



UNIVERSIDAD
**SAN IGNACIO
DE LOYOLA**

FACULTAD DE INGENIERÍA

Carrera de Ingeniería Empresarial y de Sistemas

**IMPLEMENTACIÓN DE UN NUEVO SISTEMA DE
MONITOREO EN GMD PARA AUMENTAR LA
EFICACIA OPERATIVA**

**Tesis para optar el Título Profesional de Ingeniero Empresarial y de
Sistemas**

BRYAN CISNEROS GÓMEZ

Asesora:

Carmen Rosa Chávez Valderrama

**Lima – Perú
2016**



FACULTAD DE INGENIERÍA

Carrera de Ingeniería Empresarial y de Sistemas

**IMPLEMENTACIÓN DE UN NUEVO SISTEMA DE MONITOREO EN GMD PARA
AUMENTAR LA EFICACIA OPERATIVA**

**Tesis para obtener el Título Profesional de Ingeniero
Empresarial y de Sistemas**

BRYAN CISNEROS GÓMEZ

ASESORA:

Carmen Rosa Chávez Valderrama

Walter Marticorena

Ramos

Moisés Egües

Martínez

Gustavo Luna Victoria

León

LIMA – PERÚ

2016

DEDICATORIA

Dedico esta tesis en primer lugar a Dios porque me ha permitido llegar a este momento de mi vida profesional. A mis padres y hermanos que son mi motor y motivo para ser una mejor persona y un gran profesional, porque fueron quienes me acompañaron en el largo camino que recorrí para poder cumplir esta meta y porque siempre me demostraron su apoyo y ayuda incondicional.

AGRADECIMIENTO

En primer lugar agradezco a Dios porque me dio las fuerzas necesarias todos los días para trabajar y estudiar al mismo tiempo.

A mi madre porque estuvo pendiente de mí en cada amanecida y celebrar conmigo los logros obtenidos en estos años universitarios.

A mi padre porque siempre me ha guiado para ser una persona independiente y lograr sus metas por sus propios medios.

A mis hermanos por alegrarme en mis momentos de estrés con sus bromas y ocurrencias.

A la Dra. Carmen Rosa Chávez Valderrama por su asesoría brindada durante el desarrollo de este trabajo.

Y a todas las personas que colaboraron conmigo en la realización de este trabajo.

RESUMEN

En la presente tesis discutiremos sobre el proyecto de implementación de un nuevo sistema de monitoreo utilizado por la empresa GMD S.A. como parte de la herramienta para la gestión de eventos sobre los distintos equipos dentro del centro de cómputo, en especial los servidores y aplicaciones en calidad de hosting dentro del área de servicios datacenter.

La tesis desarrollada abarca como principal problema la ineficacia operacional en el monitoreo de equipos dentro del centro de datos del proveedor de servicios, debido a la obsolescencia de sus actuales sistemas de monitoreo.

Se brindará una descripción de las principales terminologías teóricas utilizadas durante el desarrollo de este trabajo, así como una explicación de lo desarrollado en cada una de 3 fases del proyecto, las cuáles son: evaluación de requerimientos, evaluación técnica-cualitativa e implementación del sistema de monitoreo.

Se presentará los resultados de las pruebas realizadas durante el proyecto, así como su evaluación financiera resultado de las estimaciones de costos incurridos para la implementación del sistema en un periodo de 60 meses. Finalmente se explicarán las conclusiones, es decir se mostrarán los resultados de haber cumplido con los objetivos establecidos y recomendaciones encontradas al finalizar el proyecto para que se puedan realizar mejoras futuras en otras tesis.

Palabras clave:

ITIL, eventos, satisfacción del cliente, sistema de monitoreo, mejora continua, eficacia operacional.

ÍNDICE

1	CAPÍTULO I: INTRODUCCIÓN	1
1.1	JUSTIFICACIÓN.....	1
1.2	DEFINICIÓN DEL PROBLEMA.....	1
1.3	OBJETIVOS.....	2
1.3.1	GENERAL	2
1.3.2	ESPECÍFICOS	2
1.4	CONTRIBUCIÓN DEL BACHILLER.....	3
1.5	ALCANCE Y LIMITACIONES	3
1.5.1	ALCANCES.....	3
1.5.2	LIMITACIONES	4
1.6	BREVE RESUMEN DE LAS FASES DE DESARROLLO.....	5
2	CAPÍTULO II: MARCO CONTEXTUAL.....	7
2.1	DESCRIPCIÓN DE LA EMPRESA DONDE SE DESARROLLA LA TESIS	7
2.2	MACRO PROCESO DE LA ORGANIZACIÓN	8
2.3	PRESENTACIÓN DEL ÁREA FUNCIONAL.....	9
3	CAPÍTULO III: MARCO CONCEPTUAL.....	11
3.1	DIRECCIÓN DE PROYECTOS.....	11
3.2	GESTIÓN DE EVENTOS.....	12
3.3	EVOLUCIÓN Y TENDENCIAS DE LAS HERRAMIENTAS DE MONITOREO DE REDES	13
3.3.1	PRIMERA GENERACIÓN	14
3.3.2	SEGUNDA GENERACIÓN	15
3.3.3	TERCERA GENERACIÓN.....	16
3.3.4	CUARTA GENERACIÓN	18
4	CAPÍTULO IV: MARCO METODOLÓGICO.....	21
4.1	FASE 01: EVALUACIÓN DE REQUERIMIENTOS.....	22
4.2	FASE 02: EVALUACIÓN DE LA HERRAMIENTA.....	22
4.3	FASE 03: IMPLEMENTACIÓN DEL SISTEMA.....	23
5	CAPÍTULO V: EVALUACIÓN DE REQUERIMIENTOS PARA EL SISTEMA DE MONITOREO.....	25
5.1	LEVANTAMIENTO DE INFORMACIÓN DE LA SOLUCIÓN ACTUAL	25
5.2	ANÁLISIS DE LA SITUACIÓN ACTUAL.....	26
5.3	DESARROLLO DE DOCUMENTO RFP	30
6	CAPÍTULO VI: EVALUACIÓN DE LA HERRAMIENTA DEL SISTEMA DE MONITOREO 31	
6.1	ELABORACIÓN DE LA MATRIZ DE EVALUACIÓN TÉCNICA.....	31
6.2	SELECCIÓN DE LA MEJOR SOLUCIÓN	34
7	CAPÍTULO VII: IMPLEMENTACIÓN DEL SISTEMA DE MONITOREO	36
7.1	DISEÑO TÉCNICO	36

7.1.1	ARQUITECTURA LÓGICA.....	36
7.1.2	ARQUITECTURA FÍSICA	37
7.1.3	DETALLE DE LA ARQUITECTURA PROPUESTA	38
7.1.4	PROBES A IMPLEMENTAR	40
7.2	IMPLANTACIÓN DE SISTEMA DE MONITOREO DE SERVIDORES Y APLICACIONES	47
7.2.1	ENFOQUE GENERAL.....	47
7.2.2	MANEJO DE ALARMAS	49
7.2.3	USER LOGINS	51
7.2.4	REPORTES Y PERCENTIL 95	51
8	CAPÍTULO VIII: EVALUACIÓN FINANCIERA DEL PROYECTO	58
8.1	DATOS GENERALES DEL PROYECTO.....	58
8.2	ESTRUCTURA DE COSTOS DEL PROYECTO.....	58
8.3	FLUJO DE CAJA DEL PROYECTO	61
9	CONCLUSIONES	63
10	RECOMENDACIONES	64
11	BIBLIOGRAFÍA.....	65
12	APÉNDICES	66
12.1	APÉNDICE 01: ÁRBOL DE PROBLEMAS.....	66
12.2	APÉNDICE 02: ÁRBOL DE OBJETIVOS	67
12.3	APÉNDICE 03: CONSIDERACIONES PARA DETERMINAR EL HARDWARE Y SOFTWARE DE LA ARQUITECTURA.....	68
12.4	APÉNDICE 04: TABLAS RESUMEN DE PUERTOS A HABILITAR PARA LAS REDES DE GMD.....	72
12.5	APÉNDICE 05: REQUERIMIENTOS PARA LOS PROBES A IMPLEMENTAR	77
12.6	APÉNDICE 06: MÉTRICAS A MONITOREAR POR TIPO DE PROBE.....	85
12.7	APÉNDICE 07: LISTA DE CANTIDAD DE EQUIPOS A DESCUBRIR POR DIFERENTES CLIENTES	99
12.8	APÉNDICE 08: DETALLE DE FLUJO DE CAJA MENSUAL.....	106
13	CRONOGRAMA	111

ÍNDICE DE TABLAS

Tabla N° 1: Cuadro de actividades para cumplir objetivos de la fase 01	22
Tabla N° 2: Cuadro de actividades para cumplir objetivos de la fase 02	22
Tabla N° 3: Cuadro de actividades para cumplir objetivos de la fase 03	23
Tabla N° 4: Identificación de interesados y nivel de interés o influencia	26
Tabla N° 5: Tabla de requerimientos de herramienta de monitoreo.....	27
Tabla N° 6: Cuadro de identificación de proveedores del servicio	30
Tabla N° 7: Tabla de puntuación técnica del componente software de la herramienta del sistema de monitoreo.....	31
Tabla N° 8: Tabla resumen de puntuación técnica del componente software de la herramienta del sistema de monitoreo	33
Tabla N° 9: Cuadro comparativo de beneficios cualitativos	34
Tabla N° 10: Cuadro resumen de la evaluación de la mejor solución.....	34
Tabla N° 11: Tabla resumen de cantidad equipos y licencias requeridas	58
Tabla N° 12: Tabla de estructura de costos estimados del proyecto.....	59
Tabla N° 13: Tabla de flujo de caja del proyecto.....	61
Tabla N° 14: Tabla resumen de distribución de costos del proyecto.....	62
Tabla N° 15: Tabla para determinar el tamaño de implementación de CA Nimsoft.....	68
Tabla N° 16: Tabla resumen de habilitación de puertos para la red Infraestructura en Cliente	72
Tabla N° 17: Tabla resumen de habilitación de puertos para la red Cloud.....	73
Tabla N° 18: Tabla resumen de habilitación de puertos para la red híbridos.....	74
Tabla N° 19: Tabla resumen de habilitación de puertos para la red Islas	75
Tabla N° 20: Tabla de requerimientos del <i>probe</i> CDM.....	77
Tabla N° 21: Tabla de requerimientos del <i>probe</i> Processes.....	77
Tabla N° 22: Tabla de requerimientos del <i>probe</i> Oracle	78
Tabla N° 23: Tabla de requerimientos del <i>probe</i> Sqlserver.....	79
Tabla N° 24: Tabla de requerimientos del <i>probe</i> interface_traffic	80
Tabla N° 25: Tabla de requerimientos del <i>probe</i> CDM Exchange_monitor	81
Tabla N° 26: Tabla de requerimientos del <i>probe</i> ad_server	81
Tabla N° 27: Tabla de requerimientos del <i>probe</i> netapp	82
Tabla N° 28: Tabla de requerimientos del <i>probe</i> VMWare	82
Tabla N° 29: Tabla de requerimientos del <i>probe</i> url_response	83
Tabla N° 30: Tabla de requerimientos del <i>probe</i> snmpcollector.....	83
Tabla N° 31: Tabla de requerimientos del <i>probe</i> net_connect	84
Tabla N° 32: Tabla de métricas del <i>probe</i> CDM.....	85
Tabla N° 33: Tabla de métricas del <i>probe</i> Processes.....	86
Tabla N° 34: Tabla de métricas del <i>probe</i> Oracle	86
Tabla N° 35: Tabla de métricas del <i>probe</i> Sqlserver.....	87
Tabla N° 36: Tabla de métricas del <i>probe</i> Exchange_monitor	87
Tabla N° 37: Tabla de métricas del <i>probe</i> ad_server.....	94
Tabla N° 38: Tabla de métricas del <i>probe</i> netapp	95
Tabla N° 39: Tabla de métricas del <i>probe</i> VMWare	96
Tabla N° 40: Tabla de métricas del <i>probe</i> url_response	97
Tabla N° 41: Tabla de cantidad de servidores a descubrir	99
Tabla N° 42: Tabla de equipos de comunicaciones a descubrir	102

ÍNDICE DE FIGURAS

Figura N° 1: SGI.MP.01 Procesos Generales GMD	9
Figura N° 2: Procesos del Área Servicios Datacenter	10
Figura N° 3: Ejemplo de monitoreo de 1ª Generación	15
Figura N° 4: Ejemplo de monitoreo de 2ª Generación.....	16
Figura N° 5: Ejemplo de monitoreo de 3ª Generación.....	17
Figura N° 6: Ejemplo de monitoreo de 4ª Generación.....	18
Figura N° 7: Evolución de herramientas de monitoreo.....	20
Figura N° 8: Diagrama de secuencia del proyecto	24
Figura N° 9: Arquitectura de red de monitoreo de GMD actual	25
Figura N° 10: Arquitectura Lógica de CA NimSoft Monitor.....	36
Figura N° 11: Arquitectura Propuesta NimSoft	38
Figura N° 12: Monitoreo Local de Sistemas Operativos a través de CDM, interface_traffic y processes Probes.....	41
Figura N° 13: Monitoreo Remoto de Sistemas Operativos a través de snmpcollector Probe	41
Figura N° 14: Monitoreo Remoto de Interfaz de red a través de interface_collector Probe.....	42
Figura N° 15: Monitoreo Local de bases de datos a través de Sqlserver y Oracle Probes	43
Figura N° 16: Monitoreo Local de Directorio Activo a través de ad_server Probe	44
Figura N° 17: Monitoreo Local de Exchange Server a través de Exchange_monitor Probe.....	44
Figura N° 18: Monitoreo Remoto de Storage a través de NetApp Probe	45
Figura N° 19: Monitoreo Remoto de Servidores ESX a través de VMWare Probe.....	46
Figura N° 20: Monitoreo Remoto de URLs a través de url_response Probe	47
Figura N° 21: Flujo de Alarmas a través de alarm_enrichment	50
Figura N° 22: Flujo de Alarmas generadas desde CA NimSoft	50
Figura N° 23: Lista de Dashboards que trae el Portal por defecto	52
Figura N° 24: Diseñador de Reportes de CA NimSoft.....	53
Figura N° 25: Reporte obtenido por CA NimSoft.....	54
Figura N° 26: Dashboard Out of the Box de Monitoreo Exchange.....	55
Figura N° 27: Dashboard Out of the Box de Monitoreo de Servidores.....	55
Figura N° 28: Dashboard Out of the Box de Monitoreo de SQL Server	56
Figura N° 29: Dashboard Out of the Box de Monitoreo de NetApp	56
Figura N° 30: Dashboard Out of the Box de Monitoreo de VMware	57
Figura N° 31: Árbol de problemas	66
Figura N° 32: Árbol de objetivos.....	67

ÍNDICE DE ABREVIATURAS

ITIL	Information Technology Infrastructure Library
TI	Tecnología de Información
RFP	Request for proposal
ISO	International Organization for Standardization
OHSAS	Occupational Health and Safety Assessment Series
NTP	Norma Técnica Peruana
CMMI	Capability Maturity Model Integration
PMI	Project Management Institute
IDC	International Data Corporation
SGI	Sistema de gestión integrado
CPU	Central processing unit
ETC	Etcetera
WAN	Wide Area Network
APM	Application performance monitor
MSP	Multi Service Provider
UMP	Unified Management Portal

1 CAPÍTULO I: INTRODUCCIÓN

1.1 JUSTIFICACIÓN

Esta tesis tiene como principal objetivo realizar la implementación de un nuevo sistema de monitoreo para aumentar la eficacia operativa dentro del centro de cómputo del proveedor de servicios estudiado. Este nuevo sistema de monitoreo permitirá lograr el cumplimiento de los acuerdos de niveles de servicios ofrecidos a sus clientes mejorando la gestión de eventos, a nivel de *hardware* y *software*, a través de una vista unificada de monitoreo, ayudando a detectar tempranamente las anomalías en los sistemas informáticos con el fin de realizar un rápido diagnóstico y disminuir el tiempo de detección de posibles incidencias en los servicios y, por consiguiente, reducir el tiempo de indisponibilidad de los sistemas informáticos, que sus clientes usan para soportar sus procesos de negocio, logrando como beneficio el incremento de nivel de satisfacción de dichos clientes y el prestigio del proveedor de servicios en su mercado objetivo.

1.2 DEFINICIÓN DEL PROBLEMA

Actualmente, el proveedor de servicio alberga dentro de su centro de cómputo distintos servidores (*hardware*) y aplicaciones (*software*), que forman parte de los sistemas informáticos de sus distintos clientes, y por los cuáles se han ofrecido acuerdos de nivel de servicios garantizando la disponibilidad y capacidad de la infraestructura provista para dichos sistemas informáticos.

Este proveedor de servicio cuenta con múltiples sistemas de monitoreo y que no se encuentran integrados entre sí, generando de esta manera dificultad para acceder a la información en tiempo real y complejidad para el despliegue del monitoreo de la infraestructura requeridos por el mercado el día de hoy.

Además, la ausencia de procesos adecuados para la gestión de eventos y la falta de trazabilidad de estadísticas para la atención de los clientes no permite una adecuada gestión del servicio ofrecido a los clientes.

El problema radica en la reducida eficacia operativa dentro del centro de cómputo, ocasionadas por los sistemas de monitoreo obsoletos e independientes entre sí. Debido a esto, se incumplen los acuerdos de nivel de servicio ofrecidos a sus clientes, generando alta insatisfacción de sus clientes por el servicio *Hosting* contratado.

Para mayor detalle sobre la determinación del problema, referirse al apéndice 01.

1.3 OBJETIVOS

1.3.1 GENERAL

Realizar la implementación de un sistema de monitoreo para aumentar la eficacia operativa del centro de cómputo del proveedor de servicios *Hosting*.

1.3.2 ESPECÍFICOS

Para lograr el objetivo general se requiere que se cumplan los siguientes objetivos:

- Realizar la evaluación de requerimientos de la nueva herramienta para el sistema de monitoreo que integre todo el alcance de monitoreo a fin de reducir la complejidad de despliegue de agentes
- Realizar la evaluación técnica-económica de la nueva herramienta para el sistema de monitoreo para contar con una única plataforma de monitoreo integrada y centralizada
- Realizar la implementación de la herramienta para el sistema de monitoreo de los servicios de *Hosting* para brindar fácil acceso a información en tiempo real

Para mayor detalle sobre la determinación de los objetivos, referirse al apéndice 02.

1.4 CONTRIBUCIÓN DEL BACHILLER

Actualmente, mi rol en la empresa descrita es de ingeniero de preventa en servicios de tercerización de tecnología, mi contribución dentro del proyecto fue realizar la recopilación de requerimientos de parte del área usuaria, realizar la evaluación y determinación de la mejor herramienta para satisfacer las necesidades de la organización.

Dentro de las actividades relevantes realice la evaluación técnica-económica de las herramientas de monitoreo y servicios ofrecidos por distintos proveedores especializados del mercado. Posteriormente el área de implementación del área de *ISO* en GMD se encargó de la implementación y pruebas pilotos del proyecto, lo que brindó como resultado los documentos de arquitectura final para que el área de Servicios *Datacenter* finalice con el despliegue final del proyecto.

1.5 ALCANCE Y LIMITACIONES

1.5.1 ALCANCES

El alcance de esta tesis es brindar las pautas necesarias para poder implementar un sistema de monitoreo, que permitirá la automatización en la generación de eventos, de tipo alertas e informativas, relacionados a los componentes de *hardware* y *software* de servidores y aplicaciones dentro del centro de datos del proveedor de servicios a través de umbrales establecidos para los distintos tipos de componentes de acuerdo a las necesidades de cada cliente y a las buenas prácticas del mercado.

En primer lugar se realizará la evaluación de requerimientos necesitados por el área y personal que serán usuarios de este nuevo sistema, a fin de elaborar el documento de requerimientos de propuesta con el cuál serán evaluados, de manera técnica y económicamente, 2 herramientas de clase global, las cuáles son Orion “*SolarWinds*” y CA “*NimSoft Monitor*”.

Posteriormente, se realizará la implementación del nuevo sistema de monitoreo, que consistirá en realizar el diseño de la solución y su implementación. Para ello se implementará una infraestructura de servidores que permita recolectar las alertas sobre la disponibilidad de los servidores y aplicaciones a monitorear, las cuáles serán visualizadas en una única pantalla por los operadores del centro de datos, permitiéndoles identificar rápidamente el componente fallido a través de semáforos de control.

Finalmente, se realizará el despliegue de esta solución y se generará toda la documentación sobre la arquitectura desplegada y los manuales adecuados para la actualización y/o integración de nuevos elementos a monitorear de los equipos en el centro de cómputo del proveedor de servicio como parte de la gestión de conocimiento de la empresa.

1.5.2 LIMITACIONES

La presente tesis se basa en la premisa de que la empresa cuenta con un Sistema de Gestión de Conocimiento ya implementado, para el mantenimiento y actualización de la documentación del proyecto de implementación del sistema de monitoreo de servidores y aplicaciones.

Así mismo, otra premisa de la tesis, es que, el sistema quedará implementado para realizar el monitoreo de los servidores y aplicaciones dentro del centro de datos. Sin embargo, este sistema podrá realizar otro tipo de monitoreo, tales como transacciones y procesos de negocios, para ello se tendrán que adicionar licencias de estas funcionalidades y las configuraciones respectivas.

Además, esta tesis se basa en la premisa de que la empresa ya cuenta con un sistema para la gestión de incidencias. La integración de este nuevo sistema de monitoreo con el sistema de gestión de incidencias y la automatización de creación de tickets de incidencias, generadas por la activación de las alertas del nuevo sistema de monitoreo de servidores y aplicaciones no se encuentran en el alcance de esta tesis.

Esta tesis solamente toma en consideración el proceso de gestión de eventos actual de la empresa en mención, como parte de la fase de operación dentro del ciclo de vida del servicio de acuerdo a *ITIL*, para considerarlo durante el diseño del nuevo sistema de monitoreo a implementar.

Finalmente, esta tesis, no considera dentro de la implementación del nuevo sistema de monitoreo, el diseño e implementación de los planes de recuperación de dicho sistema en casos de contingencia.

1.6 BREVE RESUMEN DE LAS FASES DE DESARROLLO

Así mismo para el análisis en la herramienta de monitoreo, con respecto a la gestión de eventos, se tomará las mejores prácticas indicadas en *ITIL* que ayude a gestión de servicios de TI como parte de la etapa de operación dentro del ciclo de vida del servicio para el proveedor de servicio.

Esta tesis se divide en 3 fases para la implementación del nuevo sistema de monitoreo de servidores y aplicaciones, las cuáles se describen a continuación:

Fase 01: Evaluación de requerimientos del sistema de monitoreo para servidores y aplicaciones

En esta fase se realizará la formulación de los requerimientos que el sistema de monitoreo deba cumplir para satisfacer la necesidad del área usuaria y se formulará el documento de requerimiento de propuesta (*RFP*) de servicios que contengan los alcances solicitados por el área usuaria.

Fase 02: Evaluación de la herramienta para el sistema de monitoreo para servidores y aplicaciones

En esta fase, se realizará la evaluación técnica-económica de todas las herramientas ofrecidas por los distintos proveedores de servicios que cumplan lo solicitado en el *RFP* y se emitirá la matriz de evaluación de las características con los puntajes establecidos para que se tome una decisión para la herramienta el sistema de monitoreo de servidores y aplicaciones.

Fase 03: Implementación del sistema de monitoreo de servidores y aplicaciones

En esta fase se realizará el diseño de la arquitectura del sistema de monitoreo de servidores y aplicaciones, en donde se detallan los requerimientos necesarios para el correcto despliegue del sistema y se realizará el despliegue del monitoreo en producción del nuevo sistema. Además se elaborará la documentación final para el posterior despliegue de toda la migración de equipos del centro de cómputo.

