Universidad Hispanoamericana

**Facultad de Ingeniería Informática**

Trabajo Final de Graduación:

# Rediseño del proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma.

Sustentante:

**Oscar A. Corrales Carmona**

Tutor:

**Ing. Edgar Ugalde Saborío, MATI**

**18 de febrero de 2024**

## Índice General

## Índice de Tablas

**Índice de Figuras**

# Declaración Jurada

**DECLARACIÓN JURADA**

Yo Oscar Alonso Corrales Carmona mayor de edad, portador de la cédula de identidad número 1-1165-0108 egresado de la carrera de Ingeniería Informática , de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática con énfasis en Sistemas de Información , juro solemnemente que mi trabajo de investigación titulado: Desarrollo de un rediseño del proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma , es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público. en fe de lo anterior, firmo en la ciudad de San José, a los 21 días del mes de febrero , del año dos mil veinticuatro .

Firma del estudiante

Cédula 1-1165-0108

# Carta de Aprobación del Tutor

Alajuela, 24 de febrero de 2024

**CARTA DEL TUTOR**

***MATI Katia Huertas***
***Escuela Ingeniería de Informática***
***Universidad Hispanoamericana***

Estimado señor:

El estudiante Corrales Carmona Oscar, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado ***Desarrollo del rediseño del proceso de monitoreo de infraestructura de TI ofrecido por empresa GosysPro para la obtención de un ciclo de mejora de Lean Six Sigma e incluyendo las mejores prácticas de Cobit 2019,*** el cual ha elaborado para optar por el grado académico de licenciatura

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

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

| | | | |
|---|---|---|---|
| a) | ORIGINAL DEL TEMA | 10% | 10 |
| b) | CUMPLIMIENTO DE ENTREGA DE AVANCES | 20% | 20 |
| C) | COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION | 30% | 27 |
| d) | RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES | 20% | 18 |
| e) | CALIDAD, DETALLE DEL MARCO TEORICO | 20% | 20 |
| | TOTAL | 100% | 95 |

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

Atentamente,

Digitally signed by EDGAR ALBERTO UGALDE SABORIO (FIRMA)
Reason: I attest to the accuracy and integrity of this document
Location: 20403, Jesús María, San Mateo Alajuela, Costa Rica
Date: 2024.02.27 00:54:58 -06'00'

***Ing. Edgar Ugalde Saborío, MATI***
***Cédula identidad 1-1102-0350***
***Carné CPIC 3163***

# Carta de Aceptación del CEO de GosysPro

GOSYSPRO
INNOVATING IT SERVICES

13 de marzo 2023

Oficio Nº 0124 – 2023

**Asunto:** Autorización para realizar tesis universitaria Oscar Corrales Carmona

Señor
Julián Córdoba Sanabria
Coordinador de Investigación
Universidad Hispanoamericana

Estimado Señor:

Reciba un cordial saludo.

Por este medio, me permito manifestar el interés de nuestra empresa GosysPro en el proyecto denominado DESARROLLO DE UNA AUDITORÍA AL PROCESO DE MONITOREO Y OBSERVABILIDAD REALIZADO POR LA EMPRESA GOSYSPRO". El cual será presentado por el estudiante Oscar Alonso Corrales Carmona, cédula de identidad 1-1165-0108 para ser realizado en el Centro de Operaciones de red NOC).

Cabe resaltar que este proyecto será de gran valor para nuestra firma ya que servirá para mejorar el servicio de monitoreo que ofrecemos actualmente según los estándares de la industria. En adición a lo anterior. Yo en mi calidad de propietario de la firma GosysPro participaré en la defensa y patrocinio del estudiante.

Quedo atento a cualquier consulta o detalle adicional.

Atentamente,

**ING. Ronaldo Salas Apú**
CEO y propietario
**GosysPro**

CC: archivo

GosysPro
Teléfono 8821932 | Correo: rsalas@gosyspro.com | www.gosyspro.com

# Carta de Aprobación del Lector

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera de Informática

Estimado señor

El estudiante Oscar Corrales Carmano, cédula de identidad 1-1165.0108, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "Rediseño del proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma".

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

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

Atte.

Randall Vargas Villalobos

Firmado digitalmente por Randall Vargas Villalobos
Fecha: 2024.04.22 07:29:58 -06'00'

Firma
Randall Vargas Villalobos
Cédula: 1-1140-0113

# Carta de autorización para publicación de documento en CENIT

**UNIVERSIDAD HISPANOAMERICANA**
**CENTRO DE INFORMACION TECNOLOGICO (CENIT)**
**CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION**

San José, 24 de abril de 2024

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Oscar Alonso Corrales Carmona con número de identificación 1-1165-0108, autor (a) del trabajo de graduación titulado Rediseño del proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma, presentado y aprobado en el año 2024 como requisito para optar por el título de SÍ ; (SI / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Cédula 1-1165-0108

Firma y Documento de Identidad

**Dedicatoria**

El presente documento se lo deseo dedicar a mi amada tía Rebeca Carmona Seas (QDDG), quien siempre creyó en mí y me invitó a nunca rendirme y creer en mis sueños y anhelos. Mi madrina amada, para ti con amor.

