico, con el fin de tener una mayor participación y compromiso al igual que en los departamentos de jefaturas.

También, la capacitación al personal acerca del uso del sistema será necesario, ya que eliminará la dependencia de tener una sola persona encargada de la administración y configuración del monitoreo y conocer las diferentes alertas que se recibirán cuando un evento se presente en la infraestructura.

Por último, de ser necesario a futuro incorporar al sistema un LDAP para manejar diferentes roles de acceso que será útil para administrar temas de seguridad que no fueron solicitados para la elaboración de este proyecto.

## Bibliografía

IBM. (Sin fecha). Introducción a WebSphere. Recuperado de

<https://www.ibm.com/developerworks/ssa/websphere/newto/>

IBM. (Sin fecha). WebSphere Application Server. Recuperado de [http://www-](http://www-03.ibm.com/software/products/es/appserv-was/)

[03.ibm.com/software/products/es/appserv-was/](http://www-03.ibm.com/software/products/es/appserv-was/)

amdocs. (2017). *A CONNECTED WORLD OF EMPOWERED INDIVIDUALS AND INCLUSIVE COMMUNITIES*. Recuperado de

<https://www.amdocs.com/about/corporate-social-responsibility>

amdocs. (2017). *ABOUT AMDOCS*. Recuperado de <https://www.amdocs.com/about>

Bon, J., Jong, A., Kolthof A., Pieper M., Tjassing R., Veen, A., & Verheijen, T. (2008).

Diseño del Servicio Basada en ITIL V3 - Guía de Gestión. Holanda, Amersfoort: Van Haren Publishing, Zaltbommel

Bon, J., Jong, A., Kolthof A., Pieper M., Tjassing R., Veen, A., & Verheijen, T. (2008).

Estrategia del Servicio Basada en ITIL V3 - Guía de Gestión. Holanda, Amersfoort: Van Haren Publishing, Zaltbommel

Bon, J., Jong, A., Kolthof A., Pieper M., Tjassing R., Veen, A., & Verheijen, T. (2008).

Mejora Continua del Servicio Basada en ITIL V3 - Guía de Gestión. Holanda, Amersfoort: Van Haren Publishing, Zaltbommel

Bon, J., Jong, A., Kolthof A., Pieper M., Tjassing R., Veen, A., & Verheijen, T. (2008).

Operación del Servicio Basada en ITIL V3 - Guía de Gestión. Holanda, Amersfoort: Van Haren Publishing, Zaltbommel

Apache (Sin fecha). Apache Tomcat. Recuperado de <http://tomcat.apache.org/>

Bon, J., Jong, A., Kolthof A., Pieper M., Tjassing R., Veen, A., & Verheijen, T. (2008).

Bon, J. V. (2008, p.28). Fundamentos de la Gestión de Servicios de TI basada en ITIL.

Cegarra, J. (2004). Metodología de la investigación científica y tecnológica. Madrid, ES: Ediciones Díaz de Santos.

Deloitte. (2016). SAM Administración de Activos de Software. Recuperado de [https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Administracion\\_activos\\_software-2016.pdf](https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Administracion_activos_software-2016.pdf)

Ediciones Van Haren Publishing, tercera edición.

Hueso, L. (2014) Base de datos: grado superior. Madrid, ES: RA-MA Editorial.

IBM (Sin fecha). Generating a private/public RSA key pair. Recuperado de [https://www.ibm.com/support/knowledgecenter/en/SS42VS\\_7.2.6/com.ibm.qradar.doc/t\\_qradar\\_adm\\_gen\\_pub\\_priv\\_key.html/](https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.6/com.ibm.qradar.doc/t_qradar_adm_gen_pub_priv_key.html/)

IBM. (Sin fecha). IBM AIX Sistema operativo UNIX basado en estándares abiertos seguro, escalable y sólido. Recuperado de <https://www-03.ibm.com/systems/es/power/software/aix>

ISACA. (2012). COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Recuperado de <http://www.isaca.org/cobit/pages/cobit-5-spanish.aspx>

IT Consultores. (s.f). Conozca los beneficios de los Servicios de Nagios en Colombia para monitorear infraestructura tecnológica. Recuperado de

<http://itconsultores.com.co/conozca-los-beneficios-los-servicios-nagios-colombia-monitorear-infraestructura-tecnologica/?lang=en>

Luna, F., Sanz P. (2011). Programación de Shell Scripts. Madrid, ES: Editorial Universidad Autónoma de Madrid.

Oracle. (Sin fecha). ¿Qué es la tecnología Java y para qué la necesito? Recuperado de [https://www.java.com/es/download/faq/whatis\\_java.xml](https://www.java.com/es/download/faq/whatis_java.xml)

Ordax, J., Aranzazu, P. (2012). Programación web en java. Madrid, ES: Ministerio de Educación de España, 2012.

Redicsa. (s.f). Diez razones para elegir TOPdesk. Recuperado de [http://www.redicsa.com/10\\_Reasons\\_to\\_Choose\\_TOPdesk.pdf](http://www.redicsa.com/10_Reasons_to_Choose_TOPdesk.pdf)

STI. (s.f). Monitoreo de Operaciones TI. Recuperado de <http://www.sti.com.ve/gestion-de-procesos/>

Sampieri, R., Fernández, C., Baptista, M. (2010). Metodología de la investigación (5a. ed.). México, D.F.: McGraw-Hill Interamericana-

Transición del Servicio Basada en ITIL V3 - Guía de Gestión. Holanda, Amersfoort: Van Haren Publishing, Zaltbommel

Terán, J. (2010). Manual de Introducción al lenguaje HTML. Formación para el Empleo. Madrid, ES: Editorial CEP, S.L.

## **APÉNDICES Y ANEXOS**

## 1. APÉNDICE 1: CUESTIONARIO

1- ¿Existe actualmente una herramienta de monitoreo de infraestructura?

Sí

No

2- ¿Consideras que el proceso de monitoreo está estandarizado para todos los incidentes?

Sí

No

3- ¿Con qué frecuencia necesita habilitar y deshabilitar el monitoreo?

Frecuentemente

Esporádicamente

Rara vez

4 - ¿Existe un método de notificación para identificar un incidente de manera ágil?

Sí

No

5- ¿Cuán a menudo ocurren los incidentes relacionados con la infraestructura?

Frecuentemente

Esporádicamente

Raramente

6- ¿Se cumplen los SLAs para resolver incidentes?

Sí

No

7- ¿Hay algún impacto después de resolver un incidente?

Sí

No

8- ¿Existen medidas preventivas para prevenir un incidente?

Sí

No

9- ¿Con qué frecuencia necesita crear alertas nuevas?

Frecuentemente

Esporádicamente

Rara vez

10- ¿Con qué frecuencia necesita modificar las alertas?

Frecuentemente

Esporádicamente

Rara vez

11- ¿Tiene un historial de incidentes registrados?

Sí

No

12- ¿Con qué frecuencia necesita obtener información sobre el incidente anterior?

Frecuentemente

Esporádicamente

Rara vez

1. ¿Conoce todos los aspectos relacionados con la herramienta de monitoreo de infraestructura?
2. ¿Cuál es su impresión sobre el uso de la herramienta de monitoreo?
3. ¿Cómo resuelves incidentes o problemas cuando ocurren?
4. ¿Considera que la herramienta de monitoreo es confiable?
5. ¿Qué puntos considera importantes para el monitoreo de la infraestructura?