Seguidamente, demos inicio al desarrollo de esta tesis a través de la presentación de la empresa estudiada y los procesos de negocio involucrados, como se explica a continuación en el capítulo II.

2 CAPÍTULO II: MARCO CONTEXTUAL

2.1 DESCRIPCIÓN DE LA EMPRESA DONDE SE DESARROLLA LA TESIS

GMD, es la empresa de *Outsourcing* de Procesos de Negocios y *Outsourcing* de Tecnología de la Información (TI) con mayor confiabilidad y experiencia del Perú. Forma parte del grupo de ingeniería #1 del Perú, Graña y Montero y cuenta con 30 años de experiencia desarrollando e implementando exitosamente soluciones que generan valor a los procesos de negocios de sus clientes, un staff de más de 2000 profesionales y certificaciones internacionales como *ISO 9001*, *ISO 27001*, *OSHAS 1800*, *ISO 20000*, *NTP 392-030* y metodologías de clase mundial *CMMI-3*, *ITIL* y *PMI*, que le han permitido consolidar su operación.

GMD cuenta con la mejor infraestructura, la fábrica de software más grande del país, 2 *datacenter* de clase mundial, 1 de los cuales está certificado *Tier III* y 2 *call center* en alta disponibilidad para los servicios de mesa de ayuda.

Desde el inicio de sus operaciones en 1984, GMD ha crecido por encima de las predicciones del mercado gracias a su estrategia de flujos estables lo que le ha permitido sentar las bases para un crecimiento sólido y seguro. Hoy GMD es una organización de clase mundial con más de 250 clientes corporativos.

Recientemente, GMD ha sido reconocida como la empresa líder en soluciones de *Outsourcing* en el Perú, por la empresa de *IDC* (International Data Corporation), líder en investigación de mercado.

Los ingresos anuales de GMD en el 2015 ascendieron a \$83 millones, de los cuales US\$ 64 millones provienen de los negocios de *Outsourcing*, que representa un 77% de la actividad total de GMD.

2.2 MACRO PROCESO DE LA ORGANIZACIÓN

Los macro procesos de negocio de GMD y sus filiales se muestran en la **Figura N°1**. A continuación se describirán los macro procesos establecidos para poder cumplir con los objetivos de negocio de GMD:

SGI.MP.01 PROCESOS GENERALES GMD

Este macro proceso permite establecer, documentar, implementar y mantener el sistema de gestión integrado (SGI) de GMD y sus filiales, así como mejorar continuamente su eficacia de acuerdo con los requisitos de la norma *ISO 9001:2008*.

MACRO PROCESO: RESPONSABILIDAD DE LA DIRECCIÓN

Este macro proceso proporciona evidencia del compromiso de la alta gerencia para desarrollar e implantar el Sistema de Gestión Integrado (SGI) y la mejora continua de la eficacia del mismo.

MACRO PROCESO: GESTIÓN DE LOS RECURSOS

Este macro proceso determina y proporciona los recursos necesarios para implementar y mantener el Sistema de Gestión Integrado y aumentar la satisfacción del cliente mediante el cumplimiento de sus requisitos.

MACRO PROCESO: REALIZACION DEL PRODUCTO

Este macro proceso permite planificar y desarrollar los procesos necesarios para la realización del producto. Esta planificación es coherente con los requisitos de los otros procesos del Sistema de Gestión Integrado. El resultado de esta planificación se presenta a través de planes de calidad.

MACRO PROCESO: MEDICIÓN, ANÁLISIS Y MEJORA

Este macro proceso permite planificar e implementar los procesos de seguimiento, medición, análisis y mejora necesarios para demostrar la conformidad con los requisitos del servicio, asegurar la conformidad del Sistema de Gestión de Calidad y mejorar continuamente la eficacia del Sistema de Gestión Integrado. Esto comprende la determinación de métodos aplicables, incluyendo técnicas estadísticas, y el alcance de su uso.

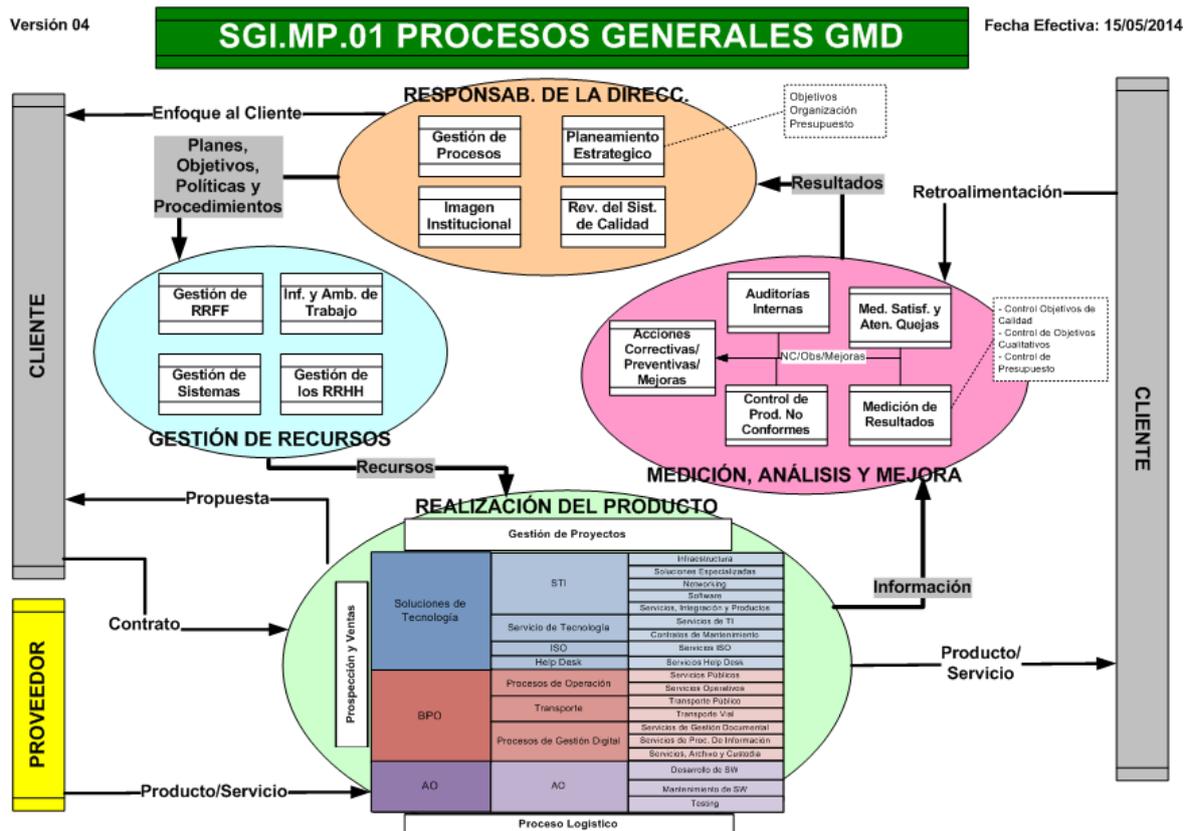


Figura N° 1: SGI.MP.01 Procesos Generales GMD

Fuente: Sistema de conocimiento propio de GMD

2.3 PRESENTACIÓN DEL ÁREA FUNCIONAL

En la figura N°2, se muestran los procesos del área de *Datacenter*, sobre el cual se implantó el nuevo sistema de monitoreo. Este nuevo sistema afectará al subproceso denominado “monitoreo”, y dentro de esta subproceso, se realizará la mejora en la actividad específica de monitoreo.

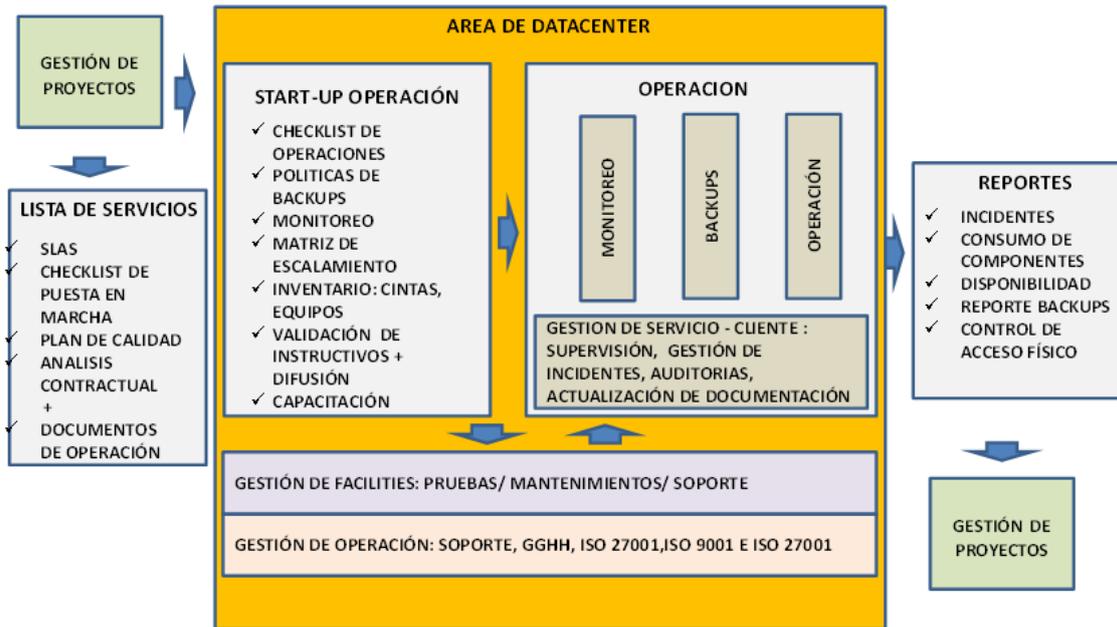


Figura N° 2: Procesos del Área Servicios Datacenter

Fuente: Sistema de conocimiento propio de GMD

La actividad denominada monitoreo, consiste en realizar el monitoreo preventivo para determinar si los sistemas informáticos superan los umbrales establecidos ocasionando de esta manera comportamiento anómalo en las operaciones diarias.

En el capítulo siguiente, se desarrolla el marco conceptual de la presente tesis, que detalla y explica la evolución de las herramientas de monitoreo de redes, sus tendencias de acuerdo a lo exigido por el mercado de tecnología de información para estar alineado a los procesos de negocios de los distintos clientes y las metodologías y buenas prácticas empleadas para la gestión del proyecto a través de las buenas prácticas de *PMI* y la gestión de eventos a través de *ITIL* respectivamente.

3 CAPÍTULO III: MARCO CONCEPTUAL

3.1 DIRECCIÓN DE PROYECTOS

La Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®) — Quinta Edición establece lineamientos para la dirección de proyectos individuales y define conceptos relacionados con la dirección de proyectos.

La Guía del PMBOK® contiene el estándar, reconocido a nivel global y la guía para la profesión de la dirección de. Por estándar se entiende un documento formal que describe normas, métodos, procesos y prácticas establecidos.

Para poder continuar, es necesario saber que es un proyecto: *“Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. La naturaleza temporal de los proyectos implica que un proyecto tiene un principio y un final definidos. El final se alcanza cuando se logran los objetivos del proyecto, cuando se termina el proyecto porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto.”* ((Guía del PMBOK®) — Quinta edición, 2013, p. 10).

Como se ve, un proyecto puede generar un servicio, como en el caso de GMD, es por ello que es necesario llevar una adecuada dirección de proyectos, pero ¿qué es la dirección de proyectos?. Bien, de acuerdo a la guía del PMBOK – Quinta Edición, *“La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo. Se logra mediante la aplicación e integración adecuadas de los 47 procesos de la dirección de proyectos, agrupados de manera lógica, categorizados en cinco Grupos de Procesos. Estos cinco Grupos de Procesos son; 1) Inicio, 2) Planificación, 3) Ejecución, 4) Monitoreo y Control, y 5) Cierre.”*.

En este sentido, esta tesis incorpora las mejores prácticas de mercado con relación a la dirección de proyectos, estando estructurado de acuerdo con cada uno de los grupos de procesos para llevar el adecuado control del proyecto de implementación.

3.2 GESTIÓN DE EVENTOS

La gestión de eventos, de acuerdo a ITIL v3, inicia con el monitoreo de todos los sucesos importantes que se produzcan para poder anticiparse a los problemas, resolverlos o incluso prevenirlos. Esta función representa una tarea en sí misma y por tanto constituye un proceso independiente dentro del ciclo de vida: la Gestión de Eventos.

De acuerdo a ITIL v3, 2011, *“Se denomina evento a todo suceso detectable que tiene importancia para la estructura de la organización TI, para la prestación de un servicio o para la evaluación del mismo. Ejemplos típicos de eventos son las notificaciones creadas por los servicios, los elementos de configuración o las herramientas de monitorización y control”*.

Es por ello que lo más importante en la Gestión de Eventos es, una buena monitorización y unos efectivos sistemas de control, los cuáles existen de dos tipos:

- Herramientas de monitorización activa. Se comprueban los elementos de configuración uno a uno para verificar su estado y disponibilidad. Si detecta excepciones, la herramienta de monitorización genera una alerta y la envía al equipo o mecanismo de control asignado.
- Herramientas de monitorización pasiva. Detectan y correlacionan alertas operacionales generadas por los propios elementos de configuración.

Existen varios tipos de eventos dependiendo de su impacto en el sistema:

- Eventos que indican que el servicio está operando con normalidad.
- Eventos que indican una excepción.
- Eventos que indican una operación inusual pero no excepcional, y que requieren una monitorización exhaustiva.

La Gestión de Eventos, además de detectar y notificar los sucesos, se encarga de clasificarlos y dimensionar su impacto en el servicio. Llegado el caso, se ocupa también de documentar el evento y derivarlo al proceso correspondiente para que tome medidas:

- A la Gestión de Incidencias, en caso de que el evento suponga una interrupción no planificada del servicio o fallos en uno o más elementos de configuración.
- A la Gestión de Problemas, si una incidencia se repite a menudo y no se conoce la causa que la provoca.

Y también envía a la Gestión de Cambios, a través de la Mejora Continua del Servicio, nuevas solicitudes de cambio basadas en la correlación de eventos.

3.3 EVOLUCIÓN Y TENDENCIAS DE LAS HERRAMIENTAS DE MONITOREO DE REDES

Presentar la información de su operación de manera tal que los ejecutivos de la organización, cuyo conocimiento en tecnología es mínima, dispongan de elementos suficientes para reconocer y fomentar la importancia de la tecnología como un componente habilitador del negocio, es uno de los retos que tienen los ejecutivos de TI, hoy en día.

Han sido muchos los esfuerzos para hacer que la industria acuerde un estándar universal, primeramente a través de protocolos como CMIP (*Common Management Information Protocol*), o SNMP (*Simple Network Management Protocol*), o bien a través de plataformas donde converge la información de todos los recursos de TI, como *HP Openview*, *IBM Tivoli*, *Sun Solstice* o *CA Infrastructure Management*, entre otros.

La evolución de las herramientas de monitoreo también se ha ido alimentando mediante la llegada de protocolos más avanzados de visualización de tráfico como *NetFlow*, *Jflow*, *Cflow*, *sflow*, *IPFIX* o *Netstream*. El propósito hoy es tener una perspectiva global del “todo” para

categorizar adecuadamente los eventos que afectan el desempeño de un servicio o del proceso de negocio involucrado.

Este arduo camino ha atravesado diferentes etapas como parte de su evolución y podríamos enumerarlas de la siguiente forma:

3.3.1 PRIMERA GENERACIÓN

La industria ha desarrollado un sinnúmero de herramientas para tratar de presentar los recursos de una forma amable y en tiempo real. “Ahí, donde está la caja en rojo, eso quiere decir que el *router* está fuera de servicio, por eso no hay conexión a la planta”, esto es lo que dice el operador de la consola de monitoreo al contralor que ha solicitado previamente un reporte al momento de mermas en las líneas de producción para un artículo que está por lanzarse al mercado.

Las herramientas de monitoreo mostraban los elementos a través de un código universal de colores:

- En verde: todo está funcionando bien;
- En amarillo: se detectó que hay algún problema temporal que no afecta la disponibilidad, sin embargo, se deben realizar ajustes para no perder la comunicación;
- En naranja: el problema se ha hecho persistente y requiere pronta atención para evitar afectaciones a la disponibilidad;
- En rojo: el dispositivo se encuentra fuera de servicio en este momento y requiere acciones inmediatas para su restablecimiento.

Parece muy sencillo comprender esta convención de colores pero usualmente el nivel de detalle es insuficiente ¿Qué pasa si el dispositivo que está en rojo sí está en funcionamiento y aun así no está realizando su función habitual? En la figura N° 3 se muestra un ejemplo de una herramienta de monitoreo de 1ª generación:



Figura N° 3: Ejemplo de monitoreo de 1ª Generación

Fuente: Evolución y tendencias de las herramientas de monitoreo de redes, Esteban San Ramón, 21/01/2011.

3.3.2 SEGUNDA GENERACIÓN

La siguiente generación de herramientas hace lo que se llama “*drill down*” o “análisis a profundidad” con el fin de evaluar el estado de los componentes dentro del dispositivo (*CPU*, memoria, espacio de almacenamiento, paquetes enviados y recibidos, broadcast, multicast, *etc.*) de manera que se puedan buscar los parámetros de ajuste y que, de la misma forma en que se aprieta una tuerca en un engranaje de una máquina, los valores que se modifiquen permitan elevar los niveles de servicio del dispositivo. En la figura N°4 se muestra un ejemplo de monitoreo de 2ª generación:



Figura N° 4: Ejemplo de monitoreo de 2ª Generación

Fuente: Evolución y tendencias de las herramientas de monitoreo de redes, Esteban San Ramón, 21/01/2011.

Este tipo de aplicaciones se apoyan en analizadores de protocolos o “*sniffers*” y en elementos físicos distribuidos conocidos como “*probes*”, cuya función es exclusivamente la de coleccionar estadísticas del tráfico y que son controlados típicamente desde una consola central.

Si volvemos al mismo escenario del operador con estas nuevas posibilidades, éste sería un ejemplo de su argumento para explicar por qué no se genera el reporte: “Las estadísticas de transmisión de paquetes nos indican que la interfaz WAN 3 del *router* está transmitiendo con altos niveles de *broadcast*, lo que está provocando que haya malos tiempos de respuesta y que, en consecuencia, se produzcan retransmisiones de paquetes”.

Tenemos considerablemente mayor información pero aún no hemos podido llevarla de una manera tangible a un ejecutivo del negocio para valorar conjuntamente el nivel de afectación que se esté dando.

3.3.3 TERCERA GENERACIÓN

Con mayores niveles de información sobre los dispositivos tenemos elementos adicionales de análisis, pero aún no existen suficientes parámetros para tomar decisiones. Ahora un problema es provocado por la conjunción de varios dispositivos que participan dentro de un

mismo servicio; la visión debe ser más integral y en la medida de lo posible correlacionar el comportamiento de elementos tan autónomos y dispersos como una base de datos, un servidor, un *switch* y hasta un enlace de comunicaciones, pero al mismo tiempo mantenerlos interdependientes porque todos participan en un mismo servicio, por ejemplo, una consulta de inventarios o el requerimiento de un pedido.

Esta generación de aplicaciones con enfoque transaccional captura ahora “flujos” de tráfico e identifica cuellos de botella y latencias a lo largo de las conexiones que existen entre los componentes de un servicio, y entrega información acerca de la salud del mismo. En la figura N° 5 se muestra un ejemplo del monitoreo de 3ª generación comentado:

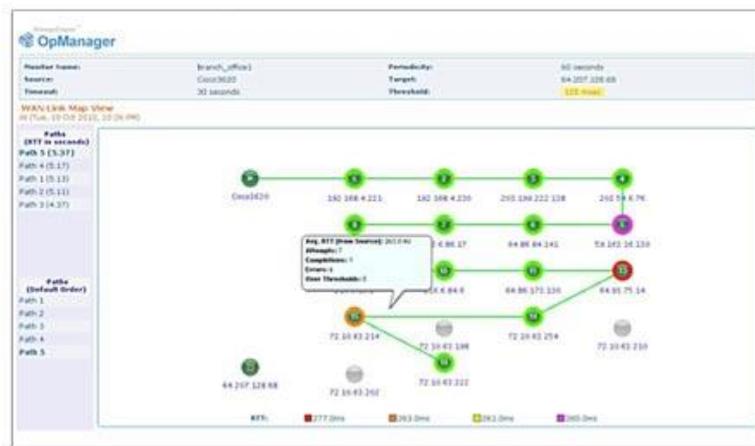


Figura N° 5: Ejemplo de monitoreo de 3ª Generación

Fuente: Evolución y tendencias de las herramientas de monitoreo de redes, Esteban San Ramón, 21/01/2011.

Haciendo el símil con un eventual caso de la vida real, se tendría una explicación más o menos como la siguiente: “...los niveles de uso de *CPU* en el servidor de base de datos están en picos que van por arriba de 80%, esto aumenta los tiempos de respuesta de la aplicación web y entonces se genera un alto número de retransmisiones que saturan el actual ancho de banda que tenemos; esta serie de factores se reflejan en que el Servicio de Consulta de Créditos en línea sea uno de los primeros afectados...”

Esta vez hemos logrado construir un puente entre los elementos de tecnología y los servicios que están disponibles para cualquier usuario de la organización. Ahora podríamos decir que todas las partes hablan el mismo lenguaje y que las decisiones podrán ser tomadas con un enfoque de la repercusión que generan en el negocio.

3.3.4 CUARTA GENERACIÓN

Llevando el crecimiento de las soluciones tecnológicas a los requerimientos de las organizaciones de hoy, llegamos a las vistas de “*dashboard*” que son indicadores que el cliente puede crear y personalizar de acuerdo a sus necesidades, además de poder seleccionar las variables que requiere correlacionar para mostrar de una manera gráfica a los tomadores de decisiones qué nivel de cumplimiento se está entregando en los procesos de negocio.

Dentro de esta generación de soluciones están aquellas que monitorean el desempeño de aplicaciones (APM, por sus siglas en inglés), donde convergen elementos de tecnología (“*Backend*”) con los sistemas de los que forman parte, y éstos con las aplicaciones que integran para llevar a cabo las transacciones que impulsan los procesos de negocio (“*Frontend*”). Esto, en otras palabras, es el análisis de punta a punta, como se muestra en la figura N° 6:



Figura N° 6: Ejemplo de monitoreo de 4ª Generación

Fuente: Evolución y tendencias de las herramientas de monitoreo de redes,
Esteban San Ramón, 21/01/2011.

El potencial de estas herramientas permite tener información simultánea de:

- Visibilidad de la infraestructura.
- Predicciones de desempeño.
- Modelado de escenarios (simulación y emulación).
- Análisis y planeación de capacidad.
- Funcionalidades de ajustes a las configuraciones.
- Mediciones de impacto al negocio (calidad, salud y riesgos en los servicios prestados).
- Experiencia del usuario.

Así pues, muchas de estas herramientas cuentan con modalidades como el análisis Causa-Raíz (“*top-down*”) que llegan hasta el ulterior elemento de tecnología que forma parte de la infraestructura del cliente; del mismo modo, a través de la integración de los elementos de la solución, se tendrán los medios para determinar cuáles son los impactos al negocio (*bottom up*) derivados de la falla de un recurso de TI.

Con esta incorporación se da visibilidad de punta a punta a transacciones críticas en ambientes que hoy proliferan en las organizaciones de las que usted y yo formamos parte y que involucran *J2EE* y *.NET*.

A través de este tipo de soluciones, la información ya está disponible a cualquier nivel en el contexto adecuado, y solamente se tiene que ver el indicador para mostrar el proceso de negocio afectado. Así pues, se podrán hacer afirmaciones del tipo “... el negocio está captando y atendiendo adecuadamente a nuestros clientes, y la expectativa de resultados en este momento nos permite afirmar que se cumplirán los objetivos de acuerdo a lo presupuestado...”