**Agradecimientos**

- Deseo agradecer en primera instancia a Dios Todopoderoso. Creador y autor de la vida, la inteligencia, la sabiduría. Por permitirme vivir cada etapa de este proceso.
- Un agradecimiento profundo a mi amada esposa Alejandra, quien nunca me dejó caer ni rendirme.
- Agradezco a mis padres Oscar y Martha quienes me dieron la vida y la mejor educación. Nunca me desampararon en el desarrollo de este trabajo, pese a muchas otras vicisitudes.
- A mis hermanos Iván, Irene, Dany, Xenia, Adriana, César, Marianela por estar siempre conmigo y sostenerme cuando estuve a punto de desfallecer.
- A don Edgar y doña Iris, por su generosidad y paciencia.
- A mis sobrinitos y ahijaditos Luciano, Daniel, Fabián y Paola.
- Al tutor Edgar Ugalde, quien siempre estuvo en disposición de ayudarme y aconsejarme, aún en días y horas no hábiles.
- A todo el personal docente de la Universidad Hispanoamericana, por transmitirme sus valiosos conocimientos.
- A mis compañeros y excompañeros de carrera, quienes me acompañaron en este largo viaje.

**Abreviaturas**

- BOT: Programa que imita el comportamiento humano
- BOT: Robot que imita o sustituye el accionar humano. Opera en forma automatizada, por lo que pueden trabajar mucho más rápido que una persona.
- CEO: Persona con el máximo nivel de poder en una organización.
- Ciclo DMAIC: Siglas en inglés de las palabras Definir, Medir, Analizar, Mejorar (Improve), Control
- Cobit 2019: Objetivos de control para tecnologías de la información y tecnologías relacionadas por sus siglas en inglés.
- KPI: Indicador clave de rendimiento (key performance indicator)
- Lean Six Sigma: Lean Six Sigma es una metodología de mejora de procesos, que busca establecer herramientas estadísticas y análisis de datos para una aplicación práctica en los proyectos de mejora de la calidad de los procesos.
- NOC: Centro de operaciones de red (network operation center)
- OLA: Acuerdo de nivel operacional (operative level agreement)
- RPA: Automatización Robótica de Procesos
- SIPOC: Proveedor, Entrada, Proceso, Salida, Cliente.
- SLA: Acuerdo de nivel de servicio (Service Level Agreement)
- SOP: Procedimientos operativos estandarizados.
- TI: Tecnologías de Información
- VSM: Value Stream Map (Mapa de Cadena de Valor)

**Resumen**

El presente documento consiste en una revisión y análisis del Servicio de Monitoreo de Infraestructura de Tecnologías de Información ofrecido por la compañía Gosys Pro.

El servicio de Monitoreo, actualmente se encuentra operativo, no obstante, el mismo se realiza de forma empírica según la experiencia del CEO y sus colaboradores. No existen manuales documentados ni estadísticas que muestren el valor generado por el proceso de monitoreo.

Por medio de la metodología Lean Six Sigma, se utilizan algunas útiles herramientas las cuales servirán para identificar la situación actual de este servicio, identificar sus brechas, y en contraparte, proponer las mejoras correspondientes.

Las mejoras propuestas ayudarán a que el servicio de Monitoreo esté alineado con el estándar Cobit 2019, así como una reducción sustancial en tiempos, costos y desperdicios.

**Abstract**

This document consists in a review and analysis of Information Technologies Monitoring Services offered by Gosys Pro.

This Monitoring Service is operative but is done empirically according to the experience of its collaborators. Some elements like documented manuals or statistics showing the generated value are missing.

Through the Lean Six Sigma methodologies, some tools will be used for identifying the current situation of this service, identify failures and propose the corresponding improvements.

The proposed improvements will help to align the Monitoring Services with Cobit 2019 standards. Also, will help to reduce costs, spent time and waste.

# Capítulo I: INTRODUCCIÓN

Conforme crecen las empresas, ellas necesitan de un servicio de Tecnologías de Información cada vez más complejo, robusto, sobre todo, Seguro. Esto por cuanto, las necesidades del negocio requieren de tecnologías de avanzada, así como metodologías ágiles de resolución de conflictos. Sería impensable la existencia de una organización careciente de la tecnología suficiente para la ejecución de sus procesos de negocio.

En la actualidad, son constantes las noticias que aluden a tópicos tales como Inteligencia de Negocios, Seguridad de la Información, Continuidad del Negocio, Servicios personalizados, así como otra gran variedad de conceptos interesantes que invocan a ciclo constante de innovación y mejora continua. Esta creciente y continua necesidad de servicios tecnológicos, nos obliga a efectuar enormes inversiones en la optimización de plataformas informáticas y de comunicación.

Es importantísimo recalcar que las empresas requieren que las plataformas tecnológicas sean lo suficientemente robustas como para poder soportar las operaciones diarias.

Con el fin de lograr este objetivo, las empresas invierten cuantiosas sumas de dinero en la adquisición de servicios de Monitoreo y Observabilidad de TI. En caso de carecer de los recursos necesarios, suelen subcontratar un servicio tercerizado.  Lo anterior para garantizar una adecuada política de continuidad de negocio la cual provea un riguroso control sobre la salud de los sistemas y así garantizar que la información sea veraz, concreta, completa, analizable y sobre todo que esté a la mano de la forma más expedita posible.

Es de todos los días escuchar frases tales como “se cayó el sistema”, “ocurrió un problema de red”, “colapsó el servidor”, “el sistema está lento”. Esto ocurre porque las políticas de continuidad del negocio son inexistentes o inmaduras. Por eso, es vital recalcar lo mencionado líneas atrás: La infraestructura tecnológica debe ser lo suficientemente robusta y ágil como para

lograr un óptimo tráfico de la información y mantener la continuidad y disponibilidad de los servicios de tecnología.

Ante esta situación, se debe contar con una adecuada política de monitoreo y observabilidad que permita prevenir posibles fallos, así como brindar una rápida respuesta en caso de que ocurra un evento.

Dicho proceso de Monitoreo y observabilidad debe responder no solo a los requerimientos de la organización, sino que debe efectuarse con excelencia y calidad comprobada. Dicha calidad debe ser consecuente con los mejores estándares de Tecnologías de Información.

Este trabajo consiste en la revisión profunda de los procesos de Monitoreo y observabilidad ofrecidos por la empresa Gosys Pro. De forma que se detecten posibles falencias, y en contraparte; proponer las respectivas para subsanar dichas brechas según las sanas prácticas dictadas por el marco Cobit 2019.

Se presenta en seguida una descripción de los antecedentes, la problemática, un breve análisis de la situación y un planteamiento de objetivos que sean de utilidad para corregir dicho problema.

## 1.1. Antecedentes

La empresa GOSYS PRO, es una “pyme” que nace en el año 2018 como una solución alternativa para las organizaciones que necesitan contar con un servicio tercerizado de Monitoreo de TI a un costo más económico que el brindado por otras opciones de la industria. Esto se debe a que los servicios ofrecidos por Gosys Pro, están alojados en la nube, y utilizan la integración de varias herramientas de código abierto.

Dicha organización tiene su domicilio en San Pablo de Heredia, cuenta con una planilla de tan solo 6 personas. Conforme la empresa vaya creciendo, será imperativo abrir nuevas plazas para contratar nuevos talentos.

Entre otros servicios, el más importante ofrecido actualmente por la empresa consiste en un Centro de Operaciones de Red (NOC). Dicho servicio está en producción y el cliente que lo recibe es una entidad financiera de capital privado.

Por su parte. El CEO de la empresa, cuenta con una experiencia superior a los 12 años en gestión de Centros de Monitoreo de TI ya que ha laborado previamente en algunas empresas tales GBM, CMA, SONDA, CHEETAH y el Instituto Nacional de Seguros.

Cabe resaltar que el sustentante del presente documento carece de cualquier vínculo laboral con la firma Gosys Pro.

Seguidamente, se presenta una pequeña descripción de los valores de la firma Gosys Pro con el fin de comprender un poco más su cultura organizacional.

**Misión de Gosys Pro:**

Ser una solución alternativa y económica como outsourcing de servicios de TI.

**Visión de Gosys Pro:**

Ser la una organización líder en el ámbito de soluciones de monitoreo y servicios varios de TI y negocio aplicando las mejores prácticas de la industria.

**Valores generales de Gosys Pro:**

- Innovación: En una constante búsqueda de nuevas formas de hacer las cosas con el fin de optimizar la calidad del servicio de monitoreo.
- Dinamismo; Consiste en una actitud activa e inquieta hacia el logro de los objetivos institucionales.
- Ética: Siempre se trabaja acorde con las mejores y sanas conductas morales, respetando lineamientos y regulaciones nacionales e internacionales.
- Responsabilidad: Responder oportuna y correctamente a los requerimientos, necesidades e imprevistos que puedan ocurrir, actuando proactiva, asertiva y positiva.

Al ser Gosys Pro una pyme con poco tiempo en operación, carece de un adecuado nivel de madurez en cuanto a estándares para el monitoreo de Servicios de Infraestructura de TI.

Reiterando lo mencionado anteriormente, Gosys Pro cuenta con un Centro de Operaciones de Red (NOC). El mismo, se encuentra operativo y cuenta con un cliente que goza de dicha facilidad en sus servicios de producción.

## 1.2. Justificación y descripción del problema

El problema raíz, consiste en que el Servicio de Monitoreo de Infraestructura de TI ofrecido por Gosys Pro carece de un adecuado nivel de madurez y estandarización. Dicha carencia podría

provocar pérdidas en cuanto a tiempo de respuesta, calidad de resolución y costos. Tanto para la organización patrocinadora, como para los clientes.

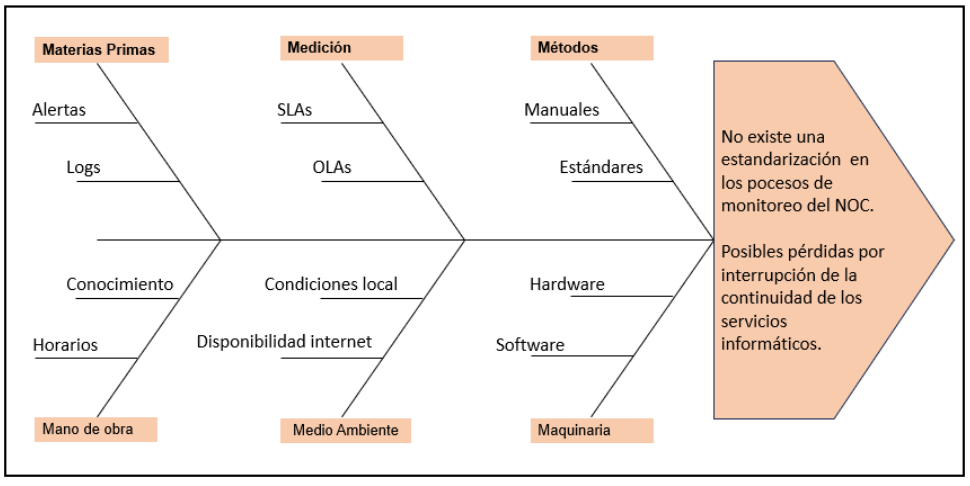
En cuanto al desarrollo de sus operaciones. Se observa de reojo que la empresa utiliza varias herramientas para realizar el proceso de monitoreo y observabilidad, de las cuales algunas son de software libre. Dichas plataformas de Monitoreo de TI conforman sistemas de vigilancia continua, alertas y escalamientos en caso de ocurrir incidencias. Dichas incidencias se resuelven en un plazo definido según los niveles de escalamiento.

Por otra parte, a nivel de mercado, la empresa tiene la expectativa de proyectarse y diversificar sus servicios para lograr un mejor posicionamiento. De esa manera, se desea brindar un valor agregado y de alta calidad a los servicios que se ofrezcan a las empresas clientes.