En la figura N° 7 se demuestra cómo se ha venido dando la evolución de las herramientas de monitoreo de acuerdo a lo explicado:



Figura N° 7: Evolución de herramientas de monitoreo

Fuente: Evolución y tendencias de las herramientas de monitoreo de redes, Esteban San Ramón, 21/01/2011.

Los fabricantes se han alineado a las más recientes tendencias de virtualización y cómputo en la nube, igualmente han ido sofisticando los métodos de medición con el fin de resultar lo menos intrusivos en las redes que monitorean. Al introducir “*probes*”, “*taps*” o “*switches*” con funcionalidades “*SPAN*” o “*port mirroring*”, y al mismo tiempo “*appliances*”, con mucha mayor capacidad de captura para almacenar la información de semanas o inclusive meses, las posibilidades de las herramientas de monitoreo han logrado superar las expectativas.

La clave siempre ha estado en la proactividad, es decir, anticiparse a una degradación en la experiencia del usuario final sobre los recursos de información; independientemente de que los indicadores sean técnicos o enfocados a procesos de negocio. Para tener la posibilidad de “afinar” en vez de “arreglar” es fundamental que las herramientas de monitoreo se acoplen adecuadamente a la infraestructura que estarán supervisando.

Se muestra a continuación el capítulo IV, dónde se explica el marco metodológico sobre el cual se ha basado el desarrollo de la tesis.

4 CAPÍTULO IV: MARCO METODOLÓGICO

Esta tesis incorpora las mejores prácticas de mercado con relación a la administración de proyectos, estando estructurado de acuerdo con la metodología mundial basada en las mejores prácticas adoptadas por el Instituto de “PMI - *Project Management Institute*”, de los Estados Unidos de América, reconocido mundialmente como formulador de los más altos estándares de calidad en la gestión de proyectos.

Así mismo para la gestión de eventos se tomará las mejores prácticas indicadas en *ITIL* que ayude a gestión de servicios de TI como parte de la etapa de operación dentro del ciclo de vida del servicio para el proveedor de servicio.

El trabajo realizado a lo largo del proceso de definición de la solución de monitoreo para servidores y aplicaciones está marcado por 3 fases: Evaluación de requerimientos del sistema de monitoreo para servidores y aplicaciones, Evaluación de la herramienta para el sistema de monitoreo para servidores y aplicaciones e Implementación del sistema de monitoreo de servidores y aplicaciones.

A continuación se muestra el detalle de las actividades y herramientas a usar con respecto a lograr los objetivos específicos y las fases identificadas:

4.1 FASE 01: EVALUACIÓN DE REQUERIMIENTOS

En la tabla N°1, se mencionan las actividades para cumplir los objetivos de la fase 01 así como las herramientas que se necesitan para cumplir dichas actividades:

Tabla N° 1: Cuadro de actividades para cumplir objetivos de la fase 01

Objetivo	Actividad	Herramienta
Realizar la evaluación de requerimientos de la nueva herramienta para el sistema de monitoreo de servidores y aplicaciones que integre todo el alcance de monitoreo a fin de reducir la complejidad de despliegue de agentes	Levantamiento de información de la solución actual	Diagrama de arquitectura de las plataformas actuales Información actual de todos los componentes que se monitorearán
	Análisis de situación actual	Identificación de <i>Stakeholders</i> Entrevista con áreas internas Entrevista con áreas internas
	Desarrollo de documento RFP	Documento Word de tipo RFP

4.2 FASE 02: EVALUACIÓN DE LA HERRAMIENTA

En la tabla N°2, se mencionan las actividades para cumplir los objetivos de la fase 02 así como las herramientas que se necesitan para cumplir dichas actividades:

Tabla N° 2: Cuadro de actividades para cumplir objetivos de la fase 02

Objetivo	Actividad	Herramienta
Realizar la evaluación técnica-cualitativa de la	Elaboración de la matriz de evaluación técnica	Herramienta Excel con tabla de puntuación técnica con respecto

Objetivo	Actividad	Herramienta
nueva herramienta para el sistema de monitoreo de servidores y aplicaciones para contar con una única plataforma de monitoreo integrada y centralizada		a los criterios de evaluación establecidos en el RFP
	Selección de la mejor solución	Presentación con análisis y resultados de la tabla de puntuación técnica y cualitativa. Análisis final de áreas internas identificadas

4.3 FASE 03: IMPLEMENTACIÓN DEL SISTEMA

En la tabla N°3, se mencionan las actividades para cumplir los objetivos de la fase 03 así como las herramientas que se necesitan para cumplir dichas actividades:

Tabla N° 3: Cuadro de actividades para cumplir objetivos de la fase 03

Objetivo	Actividad	Herramienta
Realizar la implementación de la herramienta para el sistema de monitoreo de servidores y aplicaciones de los servicios de Hosting para brindar fácil acceso a información en tiempo real	Diseño Técnico	Diseño inicial Arquitectura de solución
	Implementación de sistema de monitoreo de servidores y aplicaciones	Arquitectura, diagrama de gant, recursos, plan de comunicaciones Plan de trabajo detallado del cambio Documentos de solicitudes de cambio en producción

A continuación se muestra la figura N° 8, dónde se muestra el diagrama de secuencia de actividades utilizado para el desarrollo de esta tesis:

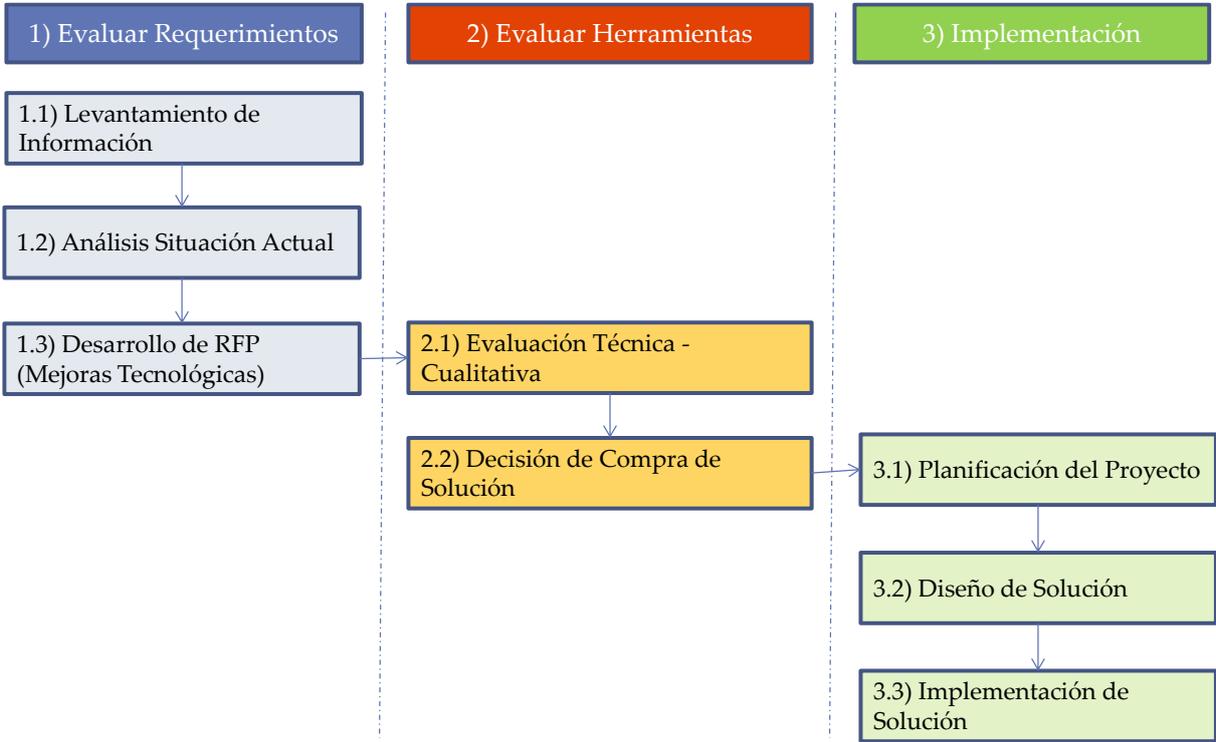


Figura N° 8: Diagrama de secuencia del proyecto

Fuente: Propia

En el siguiente capítulo desarrollaremos las actividades del primer objetivo: Evaluación de requerimientos; que consiste en la recopilación de información, análisis de situación actual y desarrollo de RFP para el nuevo sistema de monitoreo.

5 CAPÍTULO V: EVALUACIÓN DE REQUERIMIENTOS PARA EL SISTEMA DE MONITOREO

5.1 LEVANTAMIENTO DE INFORMACIÓN DE LA SOLUCIÓN ACTUAL

A continuación, en la figura N° 9, se muestra la arquitectura actual de monitoreo de GMD.

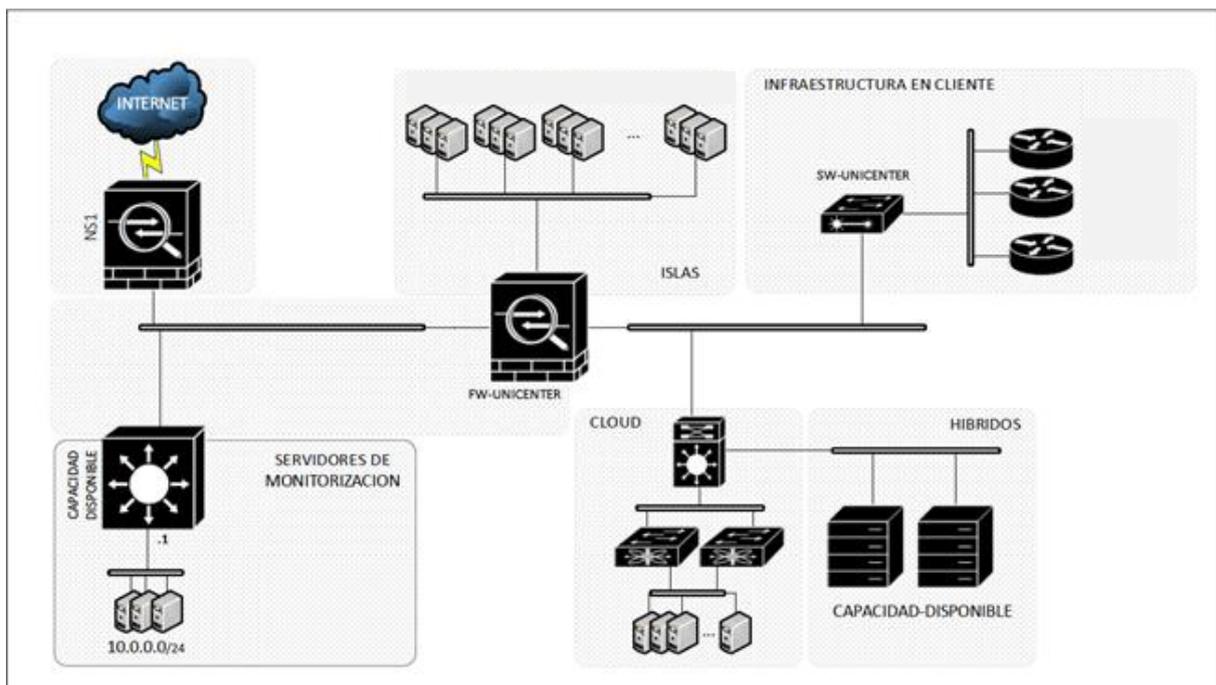


Figura N° 9: Arquitectura de red de monitoreo de GMD actual

Fuente: Sistema de conocimiento propia de GMD

Se pueden distinguir claramente varios segmentos de red:

- **Red de Monitorización.-** es el segmento de red donde están ubicados los servidores principales de la solución de monitoreo. Esta red está en el segmento 10.0.0.0/24.
- **Infraestructura en Cliente.-** conformada por los enlaces hacia las sedes de los clientes de GMD en donde residen los servidores de los clientes. En total, son 3 clientes que conforman esta red externa en donde GMD monitorea sus respectivos servidores.

- **Red Cloud.-** conformada por varios segmentos de red. Cada uno perteneciente a un cliente diferente de GMD cuya infraestructura son provistas sobre la plataforma Cloud Privada que ofrece GMD.
- **Red Híbridos.-** conformada por diferentes segmentos de red, cada uno de ellos perteneciente a un cliente diferente que permite el acceso a la red Cloud e infraestructura en Cliente
- **Red Islas.-** conformada por diferentes segmentos de red cada uno de ellos perteneciente a un cliente diferente y que no tienen comunicación con otras redes en GMD.

Nota.- para llegar a cualquiera de los servidores, desde la red de monitorización, ubicados en la Red Híbridos, Red Cloud, Red Infraestructura en Cliente, o red Islas, es necesario pasar por un servidor *firewall* por el lado de GMD y en el caso de los clientes remotos (Infraestructura en cliente) cada cliente cuenta con su propio *firewall* por lo que la apertura de puertos a realizar también debe ser realizada en estos *firewalls* de clientes.

5.2 ANÁLISIS DE LA SITUACIÓN ACTUAL

Una parte fundamental para que el proyecto tenga éxito es la identificación de los interesados durante la ejecución del proyecto. En la tabla N°4, se muestra la relación de los interesados del proyecto dentro de la empresa GMD, como se muestra a continuación:

Tabla N° 4: Identificación de interesados y nivel de interés o influencia

Cargo	Interés o influencia	Opinión del Proyecto
Gerente de Línea ISO	Muy Alta	Ofrecer un nuevo servicio de monitoreo basado en aplicaciones
Gerente de Servicios Datacenter	Alta	Aumentar el nivel de servicio ofrecido a sus clientes

Cargo	Interés o influencia	Opinión del Proyecto
Gerente de Operaciones ISO	Alta	Busca reducir costos operacionales asociados a la compleja administración
Jefe de Operaciones ISO	Media	Busca reducir complejidad administrativa de sus colaboradores
Operador de Turno Senior	Media	Interesado en utilizar la nueva consola de alertas

Luego se realizaron entrevistas con las áreas internas dónde se identificaron los requerimientos, indicados en la tabla N°5, que debe cubrir la herramienta de monitoreo. En total se listado 39 requerimiento del área usuario a satisfacer.

Tabla N° 5: Tabla de requerimientos de herramienta de monitoreo

Ítem	Requerimiento a cubrir por la herramienta de monitoreo
Requerimiento 01	Monitoreo nivel básico (memoria, disco, procesamiento y disponibilidad)
Requerimiento 02	Monitoreo de puertos.
Requerimiento 03	Monitoreo de procesos.
Requerimiento 04	Monitoreo de Disk I/O (Lectura y Escritura)
Requerimiento 05	Monitoreo de eventos del sistema operativo.
Requerimiento 06	Monitoreo de los Puertos Físicos de los servidores.
Requerimiento 07	Monitoreo de disponibilidad de páginas web. Ejemplo: www.gmd.com.pe/Portal

Ítem	Requerimiento a cubrir por la herramienta de monitoreo
Requerimiento 08	Monitoreo de almacenamiento de diferentes fabricantes, análisis en tiempo real de la actividad de LUNS.
Requerimiento 09	Monitoreo para sistemas de archivos distribuido (DFS).
Requerimiento 10	Monitoreo para sistemas Exchange con replicación (DAG), operatividad de las bases de datos.
Requerimiento 11	Monitoreo de clúster de distintas herramientas (por ejemplo el service guard, red hat suit).
Requerimiento 12	Monitoreo de replicación de distintos herramientas (por ejemplo el Business Copy, Continuos Access).
Requerimiento 13	Monitoreo de disk groups (Falla física).
Requerimiento 14	Monitoreo online de consumo de memoria por procesos (muy parecido a un “task manager”).
Requerimiento 15	Monitoreo del fallo de cualquier componente de un equipo sea este un servidor, switchs lan o san, firewall, etc. (Fuentes de Poder, Memoria RAM, CPU, Tarjetas de Red, Tarjetas HBA).
Requerimiento 16	Alertas en base a lectura de cadenas en un determinado archivo (lectura de log a nivel de sistema operativo).
Requerimiento 17	Ejecución de tareas cuando se emite una determinada alerta (Activación del mismo agente SNMP, mediante la ejecución de un script remoto desde el servidor).
Requerimiento 18	VCENTER: Disponibilidad del VCenter y tiempo de respuesta.
Requerimiento 19	VCENTER: Performance de los ESXi CPU, memoria, Discos.
Requerimiento 20	VCENTER: Performance de las Máquinas virtuales.
Requerimiento 21	VCENTER: Performance del storage.

Ítem	Requerimiento a cubrir por la herramienta de monitoreo
Requerimiento 22	VCENTER: Visualización de todo el VCenter Por medio de un dashboards unificado.
Requerimiento 23	Reporte de rendimiento de recursos (CPU, Memoria, Disco, I/O de Disco, Disponibilidad, Paginación etc).
Requerimiento 24	Reporte de temperatura de recursos (Fuentes de Poder, Memoria RAM, CPU, Tarjetas de Red, Tarjetas HBA).
Requerimiento 25	Reporte En tiempo real y Por periodos de I/O de Discos.
Requerimiento 26	Reporte de consumo de energía de recursos (Fuentes de Poder, Memoria RAM, CPU, Tarjetas de Red, Tarjetas HBA).
Requerimiento 27	REDES: Monitoreo/Reportes (RAM,CPU, Flash, Temperatura, Fuente, Ventiladores)
Requerimiento 28	REDES: Monitoreo Throughput
Requerimiento 29	REDES: Estado (L1/L2/L3)
Requerimiento 30	REDES: Estado (L2/L3)
Requerimiento 31	REDES: Monitoreo y reportes de SVI
Requerimiento 32	REDES: Monitoreo y reportes de Ancho de Banda
Requerimiento 33	REDES: Monitoreo por IP, Servicio o Aplicación (Voz, Datos y Video), en dispositivos de L2/L3 y Firewall.
Requerimiento 34	REDES: Monitoreo y reportes de Puertos Físicos:
Requerimiento 35	REDES: Monitoreo y reportes de Disponibilidad de VPN's
Requerimiento 36	REDES: Monitoreo y reportes de Servicios Publicados
Requerimiento 37	REDES: Monitoreo y reportes online del tráfico I/O SAN

Ítem	Requerimiento a cubrir por la herramienta de monitoreo
Requerimiento 38	Integración con el sistema Help Desk para la generación de ticket automático.
Requerimiento 39	Acceso a la consola vía web.

Una vez identificados el alcance de las características mínimas del sistema de monitoreo se convocaron a los siguientes proveedores con representación local en Lima, Perú, para que puedan realizar las consultas sobre los alcances indicados en el punto anterior. En la tabla N°6 se muestran los dos proveedores identificados, los cuáles fueron convocados a participar en la evaluación.

Tabla N° 6: Cuadro de identificación de proveedores del servicio

Ítem	Proveedor
1	CA
2	GIS

5.3 DESARROLLO DE DOCUMENTO RFP

El desarrollo del documento RFP constituyó el conjunto de normas establecidas por GMD S.A. para reglamentar el concurso de postores para el Servicio de Monitoreo de Infraestructura el cual se rigió por las condiciones detalladas en dicho documento. GMD S.A. requiere identificar a un proveedor que pueda brindar una solución para el monitoreo de los equipos que alberga sus Datacenter Principal y Contingencia, los cuales brindan servicios a sus cliente en la Modalidad de Hosting. La documentación descrita en este capítulo fue utilizada para la formulación del documento RFP para el sistema de monitoreo de servidores y aplicaciones.

En el capítulo a continuación desarrollaremos las actividades para cumplir nuestro segundo objetivo: Evaluación técnica-cualitativa del nuevo sistema de monitoreo, sigamos.

6 CAPÍTULO VI: EVALUACIÓN DE LA HERRAMIENTA DEL SISTEMA DE MONITOREO

6.1 ELABORACIÓN DE LA MATRIZ DE EVALUACIÓN TÉCNICA

Para la elaboración de la matriz de evaluación técnica se descompusieron dos (02) tipos de criterios. La evaluación de las características solicitadas en el RFP para el componente Software. A continuación se muestra la tabla N°7, que muestra la matriz de evaluación técnica y la ponderación de los puntajes obtenidos por las herramientas Orion SolarWinds y CA NimSoft Monitor con respecto al componente de software.

Tabla N° 7: Tabla de puntuación técnica del componente software de la herramienta del sistema de monitoreo

Ítem	Peso	GIS	CA	SolarWinds	NimSoft
Requerimiento 01	3	10	10	30	30
Requerimiento 02	2	10	10	20	20
Requerimiento 03	3	10	10	30	30
Requerimiento 04	2	10	10	20	20
Requerimiento 05	2	10	10	20	20
Requerimiento 06	3	10	10	30	30
Requerimiento 07	2	10	10	20	20
Requerimiento 08	3	6	10	18	30
Requerimiento 09	1	6	6	6	6
Requerimiento 10	1	6	10	6	10
Requerimiento 11	1	6	6	6	6

Ítem	Peso	GIS	CA	SolarWinds	NimSoft
Requerimiento 12	1	6	6	6	6
Requerimiento 13	1	8	8	8	8
Requerimiento 14	1	10	10	10	10
Requerimiento 15	2	8	8	16	16
Requerimiento 16	1	10	10	10	10
Requerimiento 17	1	10	10	10	10
Requerimiento 18	3	10	10	30	30
Requerimiento 19	3	10	10	30	30
Requerimiento 20	3	10	10	30	30
Requerimiento 21	3	10	10	30	30
Requerimiento 22	3	10	10	30	30
Requerimiento 23	3	10	10	30	30
Requerimiento 24	1	6	6	6	6
Requerimiento 25	2	10	10	20	20
Requerimiento 26	2	8	8	16	16
Requerimiento 27	3	10	10	30	30
Requerimiento 28	1	10	10	10	10
Requerimiento 29	3	10	10	30	30
Requerimiento 30	3	10	10	30	30
Requerimiento 31	3	10	10	30	30
Requerimiento 32	3	10	10	30	30

Ítem	Peso	GIS	CA	SolarWinds	NimSoft
Requerimiento 33	2	10	10	20	20
Requerimiento 34	3	10	10	30	30
Requerimiento 35	1	10	10	10	10
Requerimiento 36	2	10	10	20	20
Requerimiento 37	1	10	10	10	10
Requerimiento 38	1	10	10	10	10
Requerimiento 39	1	10	10	10	10
Total de evaluación de herramienta	80	360	368	758	774
Puntuación total en base a 40 puntos				38	39

La calificación de las herramientas de monitoreo ha sido realizada por un comité técnico de GMD, y cuyo resultado de la evaluación técnica del software se muestra en la tabla N°8, dónde se muestra el promedio ponderado para la puntuación de los productos realizado sobre un puntaje total de 40 puntos:

Tabla N° 8: Tabla resumen de puntuación técnica del componente software de la herramienta del sistema de monitoreo

SOLAR WINDS	NIMSOFT
38	39

Como se puede apreciar, la evaluación técnica ha sido reñida entre ambos componentes, siendo ganadora la solución NimSoft de CA.

6.2 SELECCIÓN DE LA MEJOR SOLUCIÓN

Una vez establecido los criterios técnicos y evaluación de las características de las soluciones, se procedió a realizar la evaluación cualitativa de las herramientas.

Así mismo, en la tabla N°9, se muestra el cuadro comparativo sobre los beneficios cualitativos, a manera resumen, de ambas herramientas evaluadas:

Tabla N° 9: Cuadro comparativo de beneficios cualitativos

Cuadro comparativo de soluciones (Beneficios cualitativos)	SolarWinds (Orion)	CA (NimSoft)
Alineamiento del ROADMAP con los objetivos de la empresa	No	Si
PARTNER de GMD	No	Si
Beneficios colaterales (Puntos Partners, prestigio de la empresa proveedora)	Medio	Alto
Nivel de Integración con herramientas implementadas	Si	Nativa
Curva de aprendizaje (Disrupción con solución actual)	Alto	Bajo

En la tabla N° 10, se muestra el el cuadro resumen de la evaluación de la mejor solución.