Ante este panorama, se presenta el siguiente Diagrama de Causa y Efecto (Ishikawa), el cual muestra las eventuales causas del problema. El Anexo 1, contiene una breve descripción de algunos primeros hallazgos.

**Ilustración 1**

*Diagrama de Causa y Efecto*



## 1.3. Identificación del Problema

Ya que existe una idea general del problema a resolver, según párrafos anteriores y la imagen expuesta en marras, se plantea la siguiente suposición o hipótesis:

Si se reestructura el proceso de monitoreo de TI siguiendo la metodología Lean Six Sigma, de acuerdo con los estándares y lineamientos Cobit 2019; se optimizará la gestión de incidencias y, en consecuencia, aumentará la excelencia operativa de la firma Gosys Pro en vista de que se acortarán los tiempos de respuesta, se reducirán costos y aumentará la calidad de la resolución de dichas incidencias.

## 1.4. Objetivos

Seguidamente, se presenta los objetivos de este proyecto, cuyas metas pretenden resolver el problema descrito en el párrafo anterior.

### 2.1.1. Objetivo General:

Rediseñar el proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma.

2.1.2. Objetivos Específicos:

1. Diagnosticar el estado del proceso de monitoreo de infraestructura de TI para el establecimiento de la situación actual con respecto a las mejores prácticas de Cobit 2019.

2. Identificar la situación deseada del proceso de Monitoreo de Infraestructura Tecnológica para establecer de las brechas.

3. Rediseñar el proceso de Monitoreo de Infraestructura de TI para el cierre de las brechas identificadas, mediante la aplicación del ciclo DMAIC.

4. Transferir el conocimiento del nuevo proceso de infraestructura para que el departamento de informática adopte de forma adecuada la nueva metodología.

5. Esbozar las recomendaciones para el siguiente ciclo de aplicación DMAIC, mediante la inducción de las herramientas desarrolladas para el nuevo proceso.

## 1.5. Alcances y Limitaciones

El alcance máximo de este proyecto consiste en realizar una revisión profunda al actual proceso de monitoreo de TI y proponer un rediseño mediante la aplicación de algunas herramientas

del ciclo DMAIC bajo el marco Lean Six Sigma. Las mejoras deben estar alineadas con el marco de sanas prácticas Cobit 2019.

Con respecto a las limitaciones; se menciona las siguientes:

1. la poca cantidad de información concerniente al proceso de monitoreo de infraestructura de TI existente en Gosys Pro. Esto debido a que, en la actualidad, los procesos de NOC en producción carecen de la suficiente documentación por parte de la empresa. No existe suficiente documentación.

2. El proyecto se enfocará solamente en la evaluación del proceso de Monitoreo de Infraestructura de TI. No contemplará otros servicios u elementos de la organización.

3. La decisión de aceptar e implementar los ajustes propuestos es tomada directamente por las autoridades de la compañía Gosys Pro.

4. Dentro del proceso de Monitoreo de TI ofrecido por Gosys Pro; existen algunos elementos que deben ser coordinados entre la empresa y sus clientes con el fin de que se aplique las mejoras sugeridas.

## 1.6. Interesados y Beneficiados (STAKEHOLDERS)

- Dirección del proyecto y propietario de la firma Gosys Pro.
- Oscar Corrales Carmona, estudiante de la carrera de Ingeniería Informática.
- Clientes activos y potenciales que requieran de los servicios de Gosys Pro
- Facultad de Ingeniería Informática de la Universidad Hispanoamericana

## 1.7. Metodología por utilizar

La metodología propuesta por Lean Six Sigma permitirá realizar el análisis de la situación actual, así como proponer el nuevo diseño del proceso de Monitoreo de infraestructura de TI, mediante la aplicación las herramientas del ciclo DMAIC.

El marco de sanas prácticas Cobit 2019, proporciona los parámetros necesarios para lograr la estandarización del nuevo proceso de Monitoreo de Infraestructura de TI.

## 1.8. Cronograma de Actividades

A continuación, se presenta diagrama de Gantt el cual presenta en orden cronológico todas las actividades realizadas desde el día que iniciaron las tutorías hasta la fecha en que se entrega el presente documento.

**Tabla 1**

*Diagrama de Gantt*

| AÑO | | 2023 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2024 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| MES | | JUN | | | | | JUL | | | | AGO | | | | | SET | | | | OCT | | | | NOV | | | | | DIC | | | | ENE | | | | FEB | | |
| FECHA | | 1 | 8 | 15 | 22 | 29 | 6 | 13 | 20 | 27 | 3 | 10 | 17 | 24 | 31 | 7 | 14 | 21 | 28 | 5 | 12 | 19 | 26 | 2 | 9 | 16 | 23 | 30 | 7 | 14 | 21 | 28 | 4 | 11 | 18 | 25 | 1 | 8 | 15 |
| SEMANA | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 |
| CAP | ACTIVIDAD | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Corregimiento de ante proyecto | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Establecimiento de nuevos objetivos | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Investigación bibliográfica | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Marco Teórico | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Confección de Marco Metodológico | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Entrevista a CEO de Gosys Pro | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Observación en sitio | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de SIPOC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Diagrama de flujo de alto nivel | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Revisión de bitácoras | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección Análisis estadístico | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Mapa de Flujo de Valor | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Resumen del diagnóstico | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Confección de SIPOC situación deseada | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección Diagrama de Flujo | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Diagrama de flujo por carriles | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Mapa de cadena de Valor | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Matriz RACI | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de SOP's | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Recomendaciones para el patrocinador | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Confección de Conclusiones y recomendaciones | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

# Capítulo II: MARCO TEÓRICO

En este capítulo, se definen algunos conceptos, así como la explicación de la metodología que se utilizará para desarrollar la investigación. Los conceptos descritos en este apartado permitirán visualizar con más claridad el problema. Serán de gran ayuda para la correcta identificación de causas y revelar la mejor forma de atacarlas. Estos conceptos serán la guía para solucionar la causa raíz, lo cual finalmente permitirá cumplir los objetivos del trabajo de investigación.