Tabla N° 10: Cuadro resumen de la evaluación de la mejor solución

Detalle	SolarWinds (Orion)	CA (NimSoft)
Evaluación técnica	38	39
Evaluación cualitativa	Medio	Alto

Como una acotación adicional de esta tesis, la Gerencia General, decidió que la herramienta del nuevo sistema de monitoreo será CA NimSoft Monitor debido a que la integración del componente de *Service*

Desk desplegado actualmente en la empresa GMD y la alianza entre GMD y CA para poder tener una herramienta de clase mundial. Además los proyectos denominados ISLAS, que actualmente cuenta GMD con entidades de gobierno, influenciaron para que la herramienta del sistema de monitoreo cumpla los requerimientos técnicos mínimos solicitados en sus contratos. Finalmente se está considerando en una siguiente fase, contar con una herramienta que permita realizar el monitoreo de servicios de TI a través de la compra de licenciamiento adicional y configuración por parte de GMD.

Una vez elegida la mejor herramienta para el nuevo sistema de monitoreo, se procederá con la implementación del sistema, el cual incluye el diseño, la implementación y documentación de la arquitectura final del sistema, el cual se explica en el siguiente capítulo.

7 CAPÍTULO VII: IMPLEMENTACIÓN DEL SISTEMA DE MONITOREO

7.1 DISEÑO TÉCNICO

7.1.1 ARQUITECTURA LÓGICA

En la figura N°10, se muestra el diagrama de la arquitectura lógica de CA NimSoft Monitor:

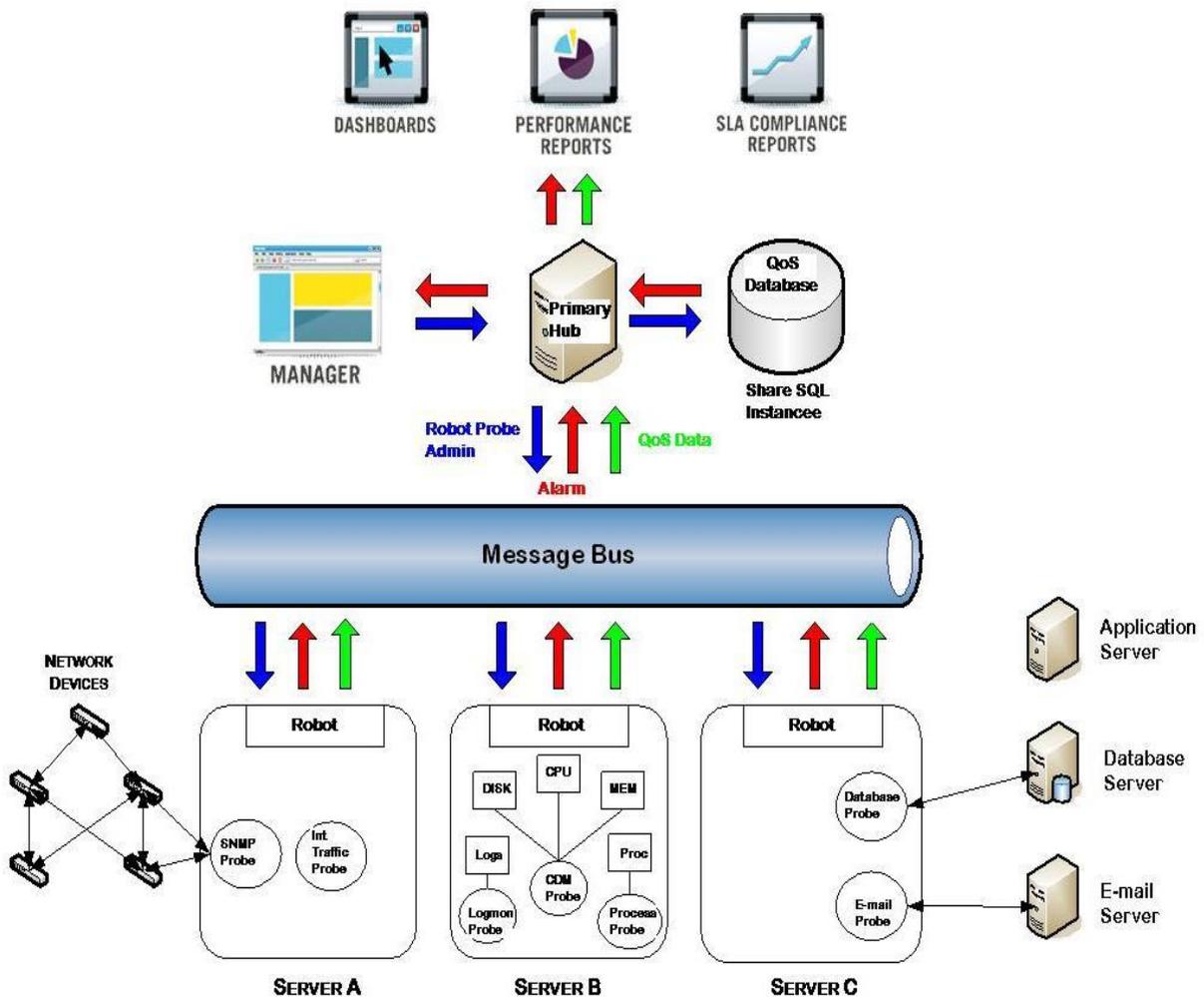


Figura N° 10: Arquitectura Lógica de CA NimSoft Monitor

Fuente: Sistema de conocimiento propio de GMD

Cada Robot tendrá por lo menos dos *Probes* instalados (*CDM*, *Processes*, etc.). Estos *probes* son los encargados de monitorear y recolectar métricas ya sea de manera local o remota. Estas métricas, una vez recolectadas, reciben el nombre de “QoS Data” y son transmitidas por el

spooler del robot a su *hub* correspondiente a través del *Message Bus*. El *hub* a su vez, retransmitirá estos “*QoS Data*” al *hub* primario (siempre y cuando este sea un *hub* secundario o un *tunnel hub*). Una vez que el “*QoS Data*” se encuentre en el *hub* primario, este será el encargado de transformar estos datos e insertarlos en la base de datos (*NIS*) para luego poder ser explotados a través de reportes o *Dashboards* en el UMP (*Unified Management Portal*). Se puede ver el flujo de este proceso, a través de la flecha verde de la figura N° 10.

Se experimenta un flujo similar cuando el *probe* detecta que alguna métrica monitoreada ha sobrepasado el umbral definido y en ese caso se genera una alarma: la alarma llega al *hub* a través del *spooler* del robot y una vez en el *hub* primario, esta alarma es procesada por el NAS (*NimSoft Alarm Server*) quien será el encargado de tomar las acciones o notificaciones definidas para esta alarma (envío de trap, envío de correo, ejecución de alguna acción, etc.). Esta alarma será almacenada, al igual que el “*QoS Data*” en la base de datos (*NIS*) para luego poder ser vista y explotada a través del *Infrastructure Manager* o de reportes en el Portal. Se puede ver el flujo de este proceso, a través de la flecha roja de la figura N° 10.

7.1.2 ARQUITECTURA FÍSICA

Esta sección configura la arquitectura de la solución, el diagrama de la figura N° 11 muestra los componentes requeridos para implementar CA NimSoft Monitor en GMD.

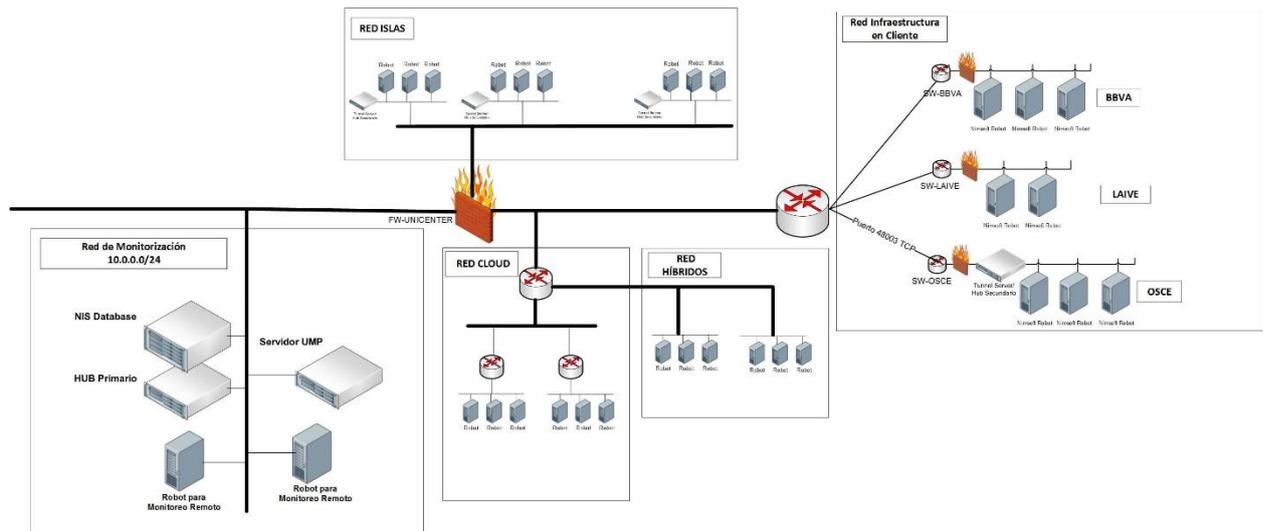


Figura N° 11: Arquitectura Propuesta NimSoft

Fuente: Sistema de conocimiento propio de GMD

7.1.3 DETALLE DE LA ARQUITECTURA PROPUESTA

La arquitectura propuesta consta de tres servidores principales para la solución:

- **1 Servidor principal de CA NimSoft Monitor**, llamado *Hub* Primario.- este servidor está diseñado para recolectar las métricas (*QoS Data*) y alarmas provenientes de los robots que se conectan directamente a este *hub* y también recolecta métricas y alarmas desde todos los *hubs* secundarios (que para esta implementación, todos serán tipo *tunnel hub*).

De acuerdo a las características de hardware, planteadas para este servidor, puede llegar a soportar la carga (recibir las métricas y alarmas) entre ochocientos a mil servidores (no se puede determinar un valor exacto, puesto que va a depender de la cantidad de *probes* a implementar por robot y la cantidad de métricas que se recolecte para estos *probes*).

Desde este servidor se deberá contar con salida a la dirección web support.nimsoft.com a fin de poder descargar los *probes* y sus respectivas actualizaciones cuando estén disponibles.

- **1 servidor de base de datos.-** donde estará alojada la base de datos de NimSoft (*NimSoft Information Store*). Esta base de datos estará sobre un servidor Microsoft SQL.
- **1 servidor UPM.-** que alojará *Unified Management Portal*, para la creación y ejecución de *dashboard*, y también, alojará el *Unified Reporter* para la creación y ejecución de reportes.

Adicionalmente, se está considerando **2 Servidores** que cumplirán la función de **Robots dedicados** para alojar los *probes* de monitoreo remoto (VMWare, netapp, url_response, snmpcollector, interface_traffic y net_connect).

Se define 2 servidores dedicados para monitoreo remoto por las siguientes razones:

- No es posible ubicar los *probes* remotos en el servidor *Hub* Primario, ya que este está diseñado para solamente recolectar métricas y alarmas de los robots (a través de los *hubs* secundarios) es decir soportará alto volumen de monitoreo (aprox. 600 robots) y no se quiere sobrecargar este *Hub* Primario.
- Sólo para el caso de monitoreo ESX, a través del *probe* VMWare, GMD cuenta con aprox. 180 servidores ESX, ésta es la principal razón para plantear 2 servidores robots dedicados para alojar estos *probes* de monitoreo remoto ya que se balanceará la carga entre ambos servidores.

Estos 5 servidores (3 Servidores Principales y 2 servidores destinados a ser Robots dedicados), estarán alojados en la red de monitorización. Para mayor detalle sobre las consideraciones y características de *hardware* y *software* necesario para la implementación de esta arquitectura, referirse al apéndice 03.

Para recolectar la información de monitoreo de los servidores ubicados detrás del *Firewall*, CA recomienda utilizar *Hubs* secundarios (de tipo *tunnel hub*) a fin de que no sea necesario habilitar múltiples puertos desde cada uno de los robots hacia el *hub* principal. Con el *tunnel*

hub, sólo será necesario habilitar un único puerto desde el *tunnel hub* (que recolectará las métricas y alarmas de sus respectivos robots) hacia el *hub* primario. Este puerto es el 48003 TCP. Sin embargo, para GMD, se ha definido habilitar ciertos puertos dependiendo de la red que se conecte. Esta información se encuentra en el apéndice 04.

7.1.4 PROBES A IMPLEMENTAR

Se implementarán los siguientes *probes*:

- **Para el monitoreo de Sistemas Operativos de Servidores:**

Es requerimiento de GMD de monitorear 621 servidores de sus diferentes clientes. Estos servidores se encuentran en distintas plataformas: Windows NT Server, Windows 2000 Server, Windows XP, Windows 7, Windows 2003, Windows 2003 R2, Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, Linux Red Hat 5, Linux Red Hat 6, Suse Linux 11, centos 5, centos 6, Ubuntu 12, AIX 7, AIX 7.1, HP-UX 11.1, HP-UX11.2, HP-UX 11.3.

Para cada uno de estos servidores se debe instalar un robot y los *probes* correspondientes para monitoreo de parámetros de sistema operativo (**CMD Probe**, **interface_traffic** y **processes Probe**), tal y como se muestra en la figura N° 12.

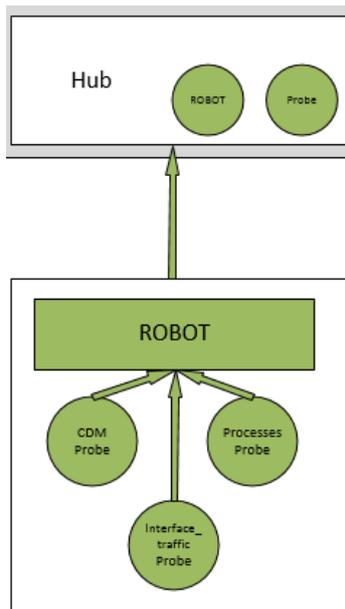


Figura N° 12: Monitoreo Local de Sistemas Operativos a través de CDM, interface_traffic y processes Probes

Fuente: Sistema de conocimiento propio de GMD

Nota: Para los sistemas operativos que no tienen soporte para instalar Robot (Windows NT Server, Windows Server, Windows XP, HP-UX 11.1) se monitoreará el CPU, Disco, Memoria y Procesos, de manera remota a través del **Snmcollector Probe**.

Este *probe* (snmpcollector) se instalará en el Robot Dedicado para monitoreo remoto 1 y Robot para monitoreo remoto 2, de acuerdo a la figura N° 13.

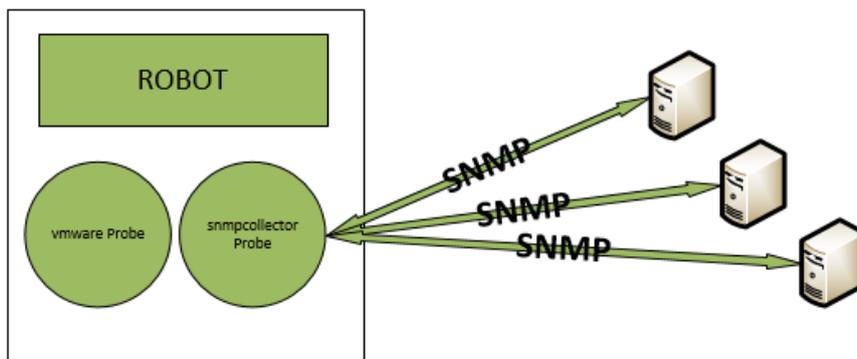


Figura N° 13: Monitoreo Remoto de Sistemas Operativos a través de snmpcollector Probe

Fuente: Sistema de conocimiento propio de GMD

De la misma manera, el *interface_traffic Probe* no tiene soporte para instalación en las plataformas Ubuntu, AIX y HP-UX (no soporta monitoreo local) por lo que se empleará el monitoreo remoto para estas plataformas no soportadas como monitoreo local.

En la figura N° 14 se muestra cómo Este *probe* (*interface_traffic*) se instalará en el Robot Dedicado para monitoreo remoto 1 y Robot para monitoreo remoto 2.

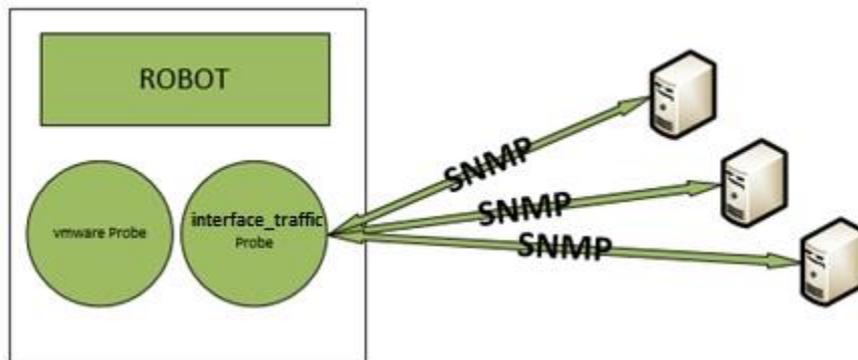


Figura N° 14: Monitoreo Remoto de Interfaz de red a través de *interface_collector Probe*

Fuente: Sistema de conocimiento propio de GMD

- **Para el monitoreo de Bases de datos de Servidores:**

GMD cuenta con 60 servidores Oracle con versiones que van desde Oracle 9i a Oracle 11g R2.

El *Probe* a instalar para monitorear estos Oracle se llama **Oracle Probe**.

GMD cuenta con 500 bases de datos MS SQL con versiones que van desde SQL Server 2000 a SQL Server 2012. El *Probe* a instalar para monitorear el SQL Server se llama **Sqlserver Probe**.

Si bien es posible instalar estos *probes* (Sqlserver y Oracle) en monitoreo remoto, es decir, contar con un robot dedicado para recolectar las métricas de los servidores SQL y Oracle, se ha decidido instalarlos en el mismo servidor donde residen las bases de datos (monitoreo local) debido a la gran cantidad de Bases de datos que se necesitan monitorear, se requiere varios

servidores adicionales (robots dedicados) para soportar el monitoreo remoto, de acuerdo como se muestra en la figura N°15.

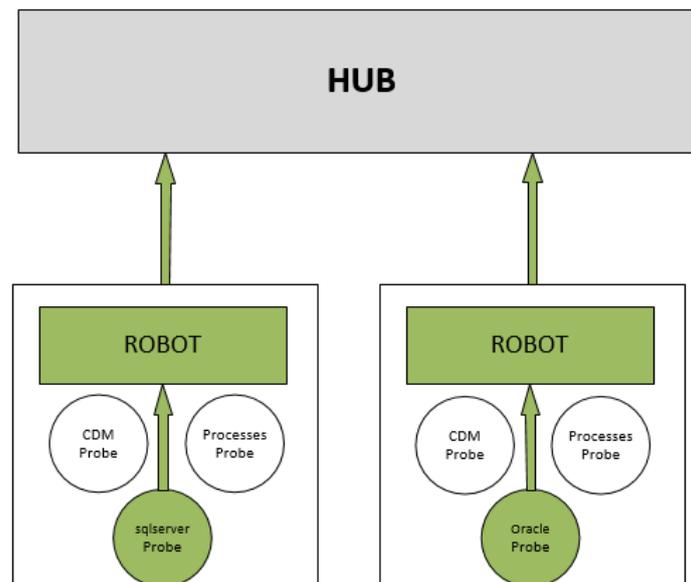


Figura N° 15: Monitoreo Local de bases de datos a través de Sqlserver y Oracle *Probes*

Fuente: Sistema de conocimiento propio de GMD

- **Para el monitoreo de directorio activo:**

GMD cuenta con 85 servidores que cumplen la función de Directorio Activo para sus diferentes clientes. Las versiones de los directorios activos van desde Active directory 2003 a Active Directory 2012. El *probe* a instalar en cada uno de estos servidores se llama **Ad_server Probe**, tal y como se muestra en la figura N° 16.

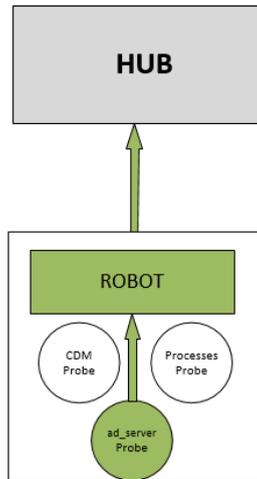


Figura N° 16: Monitoreo Local de Directorio Activo a través de ad_server Probe

Fuente: Sistema de conocimiento propio de GMD

- **Para el monitoreo de Microsoft Exchange:**

GMD cuenta con 20 servidores Microsoft Exchange que son servidores de correo para sus diferentes clientes. Estos servidores van desde la Microsoft Exchange versión 2003 a la versión Microsoft Exchange 2013. El *probe* a instalar en cada uno de estos servidores se llama **Exchange_monitor Probe**. Se puede visualizar la interacción explicada en la figura N° 17.

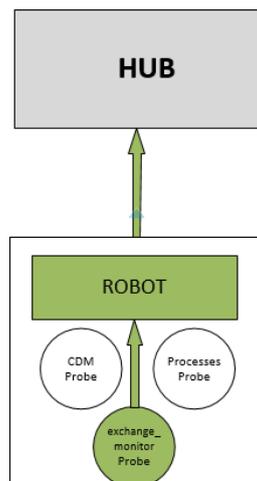


Figura N° 17: Monitoreo Local de Exchange Server a través de Exchange_monitor Probe

Fuente: Sistema de conocimiento propio de GMD

- **Para el monitoreo del Storage Netapp:**

GMD cuenta con 5 Storage Netapp versiones 8.1.2 P1 y 8.1.2 P4. El *probe* a instalar para el monitoreo de netapp se llama **Netapp Probe**.

Este *Probe* (netapp) se alojará en el Robot Dedicado para monitoreo remoto 1, como se muestra en la figura N° 18.

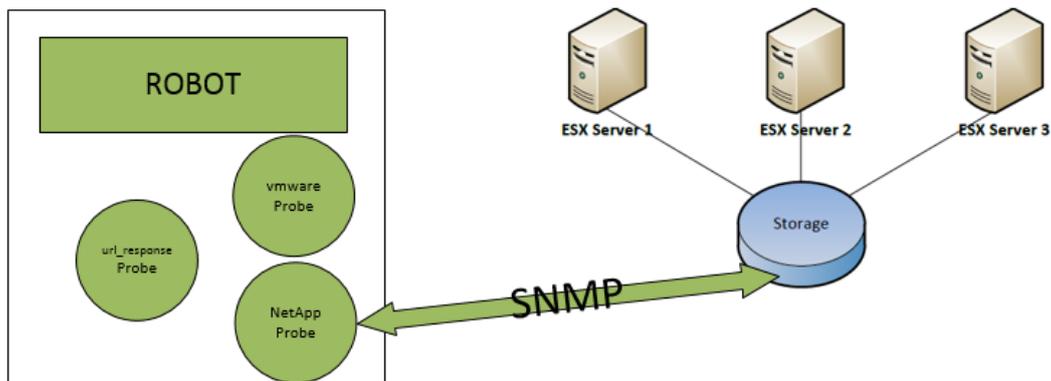


Figura N° 18: Monitoreo Remoto de Storage a través de NetApp Probe

Fuente: Sistema de conocimiento propio de GMD

- **Para el monitoreo de VMWARE:**

GMD cuenta con aprox. 180 ESX que van desde versiones 4.1 a la 5.5. El *probe* a instalar para el monitoreo de los VMWare se llama **VMWare Probe**.

Debido a la cantidad de servidores en la infraestructura de VMWare se está dimensionando instalar el *probe* en hasta 2 Robots. Por lo que este *Probe* (VMWare) se alojará en el Robot Dedicado para monitoreo remoto 1 y Robot Dedicado para monitoreo remoto 2. La figura N° 19 muestra un ejemplo de esta configuración.

Nota: Debido a que la versión actual del *probe* (6.10) sólo soporta versiones de ESX que van desde la 5.1 a la 5.5, se ha decidido utilizar una versión anterior del *probe* (6.01) que cuenta

con soporte para versiones ESX que van desde la 4.1 a la versión 5.5. (Esta versión del *probe* 6.01 fue liberada en Diciembre de 2013).

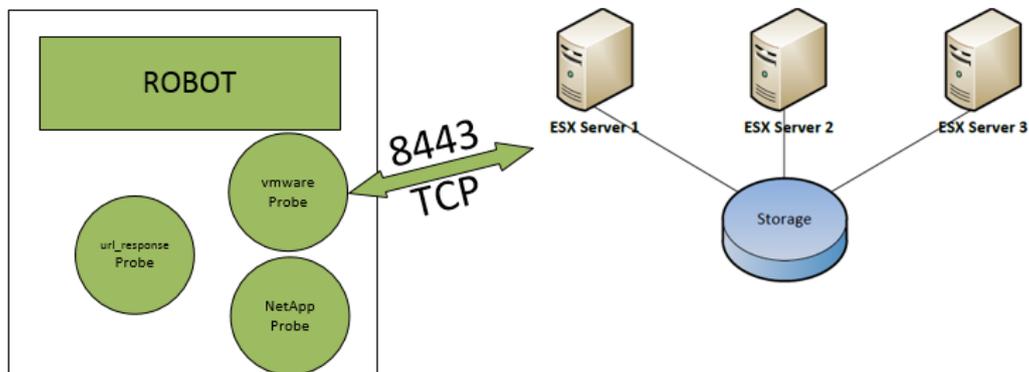


Figura N° 19: Monitoreo Remoto de Servidores ESX a través de VMWare *Probe*

Fuente: Sistema de conocimiento propio de GMD

- **Para el monitoreo de URLs:**

Es requerimiento de GMD monitorear la disponibilidad de URLs. El *Probe* a instalar se llama ***url_response Probe***.

Este *Probe* (*url_response*) se alojará en el Robot para monitoreo remoto 2.

Para poder monitorear URLs públicas es necesario otorgar los respectivos accesos de internet sobre este robot. La figura N° 20 esquematiza esta configuración.

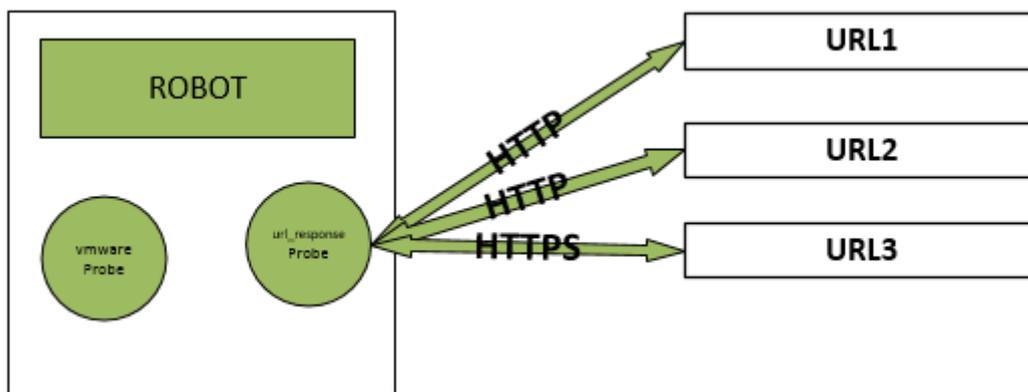


Figura N° 20: Monitoreo Remoto de URLs a través de *url_response Probe*

Fuente: Sistema de conocimiento propio de GMD

Para mayor información sobre los requerimientos sobre los *probes* a implementar y las métricas definidas para GMD con respecto a cada *probe* revisar los apéndices 05 y 06 de este documento.

7.2 IMPLANTACIÓN DE SISTEMA DE MONITOREO DE SERVIDORES Y APLICACIONES

En esta sección se describe la arquitectura de la solución a nivel de configuración. Este es el método propuesto para monitorear los servidores y aplicaciones que son requerimiento de GMD.

7.2.1 ENFOQUE GENERAL

NimSoft se debe instalar en un entorno pre-producción de tal manera que conviva con el monitoreo que se tiene actualmente con Spectrum.

Una vez terminado de implementar NimSoft Monitor (todos sus componentes, robots y *probes*), se dejará de monitorear a través de *Spectrum / eHealth* y se empezará a monitorear solamente a través de NimSoft que en ese momento entrará en un ambiente de producción.

Para implementar los Robots se hará a través del ADE lo cual permitirá un despliegue remoto y masivo de Robots (tanto a servidores Windows, Linux y Unix). Cada Robot tiene un tamaño de aprox. 20 MB por lo que se hará un despliegue controlado a fin de no afectar el tráfico de red (por ejemplo, enviar instalación de no más de 5 robots a la vez).

Una vez implementado los robots, se podrá desplegar los *Probes* de monitoreo.

Para el despliegue de *Probes* se sugiere empezar con el *Probe* de una aplicación o sistema, por ejemplo Exchange_monitor. Se debe prestar atención en configurar los umbrales de manera correcta, con los niveles de alarma correspondientes.

Donde sea posible todos los umbrales de las alarmas que están basadas en valores numéricos deben tener mensajes QoS (métricas) recolectadas de tal modo que los datos históricos puedan ser consultados en el caso de una alarma. NimSoft Monitor mantendrá las métricas recolectas en la base de datos (NIS) hasta un año de antigüedad.

Lo que sigue es la secuencia de eventos típica:

- a) Identificar la aplicación (por ejemplo Microsoft Exchange)
- b) Instalar los robots
- c) Construir plantillas de monitoreo (apoyarse en los owners de las aplicaciones para definir las métricas y los umbrales)
- d) Desplegar las plantillas de monitoreo
- e) Pruebas (que consiste en verificar que se están recolectando las métricas en los intervalos de tiempo configurados)
- f) Desarrollar Dashboard y reportes

7.2.2 MANEJO DE ALARMAS

Todas las alarmas generadas por los *Probes* en CA NimSoft Monitor serán enviadas a CA Spectrum para su manejo desde allí a través de la integración de la mesa de ayuda (CA Service Desk) con CA Spectrum.

Las alarmas a enviar a Spectrum incluirán, además de los campos que trae la herramienta por defecto (*Hostname, Source, Message, Time Received, Time Origin, Robot* y *Probe* además deberán de incluir los siguientes campos adicionales: **Cliente, Responsable y Ubicación**).

Se implementarán dos *probes* para este propósito:

- **Alarm_enrichment probe.-** a fin de poder incluir estos 3 campos requeridos para GMD.

Este *Probe* es configurado para leer datos desde diferentes fuentes. Esta fuente es referida como CMDB (no confundir con la solución CA CMDB). Actualmente, sólo es soportada como fuente la Base de Datos SQL.

El *alarm_enrichment* es un *probe* que pre-procesa (enriquece con datos adicionales) las alarmas antes de ser enviadas al *probe* NAS (NimSoft Alarm Server).

En la figura N° 21 que se muestra a continuación se visualiza el flujo de alarmas a través del *probe* *alarm_enrichment*.

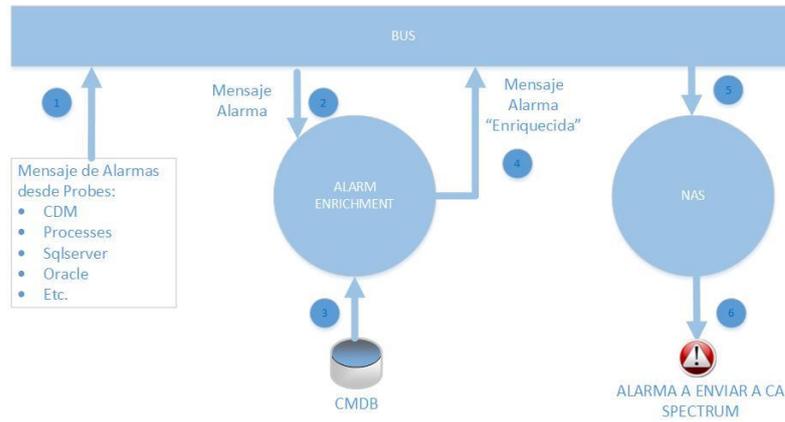


Figura N° 21: Flujo de Alarmas a través de alarm_enrichment

Fuente: Sistema de conocimiento propio de GMD

- **Snmptgw probe.-** SNMP Gateway *probe* a fin de poder enviar las alarmas al Servidor de Spectrum a través de Traps SNMP (se requiere habilitar los puertos SNMP entre el Hub Primario de NimSoft y el CA Spectrum. Para un mejor entendimiento, es necesario ver la figura N° 22 sobre el flujo de alarmas generadas desde CA Nimsoft.



Figura N° 22: Flujo de Alarmas generadas desde CA NimSoft

Fuente: Sistema de conocimiento propio de GMD

7.2.3 USER LOGINS

Hay dos tipos de *login* en NimSoft Monitor, *User Logins* y *Account Contacts*.

Account Contacts son usados por Organizaciones de tipo MSP, como es el caso de GMD, para separar lógicamente a los usuarios dentro de su propio grupo de servidores sin visibilidad fuera de este grupo. Estos usuarios sólo tienen acceso a través de *UMP* y no pueden iniciar sesión al *Infrastructure Manager*. La cuenta es enlazada a uno o muchos orígenes particulares y solamente se tiene acceso a los datos / alarmas a los cuales tienen derecho. Esto puede ser usado por GMD para proporcionar acceso de sólo lectura a reportes y *dashboard* en *UMP*.

User logins son controlados por las Listas de Control de Acceso (ACL's). Los ACL's pueden ser enlazados a grupos LDAP si se requiere.

Para este proyecto, se ha definido lo siguiente:

- Integración de los ACL's con el directorio activo de GMD a fin de tener inicio de sesión unificado.
- Existen 5 diferentes tipos de ACL's por defecto que son:
 - Superusuario: se creará 1 perfil basado en este ACL
 - Administrador: se crearán 2 perfiles basados en este ACL
 - Operador: se creará 1 perfil basado en este ACL
 - *Dashboard Designer*: no se ha definido perfil para este ACL
 - *Guest*: no se ha definido perfil para este ACL.
- Se requiere 1 *Account Contact* para 1 de los clientes de GMD

7.2.4 REPORTES Y PERCENTIL 95

A través del *Unified Management Portal*, es posible obtener y acceder a un *dashboard* de gestión para todos los elementos monitoreados. CA NimSoft Monitor ya proporciona una serie de *dashboard*, *Out of the Box*, para los diferentes elementos a monitorear en este Proyecto

(Servidores, MS SQL Server, VMWare, Active Directory, Microsoft Exchange, etc.). La figura N° 23 mostrada a continuación, es un ejemplo de la lista de *dashboards* por defecto del Portal.



Figura N° 23: Lista de Dashboards que trae el Portal por defecto

Fuente: Sistema de conocimiento de GMD

Adicionalmente, CA NimSoft Monitor, ofrece una herramienta de reportes llamada Unified Reporter integrada al Portal (UMP). Esta herramienta de reportes, además de traer algunas plantillas de reportes, a manera de ejemplo, permite crear reportes personalizados, en muy pocos minutos, de una manera muy sencilla y con una interfaz fácil de usar: basta con seleccionar las métricas que se desean aparezcan en el reporte y queda listo para su ejecución.

De acuerdo al alcance de este proyecto, los Reportes y Dashboards, serán los que proporciona la herramienta de manera Out of the Box, es decir no se crearan nuevos dashboard o reportes.

Está dentro del alcance de esta implementación el que GMD pueda ejecutar reportes de Percentil 95 para todos los reportes que requiera ejecutar. En tal sentido, deberá existir una opción en cada uno de los reportes a ejecutar, que permita habilitar esta opción de Percentil 95. Las figuras N° 24, 25 son ejemplos de reportes que se pueden obtener con la herramienta y las

figuras N° 26, 27, 28, 29 y 30 son ejemplos de visualización los dashboards de las distintas soluciones implementadas.