## 2.2. Monitoreo de Infraestructura de TI

El primer concepto que se debe tener claro es el significado del término Monitoreo de Infraestructura de TI, aplicado a este trabajo de investigación. Por lo que se explica en seguida:

Buenning, Makenzie (2023), define el concepto de Monitoreo de Infraestructura de TI de la siguiente manera:

“El monitoreo de la infraestructura es un proceso utilizado por las empresas que les permite recopilar y analizar datos sobre los componentes de la infraestructura que afectan el rendimiento de los sistemas de TI. Una infraestructura de TI consta de servidores, redes y otros elementos que se ejecutan en segundo plano y en los que confían las personas. Los datos, recopilados a través del software de monitoreo

de la infraestructura, permiten que las organizaciones de TI vean e identifiquen fácilmente las áreas potencialmente problemáticas para que los sistemas y las aplicaciones funcionen por completo."[1]

Cabe resaltar que el monitoreo es un proceso que se ejecuta en tiempo real. Por lo que los datos recopilados se obtienen en tiempo real. Cuando surge un problema, el mismo queda documentado. La repetición de dicho problema documentado se convierte en un incidente. Más adelante se describirá la diferencia entre problema e incidente.

La información obtenida por el proceso de Monitoreo permitirá realizar las siguientes funciones:

- Detectar debilidades en la infraestructura y servicios te TI.
- Predecir posibles fallos de acuerdo con la salud de los sistemas.
- Generar conocimiento sobre cómo solventar de forma integral los incidentes ocurridos.
- Facilitar la continuidad del servicio en caso de la ocurrencia de eventos que afecten la funcionalidad de los sistemas.

El proceso de monitoreo de TI requiere de la existencia de un Centro de Monitoreo. El mismo comprende a su vez servicios de Monitoreo de Operaciones de redes (NOC), así como el servicio de Monitoreo de Seguridad (SOC). Para efectos de esta investigación, el enfoque estará sobre el primero.

---

[1] Buenning, Makenzie. *Monitoreo de la infraestructura: definición y buenas prácticas. 2023*. https://www.ninjaone.com/es/blog/infraestructura-supervision-definicion-buenas-practicas/

El monitoreo de Infraestructura de TI es el proceso objeto de análisis durante el desarrollo de todo este trabajo.

## 2.3. Centro de Operaciones en Monitoreo (NOC)

De acuerdo con una conversación sostenida con el señor Salas, Ronaldo (2023). Se extrae el siguiente concepto acerca del Centro de Operaciones en Monitoreo:

> El centro de Monitoreo de Infraestructura de TI es el departamento destinado a gestionar la operativa de Monitoreo. Su función es desarrollar las labores de recopilación de datos, documentación y gestionar el conocimiento sobre los problemas e incidentes ocurridos.

Está compuesto por los siguientes elementos:

- Uno o varias herramientas de monitoreo de los servicios de TI. Dichas herramientas recopilan y documentan automáticamente y en tiempo real el estado de salud de los sistemas y redes.
- Operadores de Monitoreo son las personas que utilizan dichas herramientas para documentar los eventos y alertar al personal de las áreas competentes para solventar las incidencias ocurridas.
- Hardware, servidores, switches y demás maquinaria que tenga instalados los sistemas de Monitoreo. Pueden ser locales o estar alojados en la nube.
- Un protocolo que contiene las instrucciones y procedimientos para tratar las incidencias ocurridas.
- Un repositorio o bitácora que almacena la información de todas las alertas ocurridas.

Entre las funciones de un Centro de Monitoreo, Se puede citar las siguientes:

- Monitorear la red, los servidores y las aplicaciones para la salud y el rendimiento
- Analizar el ancho de banda e identificar proactivamente los cuellos de botella

- Monitorear y analizar continuamente las amenazas y los ataques a la seguridad
- Modificar las configuraciones de la red según las necesidades de la empresa
- Detectar y soluciona rápidamente los fallos para reducir el tiempo medio de reparación.[2]

Pese a que el trabajo de Investigación está centrado únicamente en el proceso de Monitoreo de TI. Es de suma importancia tener en cuenta los elementos descritos en líneas anteriores. Esto por cuanto se debe analizar cada uno de ellos como posibles causas del problema a resolver.

## 2.4. Antecedentes

- Proyecto: MEJORA DE LA EXCELENCIA OPERACIONAL DE LA PLANTA DE INYECCION EN LA EMPRESA MEXICHEM(AMANCO) EN EL AÑO 2017. Por Cristopher Hernández Molina

Este proyecto de investigación tuvo como principal objetivo mejorar la excelencia operacional de la planta de inyección en la empresa Mexichem Amanco, esto a través del análisis de los elementos que conforman el indicador global “OEE” para lograr el cumplimiento adecuado de los objetivos productivos de la compañía. Los resultados obtenidos, obligaron a desarrollar la

---

[2] Salas, Ronaldo. *Entrevista verbal*. 2023.

metodología DMAIC y todo un plan de implementación conformado por herramientas de ingeniería, las cuales logran la sostenibilidad y mejora continua.

Este trabajo funciona como guía ya que se desarrolla la aplicación de la metodología DMAIC propuesta por 6 Sigma.