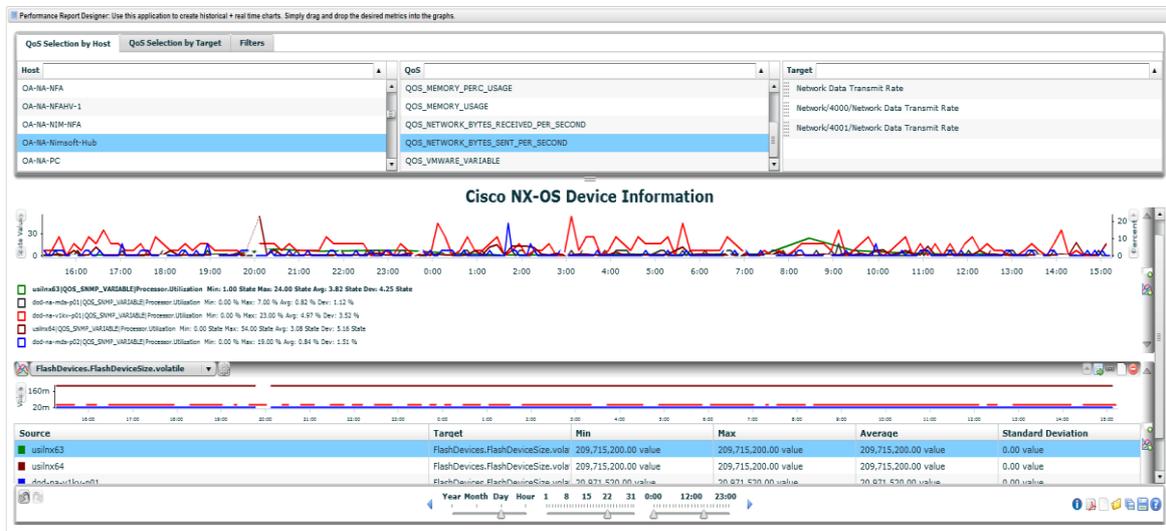


Figura N° 24: Diseñador de Reportes de CA NimSoft

Fuente: Sistema de conocimiento propio de GMD

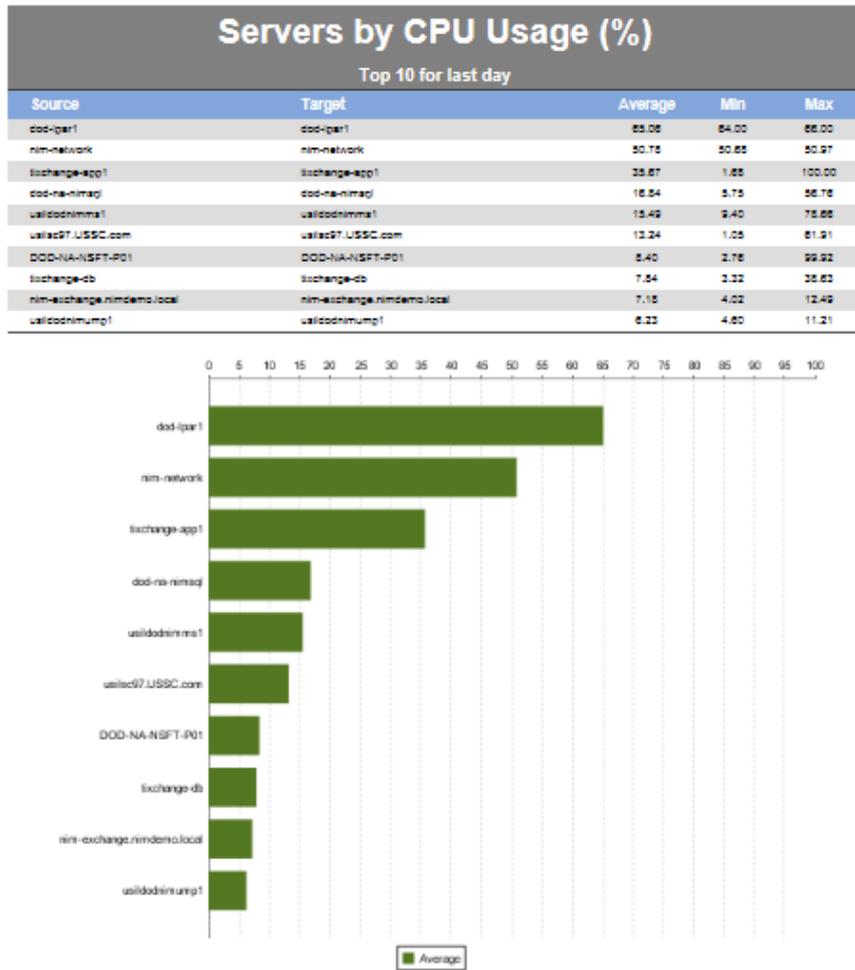


Figura N° 25: Reporte obtenido por CA NimSoft

Fuente: Sistema de conocimiento propio de GMD

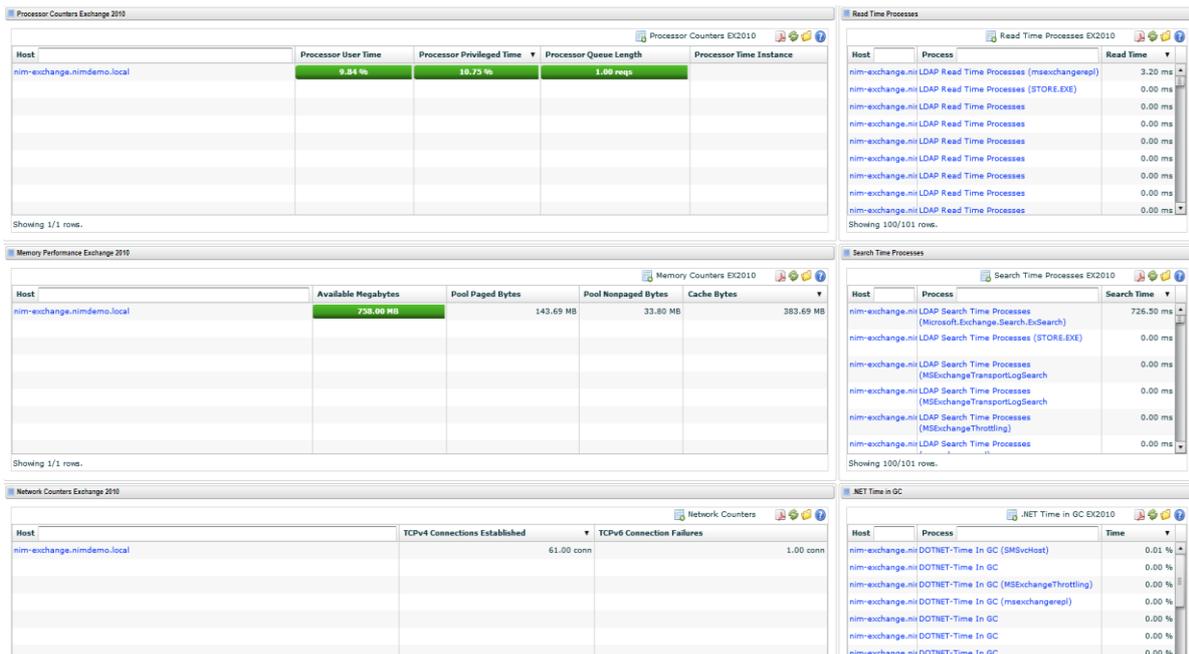


Figura N° 26: Dashboard Out of the Box de Monitoreo Exchange

Fuente: Sistema de conocimiento propio de GMD

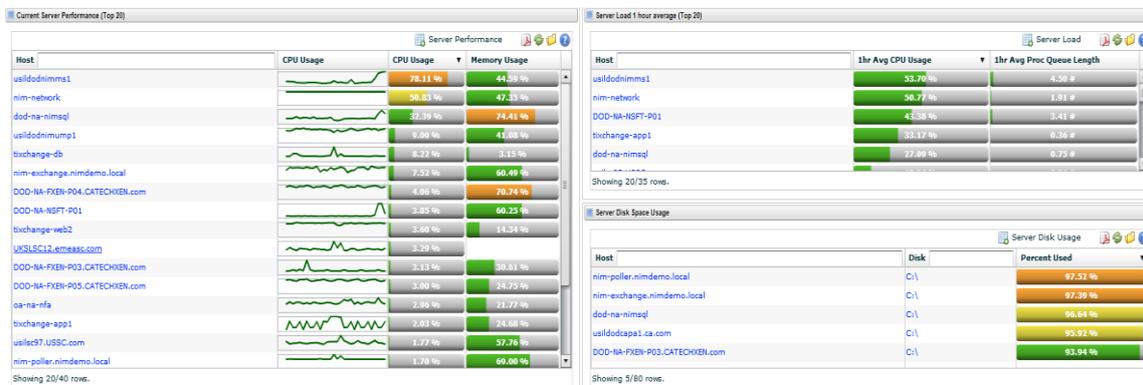


Figura N° 27: Dashboard Out of the Box de Monitoreo de Servidores

Fuente: Sistema de conocimiento propio de GMD

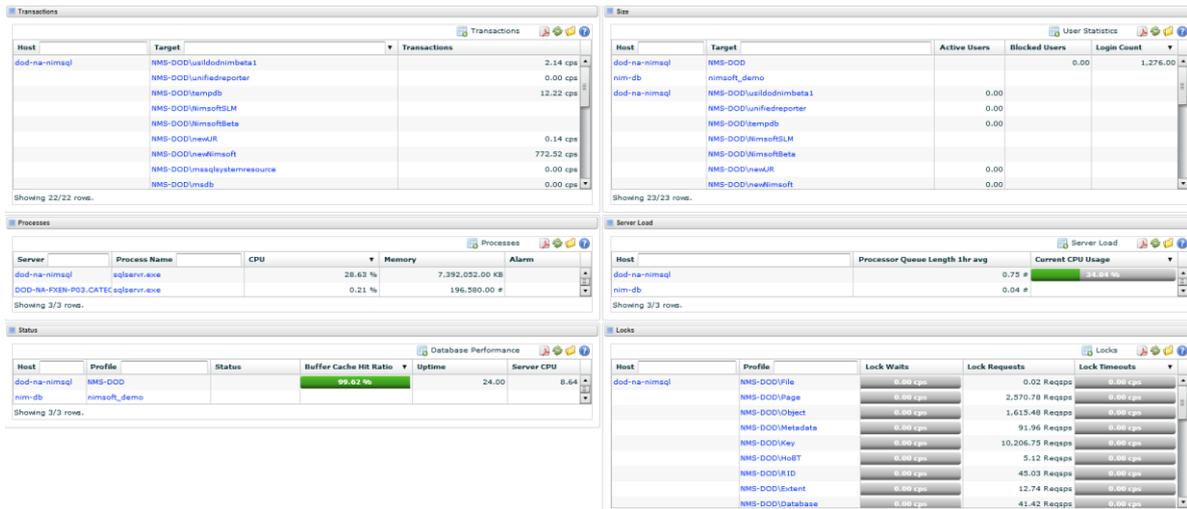


Figura N° 28: Dashboard Out of the Box de Monitoreo de SQL Server

Fuente: Sistema de conocimiento propio de GMD

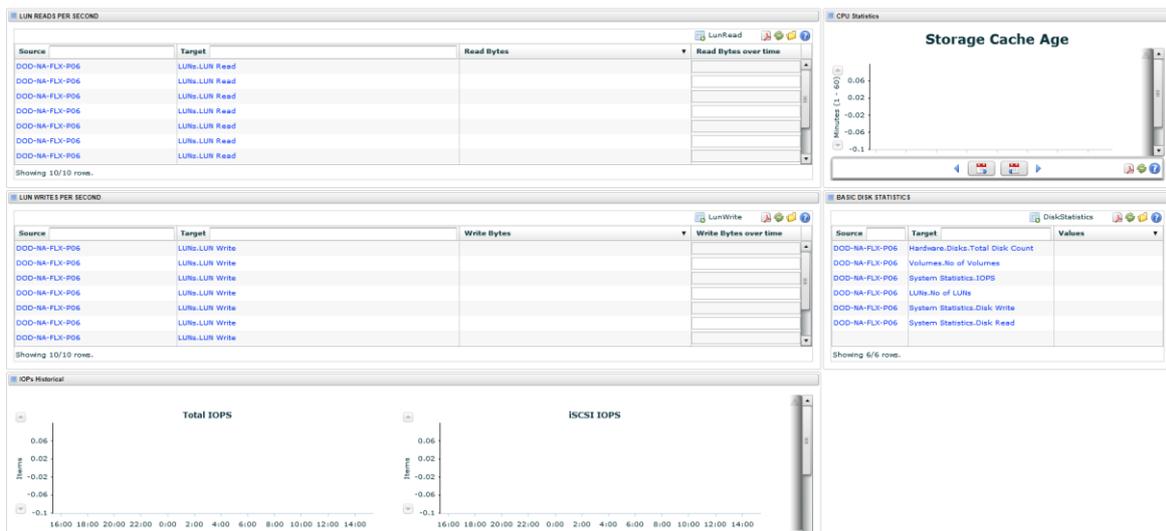


Figura N° 29: Dashboard Out of the Box de Monitoreo de NetApp

Fuente: Sistema de conocimiento propio de GMD

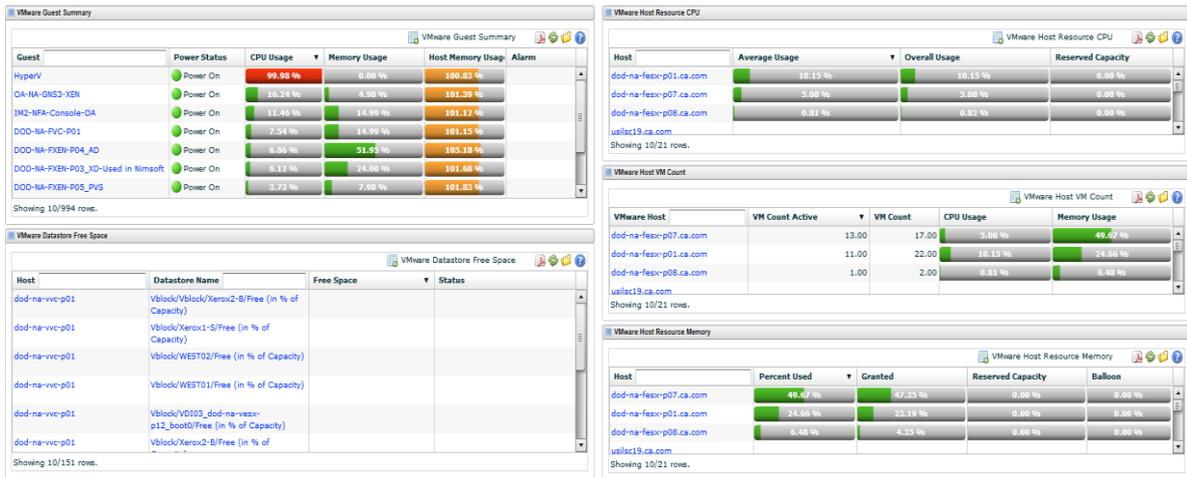


Figura N° 30: Dashboard Out of the Box de Monitoreo de VMware

Fuente: Sistema de conocimiento propio de GMD

En el siguiente capítulo, mostraremos los resultados de la evaluación financiera del proyecto de la tesis, y cómo se cuantifica este retorno de la inversión para el proyecto de mejora.

8 CAPÍTULO VIII: EVALUACIÓN FINANCIERA DEL PROYECTO

8.1 DATOS GENERALES DEL PROYECTO

La evaluación financiera del proyecto se ha calculado en base a 60 meses. Este proyecto consiste en la subcontratación de los servicios especializados de CA Consulting Services y la adquisición de licenciamiento. En la tabla N° 11 se muestra el resumen de la cantidad de equipos y licencias requeridas:

Tabla N° 11: Tabla resumen de cantidad equipos y licencias requeridas

Detalle de la solución	Cantidad
CA - IM (Spectrum)	174
NimSoft Monitor Server Pack On-Prem	621
NimSoft Monitor Server and Application Pack On-Prem	50

El detalle de la relación de equipos por cliente se encuentra en el apéndice 07.

El área de servicios datacenter no generaba ingresos como venta de servicios antes de la implementación de este proyecto, dado que su principal objetivo era el de trasladar los costos de sus servicio de soporte a los distintos proyectos provistos por GMD. Luego de la implementación de este proyecto, se ha establecido un margen mínimo, de 15% como generación de rentabilidad. Además, se han adquirido 50 licencias de tipo *NimSoft Monitor Server and Application Pack On-Prem*, dado que en un alcance inicial será aplicado a la siguiente cantidad de aplicaciones: 5 *storage* NetApp, 10 servidores Microsoft Exchange, 10 servidores directorio activo, 20 base de datos Oracle y 5 base de datos SQL, los cuáles ya han sido comprometidos con 3 proyectos como adendas a sus contratos.

8.2 ESTRUCTURA DE COSTOS DEL PROYECTO

Los costos del proyecto se encuentran divididos en 5 conceptos, como se puede visualizar en la tabla N° 12, los cuáles se describen a continuación:

1. Costo de bienes y subcontratas: Se incluyen los costos de la consultoría para la implementación del sistema de monitoreo, así como el costo por el mantenimiento de las licencias por la duración de la evaluación que es de 5 años y un último recurrente mensual por el alquiler del servicio IaaS interno de GMD para la provisión de la plataforma de servidores.
2. El segundo concepto es la mano de obra asignada, la cual incluye el personal de GMD necesario para mantener la plataforma del nuevo sistema, que son los especialistas y administradores para el sistema de monitoreo.
3. El concepto de gastos generales hace mención a la asignación de los costos directos generados por los puestos de trabajo en GMD
4. La inversión del proyecto ha sido estimada en base al costo de suscripción por primer año del licenciamiento requerido
5. Finalmente, los gastos financieros, hace mención a los costos de las cuotas de financiamiento bancario con una tasa de 8% mensual y en 36 meses realizado por GMD para la implementación del proyecto y el flujo de caja.

A continuación se muestra un cuadro resumen de los montos totales, en dólares, por 60 meses derivados de la implementación y operación de este proyecto.

Tabla N° 12: Tabla de estructura de costos estimados del proyecto

Concepto	Totales (US\$)	%
Ingresos	1,373,533	100%
Egresos	1,153,768	84.0%
Costo Bienes y Subcontrata	738,091	64.0%

Concepto	Totales (US\$)	%
Mano de Obra	229,015	19.8%
Gastos Generales	6,419	0.6%
Gastos Generales (Nro. Partida)	0	--
Gastos Generales asignados	6,419	--
Depreciación	160,938	13.9%
Depreciación	160,938	--
Gastos Financieros	19,305	1.7%
Utilidad de Proyecto	219,765	15.0%

Como se puede apreciar en la tabla anterior, el mayor componente de la estructura de costos es el componente de costos de bienes y subcontrata, que es la subcontratación de los servicios de consultoría del proveedor.

Ratios Financieros:

Este proyecto dio como resultado un ROI en el mes 37, en dónde los flujos de caja acumulados superaron los montos de inversiones y financiamiento, iniciando con la rentabilidad del proyecto.

8.3 FLUJO DE CAJA DEL PROYECTO

En la tabla N° 13 que se muestra a continuación se encuentra el flujo de caja total del proyecto:

Tabla N° 13: Tabla de flujo de caja del proyecto

Concepto	Totales (US\$)	VPN (US\$)	%
Ingresos	1,373,533	1,136,482	100.0%
Egresos	1,149,170	965,652	85.0%
Costo Bienes y Subcontrata	738,091	612,250	63.4%
Mano de Obra	229,015	190,710	19.7%
Gastos Generales	6,419	5,345	0.6%
Gastos Generales Directos	0	0	--
Gastos Generales			
Asignados	6,419	5,345	--
Inversión (Equipos y Software)	156,341	139,433	14.4%
Gastos Financieros	19,305	17,914	1.9%
Flujo de Proyecto	224,362	170,830	15.0%

Para mayor detalle sobre el flujo del proyecto mes a mes, referirse al apéndice 08.

En base a este flujo de proyecto, se ha proyectado que por lo menos se deberá de considerar un ingreso mensual de US\$ 22,892.21 entre los distintos proyectos que actualmente utilicen el nuevo sistema de monitoreo integrado. En un primer intento, en la tabla N° 14 se muestra el resumen de la estimación de distribución de los precios del proyecto basados en la cantidad de equipos a monitorear y por concepto:

Tabla N° 14: Tabla resumen de distribución de costos del proyecto

Detalle de la solución	Cantidad	Precio Unitario	Precio Total
Monitoreo Redes	174	\$ 21.71	\$ 3,777.22
Monitoreo Servidores	621	\$ 28.20	\$ 17,512.54
Monitoreo Aplicaciones	50	\$ 32.05	\$ 1,602.45
Totales			\$ 22,892.21

Esta distribución realizada se ha estimado en base a juicio de experto y de acuerdo a lo que dicta el mercado y obteniendo una rentabilidad mínima del área de servicios datacenter de 15%. La empresa aumentará sus ingresos dado que se ha ofrecido el nuevo servicio de monitoreo de aplicaciones a 3 proyectos actuales, los cuáles pagaran como adenda a sus contratos de servicios.

Este proyecto tiene un retorno de la inversión en el mes 37, en donde el flujo de caja acumulado ya se hace positivo.

9 CONCLUSIONES

- El nuevo sistema de monitoreo ya se encuentra implementado en la plataforma tecnológica de GMD. Este nuevo sistema cuenta con la infraestructura necesaria para que pueda realizar un monitoreo de 4ª generación la cual le permitirá ofrecer nuevos servicios a clientes ya existentes y/o nuevos, incrementando así sus ingresos.
- Durante la evaluación técnica-cualitativa, se realizaron decisiones de juicio de experto para la calificación y puntuación de los criterios de evaluación y se obtuvo la implementación del nuevo sistema de monitoreo que cuenta con una única interfaz de visualización, esto permite la rápida identificación del componente afectado, a nivel de servidores y aplicaciones, durante una incidencia por parte de los Operadores de Sistemas de esta manera les permite realizar el escalamiento adecuado hacia el área correspondiente para su revisión. Se logró reducir un 5% de los tiempos por evento para la detección de componente fallido.
- La implementación del nuevo sistema de monitoreo permitió incrementar la satisfacción de clientes debido a que los Gerentes de Proyectos cuentan con una trazabilidad rápida (a través de dashboard en tiempo real) para medir los acuerdos de nivel de servicio asociados a caídas de servicios durante la gestión de eventos. El aumento se dio como resultado de las encuestas de satisfacción semestrales que se realizan a los distintos proyectos como parte de la gestión de calidad de GMD.

10 RECOMENDACIONES

- Implementar la publicación del servicio de monitoreo de URL's desde internet para los servicios implementados en el COT de GMD. Para ello, es necesario implementar un equipo fuera de GMD que realice estas consultas desde una conexión a internet.
- Los Event ID que se cargarán de NimSoft Monitor a Spectrum serán los identificados durante la etapa de implementación. De requerir nuevos Event ID se cargarán a demanda en el ambiente de producción.
- Separar *One Click Server* y *Spectrum Server*, debido al consumo de RAM teniendo en consideración que el Spectrum es de 32 bits.
- Realizar la documentación del Firewall en una etapa adicional debido a que el monitoreo realizado en estos equipos es demasiado básico (Memoria y CPU) y estos serán monitoreados con SPECTRUM.
- Implementar la personalización de indicadores de desempeño de los procesos de negocio de los clientes actuales en una fase adicional.
- Actualizar el catálogo de servicios e impulsar el servicio de monitoreo en sus niveles de maduración (Marketing).
- Establecer como una política de implementación, que todo equipamiento de red se monitoree a través de Spectrum.
- Establecer como una política de implementación, que todo servidor y aplicación se monitoree a través de NimSoft Monitor.

11 BIBLIOGRAFÍA

- Martín Peña, M. L., Martínez, E. M., de Castro Martínez, V., & Díaz Garrido, E. (2014). La formación en sistemas de servicios: Nuevos retos a través de la Ciencia en Gestión e Ingeniería de Servicios. (Spanish). *Intangible Capital*, 10(2), 294-316
- Acerca de GMD, GMD, disponible en http://www.gmd.com.pe/portal/acerca_gmd.aspx, accedido el 21/01/2015.
- Software de Monitoreo: Que se debe buscar a la hora de implementar, ArandaSoft, disponible en <http://www.arandasoft.com/blog/?p=263>, accedido el 14/02/2015.
- Gestión de Eventos ITIL v3, OVERTI, disponible en <http://www.overti.es/procesos-itsm/gestion-eventos-til-v3.aspx>, accedido el 10/02/2015.
- Gestión de Eventos, OSIATIS, disponible en http://itilv3.osiatis.es/operacion_servicios_TI/gestion_eventos.php, accedido el 31/01/2015.
- Itil Service Operation 2011 Edition – Itil Lifecycle Suite
- Project Management Institute. Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®) — Quinta edición, 2013.

12 APÉNDICES

12.1 APÉNDICE 01: ÁRBOL DE PROBLEMAS



Figura N° 31: Árbol de problemas

Fuente: Propia

12.2 APÉNDICE 02: ÁRBOL DE OBJETIVOS

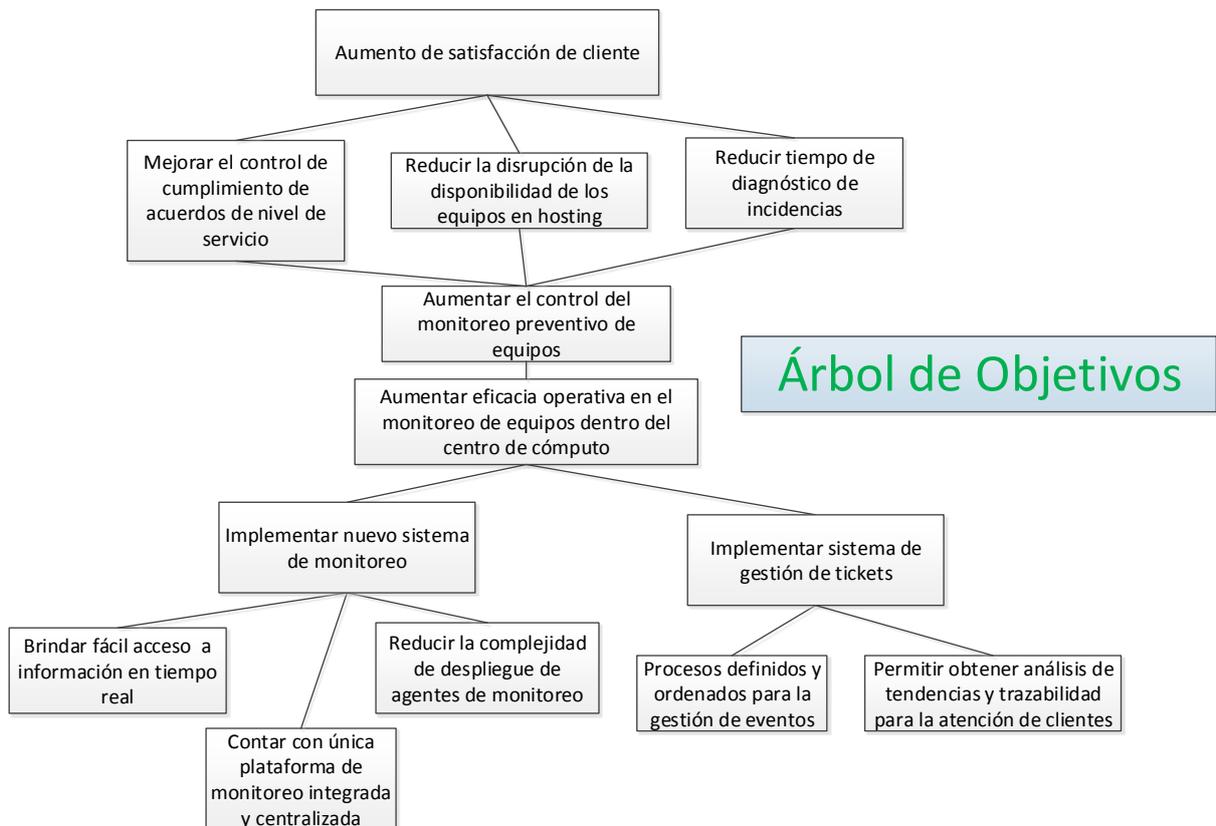


Figura N° 32: Árbol de objetivos

Fuente: Propia

12.3 APÉNDICE 03: CONSIDERACIONES PARA DETERMINAR EL HARDWARE Y SOFTWARE DE LA ARQUITECTURA

Determinación del tamaño de la implementación

El tamaño de la implementación está basado en el número de *hubs* y robots que se espera instalar.

Nos basamos en la siguiente tabla:

Tabla N° 15: Tabla para determinar el tamaño de implementación de CA Nimsoft

	Hubs	Robots
Pequeño	1	100
Mediano	5	250
Grande	20	500
Muy Grande	50	1000

De acuerdo a esta tabla nos encontramos en una implementación Grande.

Los requisitos de hardware para este tipo de implementación, de acuerdo a la Guía de Instalación de NimSoft Monitor, se muestran a continuación.

Hub Primario

Este el hub principal y todas las métricas “QoS Data” y alarmas serán ruteadas a este hub. Este servidor ejecutará todos los *probes* requeridos para su Sistema.

Hardware requerido: Cantidad 1

Función	Hardware			Software		Dependencias
	Procesador	RAM	Particiones	SO	BD	
Servidor Primario NimSoft (Hub-Server)	Dos procesadores de cuatro núcleos Clase XEON de 64 bits, 2 GHz o superior	12 GB	C: 50 Gb D: 100 Gb	Windows 2012 R2 (64 bit)		

Requerimientos de Software / Configuración:

- Java Runtime Environment 7 de 64 bits compatible (JRE)
- JRE está en la variable PATH del sistema.
- La compresión de disco NO está activada.
- Internet Explorer 10 o Firefox 28 o Chrome 33.
- Deshabilitar el anti-virus para instalación.

MS SQL Server (NIS Database)

Esta es la instancia del servidor SQL que alberga el motor de base de datos que almacena la base de datos NimSoft (NIS) la cual guarda las métricas de calidad de servicio “QoS Data”, una copia de las alarmas y la configuración del entorno.

La siguiente tabla es una estimación de los requisitos de almacenamiento de base de datos:

Database Storage basado en el tiempo de retención						
Servidores	mensajes QOS por min (estimado)	Data Engine tasa de inserción m/s	1 día (GB)	30 días (GB)	90 días (GB)	365 días (GB)
600	10	33.33	1.29	38.88	116.64	473.04

Hardware requerido: Cantidad 1

Función	Hardware			Software		Dependencias
	Procesador	RAM	Particiones	SO	BD	
Servidor NIS (base de datos)	Dos procesadores de cuatro núcleos Clase XEON de 64 bits, 2 GHz o superior	12 GB	C: 50 Gb D: 500 Gb	Windows 2012 R2 (64 bit)	MSSQL 2012	IE 10

Requerimientos de Software / Configuración:

- RAID DP de netapp (para aumentar la velocidad y la fiabilidad)
- Difundir los archivos de la base de datos en varios discos para mejorar la E/S
- La compresión de disco NO debe estar activada
- El administrador del dominio debe tener permiso para conectarse como un servicio

Unified Management Portal

Hardware requerido: Cantidad 1

Función	Hardware			Software		Dependencias
	Procesador	RAM	Particiones	SO	BD	
Servidor UMP Servidor UR	Dos procesadores de cuatro núcleos Clase XEON de 64 bits, 2 GHz o superior	12 GB	C: 50 Gb D: 150 Gb	Windows 2012 R2 (64 bit)		

Hubs Secundarios (Tunnel Hubs)

Este server ejecutará todos los *probes* requeridos para su Sistema.

Hardware requerido: Cantidad 11

Función	Hardware			Software		Dependencias
	Procesador	RAM	Particiones	SO	BD	
Hub Secundario NimSoft	1 procesador de cuatro núcleos Clase XEON de 64 bits, 2 GHz o superior	8 GB	C: 50 Gb D: 100 Gb	Windows 2008 R2 (64 bit)		

Se elige Windows 2008 para estos Hubs Secundarios (Tunnel Hubs), para dar la posibilidad que estos hubs alojen *probes* para monitoreo remoto que aún no soportan ser instalados en sistemas operativos Windows 2012.

Requerimientos de Software / Configuración:

- Java Runtime Environment 7 de 64 bits compatible (JRE)
- JRE está en la variable PATH del sistema.
- La compresión de disco NO está activada.
- Internet Explorer 10 o Firefox 28 o Chrome 33.
- Deshabilitar el anti-virus para instalación.

Robots Dedicados para monitoreo remoto

Hardware requerido: Cantidad 2

Función	Hardware			Software
	Procesador	RAM	Particiones	SO
Servidor Robot Dedicado para monitoreo remoto	1 procesador de dos núcleos Clase XEON de 64 bits, 2 GHz o superior	8 GB	C: 50 Gb D: 100 Gb	Windows 2008 R2 (64 bit)

Se ha elegido el Sistema operativo Windows 2008 R2 en lugar de Windows 2012 o Windows 2012 R2 porque hay *probes* (netapp y snmpcollector) que aún no son soportados en Sistema Operativo Windows 2012 o Windows 2012 R2.

12.4 APÉNDICE 04: TABLAS RESUMEN DE PUERTOS A HABILITAR PARA LAS REDES DE GMD

- **Para la red Infraestructura en Cliente.-** En esta red se encuentran los servidores de los 3 clientes de GMD haciendo un total aproximado de 61 servidores. se ha definido habilitar un *tunnel hub* en cada cliente. En resumen los puertos para habilitar para esta red, serían los siguientes:

Tabla N° 16: Tabla resumen de habilitación de puertos para la red Infraestructura en Cliente

Componente	Fuente	Puerto	Puerto Desc	Descripción de destino
Túneles	Túneles	48003	TCP/UDP	Sólo Red Externa Cliente. Este Puerto tiene que estar habilitado de manera bi-direccional entre el hub primario y el hub secundario (Tunnel Hub) en la red del cliente.

- **Para la red Cloud.-** En esta red se encuentran los servidores de los diferentes clientes de GMD (aprox. 30 clientes) haciendo un total aproximado de 150 servidores. Cada cliente cuenta con su propio segmento de red y se tendría que usar un *Tunnel Hub* por cada uno de estos clientes (lo que haría un total de 30 *hubs*, cada uno monitoreando un aprox. de 5 robots). Se ha decidido, entonces, no utilizar *hubs* para esta red cloud por lo que se tienen que habilitar los puertos en el *firewall* para cada uno de los 150 robots. En resumen los puertos para habilitar para esta red, serían los siguientes:

Tabla N° 17: Tabla resumen de habilitación de puertos para la red Cloud

Componente	Fuente	Puerto	Puerto Desc	Descripción de destino
Controller	Hub Primario	48000	TCP/UDP	Red Cloud. Habilitar en ambos sentidos a través del <i>firewall</i> de modo que el Infrastructure Manager de CA NimSoft Monitor puede contactar y Controlar Robots y <i>Probes</i> .
Spooler	Internal	48001	TCP/UDP	Red Cloud. Habilitar desde el Robot al -> Hub primario a través del firewall de manera que los <i>probes</i> pueden enviar mensajes al Hub a través del puerto Spooler. Los <i>probes</i> envían mensajes a los Hubs utilizando el puerto spooler (48001).
Hub	Hub Primario	48002	TCP/UDP	Red Cloud. Robots heartbeat. Este puerto (48002) tiene que estar habilitado desde el Robot al Hub Primario a través del Firewall de manera que los Hubs puedan realizar seguimiento de sus Robots.
<i>Probes</i>	<i>Probes</i>	48005- 48020	TCP	Red Cloud. Desde el Infrastructure Manager ubicado en el Hub Primario hacia los <i>probes</i> en todos

Componente	Fuente	Puerto	Puerto Desc	Descripción de destino
				los robots – esto es para configurar los <i>probes</i> .

- **Para la red híbridos.-** aquí sucede un caso similar al de la red cloud, con la diferencia que acá hay 300 robots. En este sentido, tampoco se estarían utilizando *Tunnels hub* para esta red, por lo que los puertos a habilitar serán:

Tabla N° 18: Tabla resumen de habilitación de puertos para la red híbridos

Componente	Fuente	Puerto	Puerto Desc	Descripción de destino
Controller	Hub Primario	48000	TCP/UDP	Red híbridos. Habilitar en ambos sentidos a través del firewall de modo que el Infrastructure Manager de CA NimSoft Monitor puede contactar y Controlar Robots y <i>Probes</i> .
Spooler	Internal	48001	TCP/UDP	Red híbridos. Habilitar desde el Robot al -> Hub primario a través del firewall de manera que los <i>probes</i> pueden enviar mensajes al Hub a través del puerto Spooler. Los <i>probes</i> envían mensajes a los Hubs utilizando el puerto spooler (48001).
Hub	Hub Primario	48002	TCP/UDP	Red híbridos.

Componente	Fuente	Puerto	Puerto Desc	Descripción de destino
				Robots heartbeat. Este puerto (48002) tiene que estar habilitado desde el Robot al Hub Primario a través del Firewall de manera que los Hubs puedan realizar seguimiento de sus Robots.
<i>Probes</i>	<i>Probes</i>	48005-48020	TCP	Red híbridos. Desde el Infrastructure Manager ubicado en el Hub Primario hacia los <i>probes</i> en todos los robots – esto es para configurar los <i>probes</i> .

- **Para la red Islas.**- En esta red, hay 10 Islas o segmentos de red, cada uno perteneciente a un cliente distinto y con un aprox. de 230 servidores a monitorear en total. En cada uno de los 10 segmentos de red, se define un *tunnel hub*.

En resumen los puertos para habilitar para esta red, serían los siguientes:

Tabla N° 19: Tabla resumen de habilitación de puertos para la red Islas

Componente	Fuente	Puerto	Puerto Desc	Descripción de destino
Túneles	Túneles	48003	TCP/UDP	Red Islas. Este Puerto tiene que estar habilitado de manera bi-direccional entre el hub primario y el hub secundario (Tunnel Hub).

12.5 APÉNDICE 05: REQUERIMIENTOS PARA LOS *PROBES* A IMPLEMENTAR

A continuación se listan los requerimientos para cada uno de los *Probes* a implementar en los servidores a monitorear para este proyecto:

- **Para el *Probe* CDM:**

Tabla N° 20: Tabla de requerimientos del *probe* CDM

<i>Probe</i>	CPU, Disco, Memoria
Perfil de Usuario SO	root o Administrador
Reinicio SO	No Necesario
Requerimiento de Software	Para AIX 5.X: Las rutinas para obtener métricas de memoria, utilizan libperfstat, el cual debe estar instalado.
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU 32 o 64 bits

- **Para el *Probe* Processes:**

Tabla N° 21: Tabla de requerimientos del *probe* Processes

<i>Probe</i> processes	Procesos
Perfil de Usuario SO	root o Administrador
Reinicio SO	No Necesario
Requerimiento de Software	No Especifica
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU 32 o 64 bits

- **Para el *Probe Oracle*:**

Tabla N° 22: Tabla de requerimientos del *probe Oracle*

<i>Probe Oracle</i>	DB Oracle
Perfil de Usuario SO	No Necesario
Permisos Usuario Oracle	<p>Un usuario de base de datos con el privilegio 'SELECT_CATALOG_ROLE', 'gv_\$sort_segment' y 'sys.ts\$'.</p> <p>Se debe correr un script para este usuario de monitoreo (conectado como sys):</p> <pre>create user nimmon identified by nimmon; grant connect to nimmon; grant select_catalog_role to nimmon; grant select on gv_\$sort_segment to nimmon; grant select on sys.ts\$ to nimmon;</pre> <p>Nota: El usuario "system" tiene estos permisos ya otorgados.</p>
Reinicio de DB	No Necesario
Reinicio SO	No Necesario
Requerimiento de Software	Cliente Oracle 9.x, 10.x o 11.x
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

- **Para el *Probe Sqlserver*:**

Tabla N° 23: Tabla de requerimientos del *probe* Sqlserver

Probe SQLSERVER	BD SQL
Perfil de Usuario SO	No Necesario
Permisos Usuario SQL	<p>Se debe crear un usuario en la base de datos con los siguientes permisos:</p> <ul style="list-style-type: none"> • Para versiones SQL 9 y 10 configure el permiso VIEW SERVER STATE a la base de datos master. <p>También otorgue permisos SELECT al usuario para las siguientes tablas:</p> <ul style="list-style-type: none"> • master.sys.databases • master.dbo.sysperfinfo • msdb.dbo.sysjobsteps • msdb.dbo.sysjobs • .sys.database_files • .sys.partitions • .sys.allocation_units • .sys.internal_tables • .sys.filegroups <ul style="list-style-type: none"> • Para versión SQL 8 otorgue permisos SELECT al usuario para las siguientes tablas: <ul style="list-style-type: none"> • master.dbo.sysprocesses • master.dbo.sysperfinfo • master.dbo.sysdatabases • msdb.dbo.backupset

Probe SQLSERVER	BD SQL
	<ul style="list-style-type: none"> • master.dbo.sysfiles • master.dbo.sysindexes • master.dbo.sysfilegroups
Reinicio de DB	No Necesario
Reinicio SO	No Necesario
Requerimiento de Software	MDAC 2.5 o superior + ADO Provider. Cliente Nativo de SQL Server
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

- **Para el *Probe* interface_traffic:**

Tabla N° 24: Tabla de requerimientos del *probe* interface_traffic

Probe interface_traffic	Tráfico de interfaz
Perfil de Usuario SO	root o Administrator
Reinicio SO	No Necesario
Requerimiento de Software	El SNMP en el servidor a monitorear debe soportar la MIB-II ifTable.
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

<i>Probe interface_traffic</i>	Tráfico de interfaz
Puerto	Habilitar puerto SNMP (161 UDP) entre el <i>Probe</i> y el Servidor a monitorear si es que se va a aplicar monitoreo remoto.

- **Para el *Probe Exchange_monitor*:**

Tabla N° 25: Tabla de requerimientos del *probe* CDM Exchange_monitor

<i>Probe exchange_monitor</i>	Microsoft Exchange
Perfil de Usuario SO	Administrator
Usuario Exchange	Administrator
Reinicio de Exchange	No Necesario
Reinicio SO	No Necesario
Requerimiento de Software	.NET Framework v2.0 y MS PowerShell v1.0
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

- **Para el *Probe ad_server*:**

Tabla N° 26: Tabla de requerimientos del *probe* ad_server

<i>Probe ad_server</i>	Active Directory
Perfil de Usuario SO	Administrator
Usuario AD	Administrator
Reinicio de AD	No Necesario

<i>Probe ad_server</i>	Active Directory
Reinicio SO	No Necesario
Requerimiento de Software	.NET Framework 2.0
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

- **Para el *Probe netapp*:**

Tabla N° 27: Tabla de requerimientos del *probe netapp*

<i>Probe netapp</i>	Netapp
Perfil de Usuario SO	No Necesario
Usuario Netapp	Comunidad de lectura SNMP del Storage
Reinicio de Netapp	No Necesario
Reinicio SO	No Necesario
Requerimiento de Software	Netapp 7.2.x o superior
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits
Puerto	Habilitar puerto SNMP (161 UDP) entre el <i>Probe</i> y el Storage Netapp

- **Para el *Probe VMWare*:**

Tabla N° 28: Tabla de requerimientos del *probe VMWare*

Probe VMWare	VMware monitoring
Perfil de Usuario SO	No Necesario
Usuario VMWare	Usuario con Acceso al vCenter o ESX Server
Reinicio de VMW	No Necesario
Reinicio SO	No Necesario
Puerto	Habilitar el puerto para el ambiente REST API del vCenter o Servidor ESX. Típicamente el puerto es el 8443.

- **Para el *Probe url_response*:**

Tabla N° 29: Tabla de requerimientos del *probe url_response*

Probe url_response	url_response
Perfil de Usuario SO	No Necesario
Usuario	Usuario con salida a Internet (si aplica)
datos del proxy	Ip y datos de autenticación si los hubiera
SSL	Datos y contraseña del certificado si fuera necesario
Reinicio SO	No Necesario
Requerimiento de Software	No Especifica
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

- **Para el *Probe snmpcollector*:**

Tabla N° 30: Tabla de requerimientos del *probe snmpcollector*

<i>Probe snmpcollector</i>	snmp monitoring
Perfil de Usuario SO	No Necesario
Perfil de Usuario	Comunidad SNMP de lectura de los servidores a monitorear
Reinicio SO	No Necesario
Requerimiento de Software	.NET versión 3.5
Requerimiento de Memoria	Se requiere de 2.5 GB de memoria RAM (mínimo) disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPUs. 64 bits
Puerto	Habilitar puerto SNMP (161 UDP) entre el <i>Probe</i> snmpcollector y los servidores a monitorear remotamente

- **Para el *Probe net_connect*:**

Tabla N° 31: Tabla de requerimientos del *probe net_connect*

<i>Probe net_connect</i>	Conectividad de servidores
Perfil de Usuario SO	No necesario
Reinicio SO	No Necesario
Requerimiento de Software	No Especifica
Requerimiento de Memoria	Se requiere de 256 MB de memoria RAM disponible para este <i>Probe</i>
Requerimiento de CPU	3GHz dual core CPU. 32 o 64 bits

12.6 APÉNDICE 06: MÉTRICAS A MONITOREAR POR TIPO DE *PROBE*

Se han definido las siguientes métricas para monitorear por tipo de *probe*:

- Para el *Probe* CDM (monitoreo de CPU, Disco y Memoria en Windows, Linux y AIX):

Tabla N° 32: Tabla de métricas del *probe* CDM

Nombre de la métrica	Unidad	Descripción
Qos_cpu_multi_usage	Porcentaje	Individual cpu idle
	Porcentaje	Individual cpu system
	Porcentaje	Individual cpu usage (total)
	Porcentaje	Individual cpu user
	Porcentaje	Individual cpu wait
Qos_cpu_usage	Porcentaje	Cpu system
	Porcentaje	Uso de cpu
	Porcentaje	Cpu user
	Porcentaje	Cpu wait
Qos_disk_usage	Megabytes	Uso de disco
Qos_disk_usage_perc	Porcentaje	Uso de disco en porcentaje
Qos_inode_usage_perc	Porcentaje	Uso de inode en porcentaje
Qos_memory_usage	Megabytes	Uso de memoria
Qos_memory_perc_usage	Porcentaje	Uso de memoria en porcentaje
Qos_memory_swap	Megabytes	Uso de memoria swap
Qos_memory_swap_perc	Porcentaje	Uso de memoria swap en porcentaje
Qos_disk_available	Disponible	Disponibilidad de disco
Qos_computer_uptime	Segundos	Computer uptime
Iostat monitors: linux platform		
Qos_iostat_pu	Porcentaje	Porcentaje de uso de iostat
Iostat monitors: aix platform		
Qos_iostat_pcta	Porcentaje	Porcentaje de tiempo active de iostat
Qos_iostat_kbps	Kilobytes/seg	Iostat kilobytes transferred per second

- **Para el *Probe Processes* (monitoreo de procesos):**

Tabla N° 33: Tabla de métricas del *probe Processes*

Nombre de la métrica	Unidad	Descripción
Qos_process_cpu	Porcentaje	Uso de cpu del proceso
Qos_process_memory	Kilobytes	Uso de memoria del proceso
Qos_process_threads	Número	Threads del proceso
Qos_process_handles	Número	Handles del proceso

- **Para el *Probe Oracle*:**

Tabla N° 34: Tabla de métricas del *probe Oracle*

Nombre del métrica	Unidad	Descripción
Qos_oracle_flash_recovery_area_memory_free	Bytes	Monitors flash recovery area memory free
Qos_oracle_gc_service_util	Porcentaje	Calculado como: global cache service requests / logical reads measures global cache utilization. High number can result from insufficient cache size (sga). Also, it can indicate inappropriate spread of data and applications in the rac configuration.
Qos_oracle_memory_usage	Bytes	Mide la cantidad total de memoria (en bytes) user sessions consume (pga).
Qos_oracle_tablespace_free	Porcentaje	Measures percentage of free space in a table space, considering the maximal possible table space size. Note: oracle enterprise manager console does not consider maximum possible table space size on most of its screens (status 9i)!
Qos_oracle_tablespace_size	Mb	Mide el total de tamaño del table space

Nombre del métrica	Unidad	Descripción
Qos_oracle_user_locks	Locks	Lists user holding a lock. Helps to identify user, blocking other sessions (checkpoint locked_users).

- **Para el *Probe* Sqlserver:**

Tabla N° 35: Tabla de métricas del *probe* Sqlserver

Nombre de la métrica	Unidad	Descripción
Qos_sqlserver_alloc_space	Porcentaje	Free allocated space
Qos_sqlserver_av_fragmentation	Porcentaje	Average fragmentation
Qos_sqlserver_full_scans	Count/seg.	Full scans
Qos_sqlserver_long_queries	None	Monitors long running queries in seconds.
Qos_sqlserver_user_cpu	Porcentaje	Uso de cpu
Qos_sqlserver_page_reads	Count/seg.	Page reads
Qos_sqlserver_page_writes	Count/seg.	Page writes

- **Para el *Probe* Exchange_monitor:**

Tabla N° 36: Tabla de métricas del *probe* Exchange_monitor

Nombre de la métrica	Unidad	Descripción
Qos_exchange_memory_available_mbytes	Mb	Mbytes disponibles
Qos_exchange_memory_pages_input_per_second	Count	Pages input per second
Qos_exchange_memory_pages_output_per_second	Count	Pages output per second
Qos_exchange_trans_role_submission_queue_length	Msgs	Submission queue length

Nombre de la métrica	Unidad	Descripción
Qos_exchange_trans_role_retry_non-smtp_delivery_queue_length	Msgs	Retry non-smtp delivery queue length
Qos_exchange_trans_role_retry_remote_delivery_queue_length	Msgs	Retry remote delivery queue length
Qos_exchange_trans_role_largest_delivery_queue_length	Msgs	Largest delivery queue length
Qos_exchange_trans_role_poison_queue_length-transport	Msgs	Poison queue length-transport
Qos_exchange_trans_role_messages_received_per_sec-transport	Msgs/seg	Messages received per sec-transport
Qos_exchange_trans_role_messages_sent_per_sec-transport	Msgs/seg	Messages sent per sec-transport
Qos_exchange_mailbox_role_database_reads_(attached)_average_latency	Ms	Database reads (attached) average latency
Qos_exchange_mailbox_role_database_writes_(attached)_average_latency	Ms	Database writes (attached) average latency
Qos_exchange_mailbox_role_rpc_averaged_latency	Ms	Rpc averaged latency
Qos_exchange_mailbox_role_rpc_average_latency_-_mailbox	Ms	Rpc average latency - mailbox
Qos_exchange_mailbox_role_rpc_average_latency_-_client	Ms	Rpc average latency - client

Nombre de la métrica	Unidad	Descripción
Qos_exchange_mailbox_role_messages_queued_for_submission_mailbo	Msgs	Messages queued for submission mailbox
Qos_exchange_mailbox_role_messages_queued_for_submission_public	Msgs	Messages queued for submission public
Qos_exchange_mailbox_role_database_reads_average_latency	Ms	Database reads average latency
Qos_exchange_mailbox_role_database_writes_average_latency	Ms	Database writes average latency
Qos_exchange_mailbox_role_database_cache_size_information_store	Mb	Database cache size - information store.
Qos_exchange_cas_role_auto_discover_service_requests_per_sec	Reqs/sec	Auto discover service requests per sec.
Qos_exchange_cas_role_current_connections	Conn	Current connections.
Qos_exchange_cas_role_connection_attempts_per_sec	Conn/sec	Connection attempts per sec
Qos_exchange_dag_num_active_db	Db	Number of active database copies on current exchange server.
Qos_exchange_dag_num_passive_db	Db	Number of passive database copies on current mailbox server.
Qos_exchange_dag_num_mounted_db	Db	Number of mounted database copies on current mailbox server.
Qos_exchange_dag_num_not_mounted_db	Db	Number of database copies whose state is not "mounted" on current mailbox server.
Qos_exchange_dag_db_copy_queue_length	Files	Shows the number of transaction log files waiting to be copied to the passive copy log

Nombre de la métrica	Unidad	Descripción
		file folder. A copy isn't considered complete until it has been checked for corruption.
Qos_exchange_dag_db_replay_queue_length	Files	Shows the number of transaction log files waiting to be replayed into the passive copy.
Qos_exchange_dag_db_copy_status_failed	Bool	The mailbox database copy is in a failed state because it isn't suspended, and it isn't able to copy or replay log files. While in a failed state and not suspended, the system will periodically check whether the problem that caused the copy status to change to failed has been resolved. After the system has detected that the problem is resolved, and barring no other issues, the copy status will automatically change to healthy.
Qos_exchange_dag_db_copy_status_seeding	Bool	The mailbox database copy is being seeded, the content index for the mailbox database copy is being seeded, or both are being seeded. Upon successful completion of seeding, the copy status should change to initializing.
Qos_exchange_dag_db_copy_status_suspended	Bool	The mailbox database copy is in a suspended state as a result of an administrator manually suspending the database copy by running the suspend-mailboxdatabasecopy cmdlet.
Qos_exchange_dag_db_copy_status_healthy	Bool	The mailbox database copy is successfully copying and replaying log files, or it has successfully copied and replayed all available log files.
Qos_exchange_dag_db_copy_status_service_down	Bool	The microsoft exchange replication service isn't available or running on the server that hosts the mailbox database copy.
Qos_exchange_dag_db_copy_status_initializing	Bool	The mailbox database copy will be in an initializing state when a database copy has

Nombre de la métrica	Unidad	Descripción
		<p>been created, when the microsoft exchange replication service is starting or has just been started, and during transitions from suspended, servicedown, failed, seeding, singlepagerestore, lostwrite, or disconnected to another state. While in this state, the system is verifying that the database and log stream are in a consistent state. In most cases, the copy status will remain in the initializing state for about 15 seconds, but in all cases, it should generally not be in this state for longer than 30 seconds.</p>
Qos_exchange_dag_db_copy_status_resynchronizing	Bool	<p>The mailbox database copy and its log files are being compared with the active copy of the database to check for any divergence between the two copies. The copy status will remain in this state until any divergence is detected and resolved.</p>
Qos_exchange_dag_db_copy_status_mounted	Bool	<p>The active copy is online and accepting client connections. Only the active copy of the mailbox database copy can have a copy status of mounted.</p>
Qos_exchange_dag_db_copy_status_dismounted	Bool	<p>The active copy is offline and not accepting client connections. Only the active copy of the mailbox database copy can have a copy status of dismounted.</p>
Qos_exchange_dag_db_copy_status_mounting	Bool	<p>The active copy is coming online and not yet accepting client connections. Only the active copy of the mailbox database copy can have a copy status of mounting.</p>
Qos_exchange_dag_db_copy_status_dismounting	Bool	<p>The active copy is going offline and terminating client connections. Only the active</p>

Nombre de la métrica	Unidad	Descripción
		copy of the mailbox database copy can have a copy status of dismounting.
Qos_exchange_dag_db_copy_status_disconnected_and_healthy	Bool	The mailbox database copy is no longer connected to the active database copy, and it was in the healthy state when the loss of connection occurred. This state represents the database copy with respect to connectivity to its source database copy. It may be reported during dag network failures between the source copy and the target database copy.
Qos_exchange_dag_db_copy_status_disconnected_and_resynchronizing	Bool	The mailbox database copy is no longer connected to the active database copy, and it was in the resynchronizing state when the loss of connection occurred. This state represents the database copy with respect to connectivity to its source database copy. It may be reported during dag network failures between the source copy and the target database copy.
Qos_exchange_mail_send	Miliseg	Exchange mail send
Qos_exchange_dag_db_copy_status_failed_and_suspended	Bool	The failed and suspended states have been set simultaneously by the system because a failure was detected, and because resolution of the failure explicitly requires administrator intervention. An example is if the system detects unrecoverable divergence between the active mailbox database and a database copy. Unlike the failed state, the system won't periodically check whether the problem has been resolved, and automatically recover. Instead, an administrator must intervene to resolve the underlying cause of the failure

Nombre de la métrica	Unidad	Descripción
		before the database copy can be transitioned to a healthy state.
Qos_exchange_dag_db_copy_status_single_page_restore	Bool	This state indicates that a single page restore operation is occurring on the mailbox database copy.
Qos_exchange_dag_db_copy_size	Estado	Verifies that the cluster service is running and reachable on the local exchange server.
Qos_exchange_dag_cluster_service_health_status	Estado	Verifies that the instance of active manager running on the local exchange server is in a valid role (primary, secondary, or stand-alone).
Qos_exchange_dag_active_manager_health_status	Estado	Verifies that all dag members are available, running, and reachable.
Qos_exchange_dag_cluster_network_health_status	Estado	Verifies that all cluster-managed networks on the local exchange server are available.
Qos_exchange_dag_quorum_group_health_status	Estado	Verifies that the default cluster group (quorum group) is in a healthy and online state.
Qos_exchange_dag_file_share_quorum_health_status	Estado	Verifies that the witness server and witness directory and share configured for the dag are reachable.
Qos_exchange_mailbox_role_databasemounted	Bool	Indicates whether database copy is mounted on local server.
Qos_exchange_mailbox_role_exchange_search_zero_result_query	Bool	Indicates that more than one hundred search queries have returned zero results. This may indicate that a corruption or other problem affects the content indexing catalog.
Qos_exchange_mailbox_role_logical_disk_percentage_free_space	Porcentaje	Indicates the free space of logical disk in percentage.

Nombre de la métrica	Unidad	Descripción
Qos_exchange_anti_malware_anti-malware_agent_messages_scanned	Mensajes	Messages scanned is the number of messages scanned in the past minute.
Qos_exchange_anti_malware_anti-malware_agent_messages_scanned_per_second	Mensajes	Messages scanned per second is the average number of messages scanned each second, calculated over the past minute.
Qos_exchange_anti_malware_anti-malware_agent_messages_containing_malware	Mensajes	Messages containing malware is the number of messages in the past minute that contained malware.
Qos_exchange_anti_malware_anti-malware_agent_message_blocked	Mensajes	Messages blocked is the number of messages in the past minute that contained malware and were blocked.
Qos_exchange_delivery_health_monitor_aleratable_failure_dsns_within_the_last_hour	Mensajes	Hub selection resolver failures is the number of messages that encountered recipient. Ad lookup errors in hub selection.