## 2.5. Lean 6 Sigma

La metodología Lean Six Sigma es la luz principal para el desarrollo de toda esta investigación. Desde el momento en que se plantea los objetivos hasta que se solucione el problema. Cada paso se desarrolla con las herramientas de esta metodología.

### 2.5.1. Definición

A continuación, se presenta una pequeña definición y explicación de la metodología 6 Sigma de acuerdo con Gutiérrez Pulido, Humberto (2014):

> "Seis Sigma (6s) es una estrategia de mejora continua del negocio que tiene diferentes significados para diferentes grupos dentro de una organización (Harry et al., 2010). Considerando

toda la empresa, es una iniciativa estratégica que busca alcanzar una mejora significativa en el crecimiento del negocio, en su capacidad y en la satisfacción de los clientes.” [3]

Características:

- Cliente céntrico.
- Enfocado en el producto y proceso.
- Guiados por datos y basados en la información.
- Lleva un desplazamiento de mejora estructurada.
- Se enfatiza en la validación mediante importantes resultados de negocio.

Objetivos:

- Mejoramiento en la satisfacción del cliente.
- Eliminación de defectos.
- Mejoramiento de la producción.
- Reducción de variaciones.
- Fortalecimiento del balance final.

Beneficios:

- Prevención del desperdicio.
- Reducción de defectos.

---

[3] Gutiérrez Pulido, Humberto. Calidad Total y Productividad. Cuarta Edición. Editorial Mc Graw Hill. 2014. Página 296

- Disminución de tiempos.
- Ahorro en costos.
- Mejoramiento en la cuota de mercado

### 2.5.2. Ciclo DMAIC

La metodología 6 sigma está basada en el ciclo DMAIC, cuyas fases se describen a continuación:

- Definir: Es la fase inicial de la metodología Lean Six Sigma, donde se define el problema, los objetivos, equipo y procesos más importantes del proyecto.
- Medir: En esta fase se recoge la información sobre las posibles causas que afectan el proceso y afectan su desempeño, así como la determinación de las capacidades y la sigma actual del proceso.
- Analizar: Se analiza la causa raíz que afecta el desempeño actual del proceso y la tasa de errores que le generan, con la finalidad de proponer posteriormente un rediseño del proceso o producto de acuerdo a los resultados de la misma.
- Mejorar: En esta etapa de identifica las posibles características dentro del proceso que se pueden mejorar, se proponen soluciones para mitigar o eliminar las causas que originan problemas en los procesos y así lograr cumplir con las expectativas y necesidades del cliente.

- Controlar: Se elabora un plan de control del nuevo proceso con la finalidad de mantener el sigma logrado.

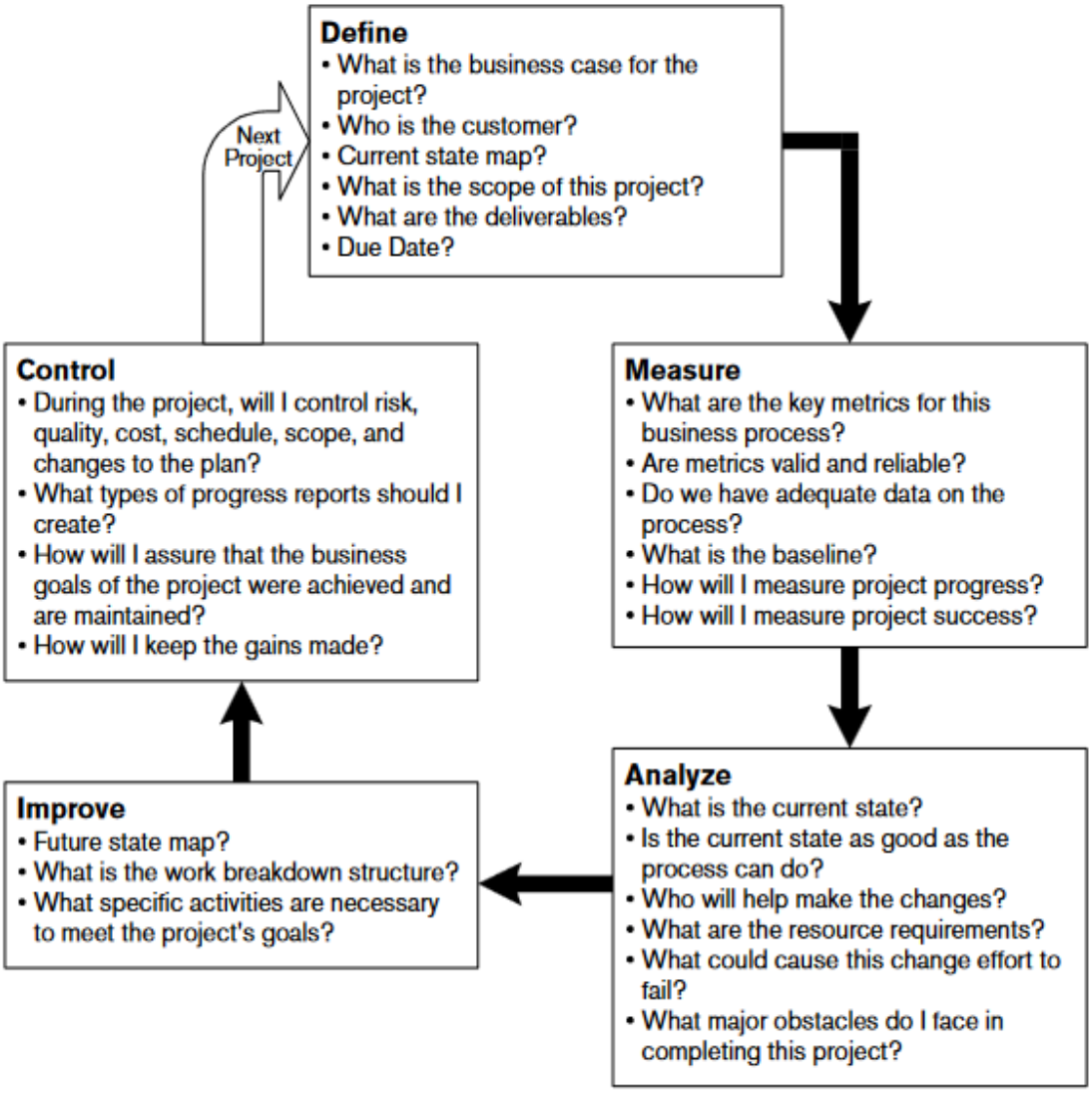
La metodología DMAIC es la parte más importante dentro de este proyecto. Será la que revelará de una forma clara y elocuente cómo los problemas generan afectación al proceso de Monitoreo de TI. Desnudará las raíces del problema, demostrará de una forma cualitativa y cuantitativa las consecuencias del problema.