- **Para el *Probe ad_server* (Active Directory):**

Tabla N° 37: Tabla de métricas del *probe ad_server*

Nombre de la métrica	Unidad	Descripción
Eventlogs		
Qos_numberofeventsfound		Numero de eventos encontrados
Files		
Qos_changed		Cambiado
Filesystems		
Qos_totalsize		Tamaño total
Performance counters		

Nombre de la métrica	Unidad	Descripción
Qos_fragmentation_failures	-	Fallas de fragmentación
Processes		
Qos_pagefaults	-	Page faults
Qos_pagefileusage	Kilobytes	Page file usage
Qos_peakpagefileusage	Kilobytes	Peak page file usage
Qos_peakvirtualsize	Bytes	Peakvirtualsize
Qos_peakworkingsetsize	Kilobytes	Peak working set size
Qos_threadcount	-	Thread count

- **Para el *Probe netapp*:**

Tabla N° 38: Tabla de métricas del *probe netapp*

Nombre de la métrica	Unidad	Descripción
Qos_storage_cifs_iops	Io por seg	Qos_storage_cifs iops
Qos_storage_cpu_utilization	Porcentaje	Qos_storage_cpu utilization
Qos_storage_failed_fan	Count	Qos_storage_failed fan
Qos_storage_failed_power_supply_count	Count	Qos_storage_failed power supply count
Qos_storage_fcp_average_latency	Ms	Qos_storage_fcp average latency
Qos_storage_fcp_iops	Io por seg	Qos_storage_fcp iops
Qos_storage_iops	Io por seg	Qos_storage_iops
Qos_storage_lun_iops	Io por seg	Qos_storage_lun iops
Qos_storage_lun_online	Info	Qos_storage_lun online
Qos_storage_lun_read_bytes	Kilobytes/se g	Qos_storage_lun read bytes
Qos_storage_lun_read_iops	Io por seg	Qos_storage_lun read iops
Qos_storage_lun_read_latency	Seg	Qos_storage_lun read latency
Qos_storage_lun_size_mb	Mbytes	Qos_storage_lun size
Qos_storage_lun_write_bytes	Kilobytes/se g	Qos_storage_lun write bytes
Qos_storage_lun_write_iops	Io por seg	Qos_storage_lun write iops

Nombre de la métrica	Unidad	Descripción
Qos_storage_lun_write_latency	Seg	Qos_storage_lun write latency
Qos_storage_number_of_failed_disks	Count	Qos_storage_number of failed disks
Qos_storage_nvram_battery_status	Info	Qos_storage_nvram battery status
Qos_storage_percent_capacity_used_aggr	Porcentaje	Qos_storage_percent capacity used
Qos_storage_percent_capacity_used_vol	Gbytes	Qos_storage_percent capacity used
Qos_storage_percent_snapshot_used_aggr	Porcentaje	Qos_storage_percent snapshot used
Qos_storage_percent_snapshot_used_vol	Porcentaje	Qos_storage_percent snapshot used
Qos_storage_tape_read	Kilobytes/seg	Qos_storage_tape read
Qos_storage_tape_write	Kilobytes/seg	Qos_storage_tape write
Qos_storage_total_average_latency	Ms	Qos_storage_total average latency
Qos_storage_total_capacity_aggr	Gbytes	Qos_storage_total capacity
Qos_storage_total_capacity_vol	Gbytes	Qos_storage_total capacity
Qos_storage_total_snapshot_capacity_aggr	Gbytes	Qos_storage_total snapshot capacity
Qos_storage_total_snapshot_capacity_vol	Gbytes	Qos_storage_total snapshot capacity
Qos_storage_volume_status	Info	Qos_storage_volume status
Qos_storage_volume_state	Info	Qos_storage_volume state
Qos_storage_lun_size_used	Gbytes	Qos_storage_lun size used
Qos_storage_lun_percent_used	Porcentaje	Qos_storage_lun percent used
Qos_storage_total_raw_capacity	Gbytes	Qos_storage_total raw capacity

- **Para el *Probe* VMWare:**

Tabla N° 39: Tabla de métricas del *probe* VMWare

Nombre del métrica	Unidad	Descripción
Qos_cpu_capacity	Megahertz	Cpu usage
Qos_cpu_usage	Porcentaje	Cpu usage (%)
Qos_cpu_usage_mhz	Megahertz	Cpu usage in mhz
Qos_disk_latency	Milisegundos	Disk latency
Qos_disk_read	Kbytes/ seg	Kbytes read for disk per second
Qos_disk_read_request	Requests/ seg	Disk read requests
Qos_disk_readwrite	Kbytes/ segundo	Kbytes written/read to/from disk per second
Qos_disk_write	Kbytes/ segundo	Kbytes written to disk per second
Qos_disk_write_request	Requests/ segundo	Disk write requests
Qos_memory_capacity	Mbytes	Total amount of memory
Qos_memory_perc_usage	Porcentaje	Memory usage in percent
Qos_memory_usage	Megabytes	Memory usage
Qos_snapshot_count	Count	Number of snapshots
Qos_snapshot_size	Gigabytes	Total disk space consumed by snapshots

- **Para el *Probe url_response*:**

Tabla N° 40: Tabla de métricas del *probe url_response*

Nombre del métrica	Unidad	Descripción
Qos_url_bytes	Bytes	Url bytes fetched
Qos_url_bytes_sec	Bytes/second	Url bytes per second
Qos_url_dnsresolve_time	Milisegundos	Time required for resolving the dns
Qos_url_download_time	Milisegundos	Time to download the contents
Qos_url_firstbyte_time	Milisegundos	Time to first byte
Qos_url_lastbyte_time	Milisegundos	Time to last byte
Qos_url_redirect_time	Milisegundos	Time for redirection

Nombre del métrica	Unidad	Descripción
Qos_url_response	Milisegundos	Url response
Qos_url_stringfound	Estado	Found string
Qos_url_tcpconnect_time	Milisegundos	Tcp connect time

12.7 APÉNDICE 07: LISTA DE CANTIDAD DE EQUIPOS A DESCUBRIR POR DIFERENTES CLIENTES

En la siguiente tabla se muestra la cantidad final de servidores agrupados por clientes a descubrir con respecto al sistema operativo y aplicaciones:

Tabla N° 41: Tabla de cantidad de servidores a descubrir

Sistemas Operativos	Cantidad
Ciente 01	48
Windows 7	1
Linux 2.6	1
Red Hat Enterprise Linux 6	5
Windows Server 2003 R2 Standard	4
Windows Server 2008 Enterprise	10
Windows Server 2008 R2 Enterprise	13
Windows Server 2008 Standard	1
HP-UX 11.23	3
Centos 8	1
ESX 4.0	6
ESX 5.0	3
Ciente 02	26
Windows Server 2003 R2 Enterprise	4
Windows Server 2003 R2 Standard	1
Windows Server 2008 R2 Standard	9
Windows Server 2008 Standard	10
ESX 4.1	2
Ciente 03	12
Windows Server 2003 Standard	4
Windows Server 2008 R2 Enterprise	6
ESX 4.0	2
Ciente 04	7
Windows Server 2003 Standard	7
Ciente 05	15
Linux 2.6	5
Windows Server 2008 Enterprise	3
Windows Server 2008 Standard	7
Ciente 06	10
Windows 7 Professional SP1	1

Sistemas Operativos	Cantidad
Windows Server 2003 Enterprise	1
Windows Server 2008 Enterprise	4
Windows Server 2008 Standard	1
HP-UX 11.31	2
HP-UX 11.11	1
Cliente 07	15
Linux 2.6	6
Windows Server 2003 Enterprise	4
Windows Server 2008 Enterprise	5
Cliente 08	24
Red Hat Enterprise Linux 5.5	3
Windows Server 2003 Enterprise	4
Windows Server 2003 R2 Enterprise	7
Windows Server 2003 Standard	3
Windows Server 2008 R2 Standard	7
Cliente 09	10
Cryptosign	2
Red Hat Enterprise Linux 5	1
TimeTools	2
Windows Server 2008 R2 Enterprise	1
Windows Server 2008 R2 Standard	4
Cliente 10	90
Windows Server 2000	1
Windows Server 2003 Enterprise	1
Windows Server 2003 R2 Enterprise	1
Windows Server 2008 Enterprise	2
Windows Server 2008 R2 Enterprise	23
Windows Server 2008 R2 Standard	7
Windows Server 2008 Standard	1
Red Hat Enterprise Linux 5	7
Red Hat Enterprise Linux 5.8	2
Ubuntu Server 12.10	1
Windows Server 2003 Enterprise	10
Windows Server 2003 R2 Enterprise	1
Windows Server 2003 Standard	1
Windows Server 2008 Enterprise	13
Windows Server 2008 R2 Enterprise	10
Windows Server 2008 Standard	1
ESXi 5.0	8
Cliente 11	7
HP-UX 11.11	7
Cliente 12	9

Sistemas Operativos	Cantidad
Windows Server 2003 Enterprise	9
Cliente 13	11
Windows Server 2003 R2 Enterprise	3
Windows Server 2003 R2 Standard	1
Windows Server 2003 Standard	1
Windows Server 2008 R2 Standard	3
Windows Server 2008 Standard	3
Cliente 14	3
Windows Server 2008 Standard	3
Cliente 15	5
Windows Server 2008 R2 Enterprise	1
Windows Server 2008 R2 Standard	2
ESX 4.0	2
Cliente 16	38
Windows Server 2008 Standard	5
Red Hat Enterprise Linux 5.5	6
Windows Server 2003 Enterprise	5
Windows Server 2008 R2 Standard	7
HP-UX 11.31	15
Cliente 17	20
Windows Server 2008 R2 Standard	7
Red Hat Enterprise Linux 6.2	8
AIX 7	5
Cliente 18	20
Red Hat Enterprise Linux 4	4
Windows Server 2003 R2 Standard	13
Windows Server 2008 R2 Standard	1
Windows Server 2000 Advanced	1
Windows Server 2000	1
Cliente 19	13
Windows Server 2008 Standard	6
Red Hat Enterprise Linux 4	5
HP-UX 11.31	1
ESXi 5.0	1
Cliente 20	65
Windows Server 2000	6
Windows Server 2003 Enterprise	2
Windows Server 2003 R2 Enterprise	1
Windows Server 2003 R2 Standard	8
Windows Server 2008 Enterprise	22
Windows Server 2008 Standard	6
Windows XP Professional	1

Sistemas Operativos	Cantidad
Red Hat Enterprise Linux 5	2
Windows Server 2008 R2 Standard	1
ESX 4.0	1
AIX 7.1	7
ESX 4.0	8
Ciente 21	91
Linux 2.6	74
Windows Server 2008 R2 Enterprise	5
Windows Server 2008 R2 Standard	2
ESX 4.0	10
Ciente 22	2
Windows Server 2008 Enterprise	2
Grand Total	541

Además de la cantidad de equipos mostrados, GMD cuenta con 80 servidores propios para brindar el servicio a sus clientes, con lo cual hace un total de 621 servidores para la compra de licencias *Nimsoft Monitor Server Pack On-Prem*.

En la tabla N° 42, se muestra la cantidad final de equipos de comunicaciones por cliente a descubrir con la herramienta:

Tabla N° 42: Tabla de equipos de comunicaciones a descubrir

Equipo de comunicación	Cantidad
Ciente 01	8
Cisco Router 1800	1
Cisco Router 1841	1
Cisco Router 2801	2
Cisco Router 871	1
Cisco RPS 300	1
Cisco Switch Catalyst 2950	1
Fortinet Antispam 400B	1
Ciente 02	4
Cisco Router 1841	1
Cisco Router 2800	1
Cisco Router 2811	1
Cisco Switch Catalyst 2950	1
Ciente 03	48

Equipo de comunicación	Cantidad
Cisco Firewall ASA 5510	3
Cisco Firewall ASA 5520	1
Cisco Firewall ASA 5540	2
Cisco MCS 7800	4
Cisco Router 1700	1
Cisco Router 1800	3
Cisco Router 1841	1
Cisco Router 2600	2
Cisco Router 2610XM	1
Cisco Router 2800	2
Cisco Router 2811	1
Cisco Router 2821	1
Cisco Router 3700	1
Cisco Router 800	1
Cisco Switch	1
Cisco Switch Catalyst 2970	1
Cisco Switch Catalyst 3750	10
Cisco Switch Catalyst 4503	1
Fortigate 200B	2
HP Procurve 2910	1
HP Storage Works 4/8	1
HP Storage Works 8/8 switch SAN	2
HP Switch GbE2c Layer 2/3	2
HP Switch SAN	2
HP Switch SAN BladeSystem c-Class	1
Cliente 04	12
Cisco Router 851	4
Cisco Switch 4503 -E	1
Cisco Switch Catalyst 2950	1
Cisco Switch Catalyst 3560G	1
Cisco Switch Catalyst 3750	2
HP San Switch 4/16	2
HP Storage Works 4/8	1
Cliente 05	44
Barracuda 330 Balanceador	2
Cisco Firewall ASA 5505 Appliance	1
Cisco Firewall ASA 5510	1
Cisco Router 1700	1
Cisco Router 1800	2
Cisco Router 1841	3
Cisco Router 1905	1
Cisco Router 1941	1
Cisco Router 2600	1

Equipo de comunicación	Cantidad
Cisco Router 2800	3
Cisco Router 2801	2
Cisco Router 2811	1
Cisco Router 2821	2
Cisco Router 2911	2
Cisco Router 3600	1
Cisco Router 3700	1
Cisco Router 3825	2
Cisco Router 7200	1
Cisco Router 7206	1
Cisco Router 800	2
CISCO Router 881	2
Cisco Router RPS	2
Cisco Switch Catalyst 2950	2
Cisco Switch Catalyst 2970	2
Cisco Switch Catalyst 3750	3
HP Storage Works MSL4048	1
SWITCH AT-8524M 24PTOS	1
Cliente 06	22
Cisco Firewall ASA 5505 Appliance	1
Cisco Router 1841	1
Cisco Router 2600	1
Cisco Router 2800	1
CISCO Router 881	1
CISCO Switch ASR-1006	1
Cisco Switch Catalyst 2900 XL, 12 Ports	1
Cisco Switch Catalyst 2950	4
Cisco Switch Catalyst 3524	1
Cisco Switch Catalyst 3560G	1
Cisco Switch Catalyst 3750	3
Cisco Switch Catalyst 4506	1
Cisco Switch Catalyst 7604	2
CISCO UCS C210 M2	1
HP Switch E01013	1
Micronet Switch	1
Cliente 07	12
Cisco Firewall ASA 5510	2
Cisco Firewall PIX 515	1
Cisco Firewall PIX 515E	1
Cisco Router 2600	1
Cisco Router 2800	2
Cisco Router 2811	1

Equipo de comunicación	Cantidad
Cisco Switch Catalyst 3550	1
Cisco Switch Catalyst 3560G	1
Cisco Switch Catalyst 3750	2
Total	150

Además de la cantidad de equipos mostrados, GMD cuenta con 24 equipos de comunicaciones propios para brindar el servicio a sus clientes, con lo cual hace un total de 174 equipos de comunicaciones para la compra de licencias *CA - IM (Spectrum)*.

12.8 APÉNDICE 08: DETALLE DE FLUJO DE CAJA MENSUAL

Concepto	PRIMER AÑO											
	1	2	3	4	5	6	7	8	9	10	11	12
Ingresos	0	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92	22,8 92
Egresos	18,2 74	18,2 74	18,2 74	18,2 74	18,2 74	21,3 62						
Costo Bienes y Subcontrata	9,47 1	9,47 1	9,47 1	9,47 1	9,47 1	12,5 59						
Mano de Obra	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7	3,81 7
Gastos Generales	107	107	107	107	107	107	107	107	107	107	107	107
Gastos Generales Directos	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Generales Asignados	107	107	107	107	107	107	107	107	107	107	107	107
Inversión (Equipos y Software)	3,87 3	3,89 8	3,92 3	3,94 8	3,97 4	3,99 9	4,02 5	4,05 1	4,07 7	4,10 3	4,13 0	4,15 6
Gastos Financieros	1,00 6	981	956	931	905	880	854	828	802	776	749	723
Flujo de Proyecto	- 18,2 74	4,61 8	4,61 8	4,61 8	4,61 8	1,53 0						
Riesgo	914	914	914	914	914	1,06 8						
GG Línea	0	389	389	389	389	389	389	389	389	389	389	389
Flujo de Caja Bruto	- 19,1 87	3,31 6	3,31 6	3,31 6	3,31 6	5,85 73	5,77 73	5,70 73	5,63 73	5,55 73	5,48 73	5,41 73
Flujo Acumulado	- 19,1 87	- 15,8 72	- 12,5 56	- 9,24 1	- 5,92 5	- 5,85 2	- 5,77 9	- 5,70 6	- 5,63 3	- 5,55 9	- 5,48 6	- 5,41 3

Concepto	SEGUNDO AÑO											
	13	14	15	16	17	18	19	20	21	22	23	24
Ingresos	22,8 92											
Egresos	21,3 62											
Costo Bienes y Subcontrata	12,5 59											
Mano de Obra	3,81 7											
Gastos Generales	107	107	107	107	107	107	107	107	107	107	107	107
Gastos Generales Directos	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Generales Asignados	107	107	107	107	107	107	107	107	107	107	107	107
Inversión (Equipos y Software)	4,18 3	4,21 0	4,23 7	4,26 4	4,29 2	4,31 9	4,34 7	4,37 5	4,40 3	4,43 2	4,46 0	4,48 9
Gastos Financieros	696	669	642	615	587	560	532	504	476	447	419	390
Flujo de Proyecto	1,53 0											
Riesgo	1,06 8											
GG Línea	389	389	389	389	389	389	389	389	389	389	389	389
Flujo de Caja Bruto	73	73	73	73	73	73	73	73	73	73	73	73
Flujo Acumulado	- 5,34 0	- 5,26 7	- 5,19 3	- 5,12 0	- 5,04 7	- 4,97 4	- 4,90 1	- 4,82 8	- 4,75 4	- 4,68 1	- 4,60 8	- 4,53 5

Concepto	TERCER AÑO											
	25	26	27	28	29	30	31	32	33	34	35	36
Ingresos	22,8 92											
Egresos	21,3 62											
Costo Bienes y Subcontrata	12,5 59											
Mano de Obra	3,81 7											
Gastos Generales	107	107	107	107	107	107	107	107	107	107	107	107
Gastos Generales Directos	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Generales Asignados	107	107	107	107	107	107	107	107	107	107	107	107
Inversión (Equipos y Software)	4,51 8	4,54 7	4,57 6	4,60 5	4,63 5	4,66 5	4,69 5	4,72 5	4,75 5	4,78 6	4,81 7	4,84 8
Gastos Financieros	361	332	303	274	244	214	184	154	124	93	62	31
Flujo de Proyecto	1,53 0											
Riesgo	1,06 8											
GG Línea	389	389	389	389	389	389	389	389	389	389	389	389
Flujo de Caja Bruto	73	73	73	73	73	73	73	73	73	73	73	73
Flujo Acumulado	4,46 2	4,38 9	4,31 5	4,24 2	4,16 9	4,09 6	4,02 3	3,95 0	3,87 6	3,80 3	3,73 0	3,65 7

Concepto	CUARTO AÑO											
	37	38	39	40	41	42	43	44	45	46	47	48
Ingresos	22,8 92											
Egresos	16,4 83											
Costo Bienes y Subcontrata	12,5 59											
Mano de Obra	3,81 7											
Gastos Generales	107	107	107	107	107	107	107	107	107	107	107	107
Gastos Generales Directos	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Generales Asignados	107	107	107	107	107	107	107	107	107	107	107	107
Inversión (Equipos y Software)	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Financieros	0	0	0	0	0	0	0	0	0	0	0	0
Flujo de Proyecto	6,40 9											
Riesgo	824	824	824	824	824	824	824	824	824	824	824	824
GG Línea	389	389	389	389	389	389	389	389	389	389	389	389
Flujo de Caja Bruto	5,19 6											
Flujo Acumulado	1,53 9	6,73 5	11,9 32	17,1 28	22,3 24	27,5 20	32,7 16	37,9 12	43,1 08	48,3 05	53,5 01	58,6 97

Concepto	QUINTO AÑO													61
	49	50	51	52	53	54	55	56	57	58	59	60		
Ingresos	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892	22,892
Egresos	16,483	16,483	16,483	16,483	16,483	16,483	16,483	16,483	16,483	16,483	16,483	16,483	16,483	0
Costo Bienes y Subcontrata	12,559	12,559	12,559	12,559	12,559	12,559	12,559	12,559	12,559	12,559	12,559	12,559	12,559	0
Mano de Obra	3,817	3,817	3,817	3,817	3,817	3,817	3,817	3,817	3,817	3,817	3,817	3,817	3,817	0
Gastos Generales	107	107	107	107	107	107	107	107	107	107	107	107	107	0
Gastos Generales Directos	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Generales Asignados	107	107	107	107	107	107	107	107	107	107	107	107	107	0
Inversión (Equipos y Software)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gastos Financieros	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flujo de Proyecto	6,409	6,409	6,409	6,409	6,409	6,409	6,409	6,409	6,409	6,409	6,409	6,409	6,409	22,892
Riesgo	824	824	824	824	824	824	824	824	824	824	824	824	824	0
GG Línea	389	389	389	389	389	389	389	389	389	389	389	389	389	389
Flujo de Caja Bruto	5,196	5,196	5,196	5,196	5,196	5,196	5,196	5,196	5,196	5,196	5,196	5,196	5,196	22,503
Flujo Acumulado	63,893	69,089	74,285	79,482	84,678	89,874	95,070	100,266	105,462	110,658	115,855	121,051	126,247	143,554

13 CRONOGRAMA

A continuación se detalle el cronograma ejecutado como parte del proyecto:

Nombre de tarea	% Complete	Work	Start	Finish
[-] Implementación de sistema de monitoreo de servidores y aplicaciones	94%	962.8 hours	Mon 28/04/14	Thu 08/01/15
[-] EJECUCIÓN	94%	962.8 hours	Mon 28/04/14	Thu 08/01/15
[-] <u>FASE 1 - Evaluación de requerimientos del sistema de monitoreo para servidores y aplicaciones</u>	100%	112 hours	Mon 28/04/14	Thu 15/05/14
Entrevista con áreas internas	100%	24 hours	Mon 28/04/14	Wed 30/04/14
Reuniones con proveedores	100%	32 hours	Mon 05/05/14	Thu 08/05/14
Levantamiento de información de la solución actual	100%	24 hours	Mon 28/04/14	Wed 30/04/14
Desarrollo de documento RFP	100%	32 hours	Mon 12/05/14	Thu 15/05/14
Hito Documento RFP elaborado	100%	0 hours	Thu 15/05/14	Thu 15/05/14
[-] <u>FASE 2 - Evaluación de la herramienta para el sistema de monitoreo para servidores y aplicaciones</u>	100%	66 hours	Mon 09/06/14	Fri 13/06/14
Revisión de la infraestructura actual y requisitos	100%	2 hours	Mon 09/06/14	Mon 09/06/14
Upgrade de SO E-Health a W2008 64 bits	100%	64 hours	Tue 20/05/14	Thu 29/05/14
Hito Herramienta de sistema de monitoreo seleccionada	100%	0 hours	Mon 18/08/14	Mon 18/08/14
Kick off	100%	2 hours	Thu 05/06/14	Thu 05/06/14
[-] <u>FASE 3 - Implementación del sistema de monitoreo de servidores y aplicaciones</u>	92%	782.8 hours	Mon 09/06/14	Thu 08/01/15
[-] Implementación del sistema de monitoreo	93%	778 hours	Mon 09/06/14	Thu 23/10/14
Estabilización del sistema de monitoreo	70%	4.8 hours	Mon 29/12/14	Wed 31/12/14
Hito Sistema de monitoreo de servidores y aplicaciones implementada	80%	0 hours	Mon 18/08/14	Wed 31/12/14
CIERRE	0%	0 hours	Thu 08/01/15	Thu 08/01/15