Por ser DMAIC una metodología cíclica, garantiza una constante revisión de las causas y consecuencias de los problemas. Lo cual permitirá plantear soluciones radicales a los mismos.

Seguidamente, se adjunta un gráfico que ilustra muy claramente cómo funciona la metodología DMAIC. Dicha ilustración plantea algunas preguntas que son una muy buena guía en cada etapa del ciclo:

**Ilustración 2**

*Ciclo DMAIC*




Fuente: Pyzdek, Tomas. *SIGMA PROJECT PLANNER*. Pag XVI

### 2.5.3. Marco del Proyecto

Profundizando en el ciclo DMAIC, se plantea el primer paso el cual consiste en la definición del proyecto. El siguiente cuadro muestra el Marco del Proyecto, primera herramienta que permite plantear y observar el problema:

**Tabla 2**

*Marco del Proyecto*

| | |
|---|---|
| **Título / Propósito** | Rediseño del proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma. |
| **Patrocinador** | Gosys Pro |
| **Sustentante** | Oscar Alonso Corrales Carmona |
| **Necesidades a ser atendidas** | No existe una estandarización de los procesos de Monitoreo de Infraestructura de TI.<br>Posibles pérdidas consecuenciales por eventuales interrupciones en la continuidad de los servicios informáticos. |
| **Declaración del problema** | El proceso de monitoreo de servicios de TI se realiza de manera inmadura y empírica. No existe documentación ni manuales estandarizados sobre la gestión de alertas por eventos e incidencias.<br>No existen métricas estandarizadas que sirvan para calcular la afectación de los servicios. |
| **Objetivo** | Rediseñar el proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma. |
| **Alcance** | El alcance del proyecto consiste en realizar un análisis de los procesos actuales de monitoreo de TI bajo el marco Lean Six Sigma, así como proponer las mejoras correspondientes según Cobit 2019 |
| **Roles y responsabilidades** | Patrocinador: Ronaldo Salas Apú. Propietario de la firma Gosys Pro.<br>Líder del Proyecto: Oscar Corrales Carmona. |
| **Recursos** | Sistemas de monitoreo |

| | |
|---|---|
| **Métricas** | Relación costo – velocidad – calidad |
| **Fecha de inicio** | 01 de Junio de 2023 (30 semanas) |
| **Entregables del proyecto** | 1. Diagnóstico de Situación Actual<br>2. Planteamiento de situación deseada<br>3. Propuesta de rediseño de proceso de Monitoreo para cierre de brechas.<br>4. Transferencia de conocimiento para adopción de la nueva metodología.<br>5. Planteamiento las recomendaciones para el siguiente ciclo DMAIC. |
| Fecha Final | 18 de febrero de 2024 |

### 2.5.4. ¿Es válido este proyecto?

De acuerdo con el diagrama de Causa Y efecto (Ishikawa). El proyecto sí es viable ya que no se deben realizar grandes esfuerzos para lograr la estandarización. Básicamente porque el sistema de Monitoreo de Infraestructura de TI puede realizarse en un ámbito pequeño, con pocos sistemas, equipos y personal. El acto de solventar las alertas e incidencias es competencia de Gosys Pro, sino por parte de las empresas clientes. La firma patrocinadora de este proyecto, solamente se encarga de mantener activo el sistema de monitoreo, registrar, documentar, clasificar, dar seguimiento y documentar las alertas según la incidencia presentada.

## 2.6. Diagrama de Causa y Efecto (Ishikawa)

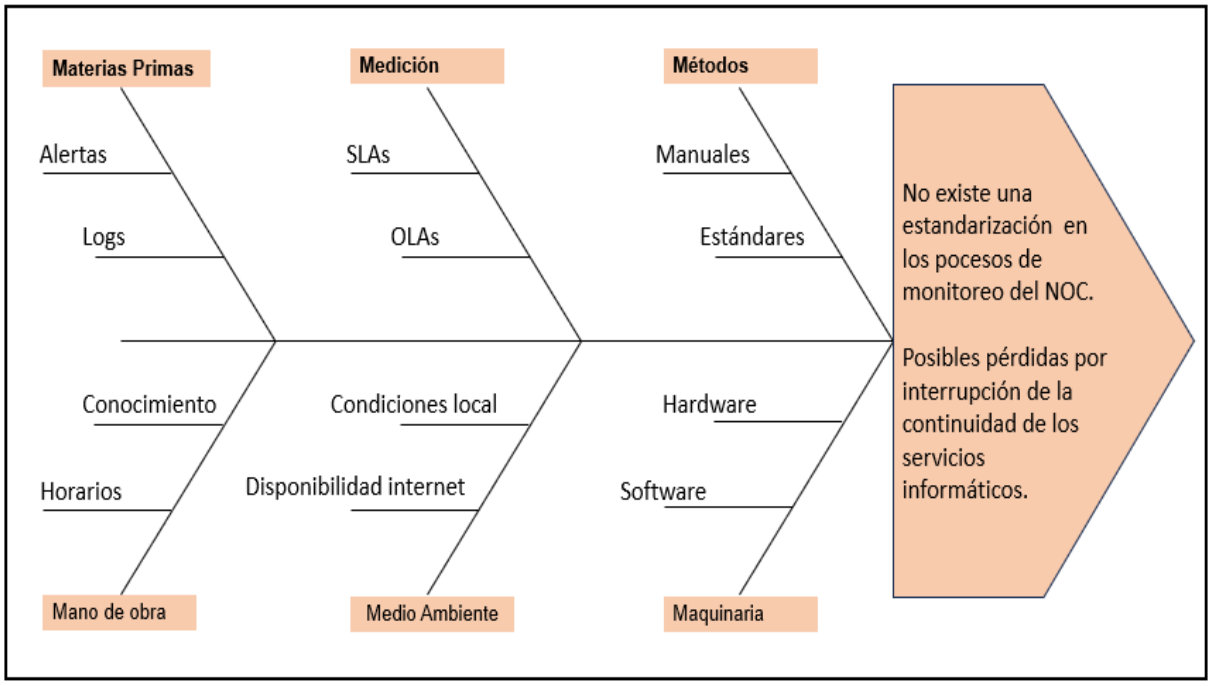
De acuerdo con Gutiérrez Pulido, (2010) en su libro Calidad Total y Productividad, se adjunta la siguiente explicación del diagrama de Causa y Efecto:

"Es un método gráfico mediante el cual se representa y analiza la relación entre un efecto (problema) y sus posibles causas." [4]

El Diagrama de Ishikawa es utilizado para relacionar el efecto (problema) con sus causas potenciales, por medio del pensamiento creativo (lluvia de ideas) representadas en una gráfica para lograr una mejor comunicación en las discusiones y el análisis.

**Ilustración 3**

*Diagrama de Ishikawa*




[4] Gutiérrez Pulido, Humberto. Calidad Total y Productividad. Tercera Edición. Editorial Mc Graw Hill. Pag 192

Esta es la herramienta que permite revisar el estado de los activos y el capital de producción con el fin de identificar las causas del problema.

A continuación, Se describe de forma breve cada una de eventuales las fuentes causantes del problema y cómo están relacionadas con el objeto de estudio de este proyecto:

- Mano de obra o gente: Conocimiento (¿la gente conoce su trabajo?), Entrenamiento (¿están entrenados los operadores?), Habilidad (¿los operadores han demostrado tener habilidad para el trabajo que realizan?), Capacidad (¿se espera que cualquier trabajador pueda llevar a cabo de manera eficiente su labor?)

El personal de Gosys Pro son menos de 10 personas. No obstante, solamente una persona se encarga de administrar la plataforma de Monitoreo. Existen 6 operadores y otras 2 personas que se encargan de labores administrativas ajenas al Core del negocio. El conocimiento se concentra solamente en 7 personas. Al ser un servicio tercerizado; los operadores de la empresa contratante son quienes gestionan las incidencias a lo interno gracias al servicio prestado por Gosys Pro.

- Métodos: Estandarización (¿las responsabilidades y los procedimientos de trabajo están definidos de manera clara y adecuada?), Excepciones (cuando el procedimiento estándar no se puede llevar a cabo, ¿existe un procedimiento alternativo claramente definido?), Definición de operaciones (¿están definidas todas las operaciones que constituyen los procedimientos? ¿Cómo se valida si la operación fue efectuada de manera correcta?)

- Máquinas o equipo: Capacidad (¿las máquinas han demostrado ser capaces?, ¿Hay diferencias entre estaciones, máquinas, cadenas, estaciones, instalaciones?), Herramientas (¿hay cambios

de herramientas periódicamente? ¿Son adecuados?), Ajustes (¿los criterios para ajustar las máquinas son claros?), Mantenimiento (¿hay programas de mantenimiento preventivo? ¿Son adecuados?).

Los servidores que sostienen las plataformas se encuentran alojados en una nube AWS. También se cuenta con un equipo local para acceder por VPN hacia dichos servidores.

- Mediciones o inspección: Disponibilidad (¿se dispone de las mediciones requeridas?), Definiciones (¿están definidas operacionalmente las características que son medidas?), Tamaño de la muestra (¿se midieron suficientes piezas?), Capacidad de repetición (¿se puede repetir con facilidad la medida?), Sesgo (¿existe algún sesgo en las medidas?).

  Los SLA's (niveles acuerdos de servicio), y OLA's (Nivel de acuerdo operacional), consisten en las métricas convenidas entre el cliente y Gosys Pro. En todo caso, serían los tiempos de resolución de incidencias.

- Medio ambiente: Ciclos (¿existen patrones o ciclos en los procesos que dependen de las condiciones del medio ambiente?), Temperatura (¿la temperatura ambiental influye en las operaciones?), Orden y limpieza (¿existen 33 políticas para mantener el orden y el aseo? ¿Se encuentran las instalaciones ordenadas y limpias?) (Gutiérrez, 2005).

  Al ser Gosys Pro una pyme con tan poco personal, carece en sí de una oficina como tal. Todas las operaciones se realizan desde el domicilio personal del CEO, así como de forma remota por parte de los operadores.

- Materias Primas: Son los insumos que nos servirán para desarrollar el proceso productivo. Las materias primas son el conjunto de alertas generadas por parte del sistema de monitoreo de TI. También las bitácoras, repositorios y demás datos recolectados por parte de los sistemas.

## 2.7. Diagrama de Flujo:

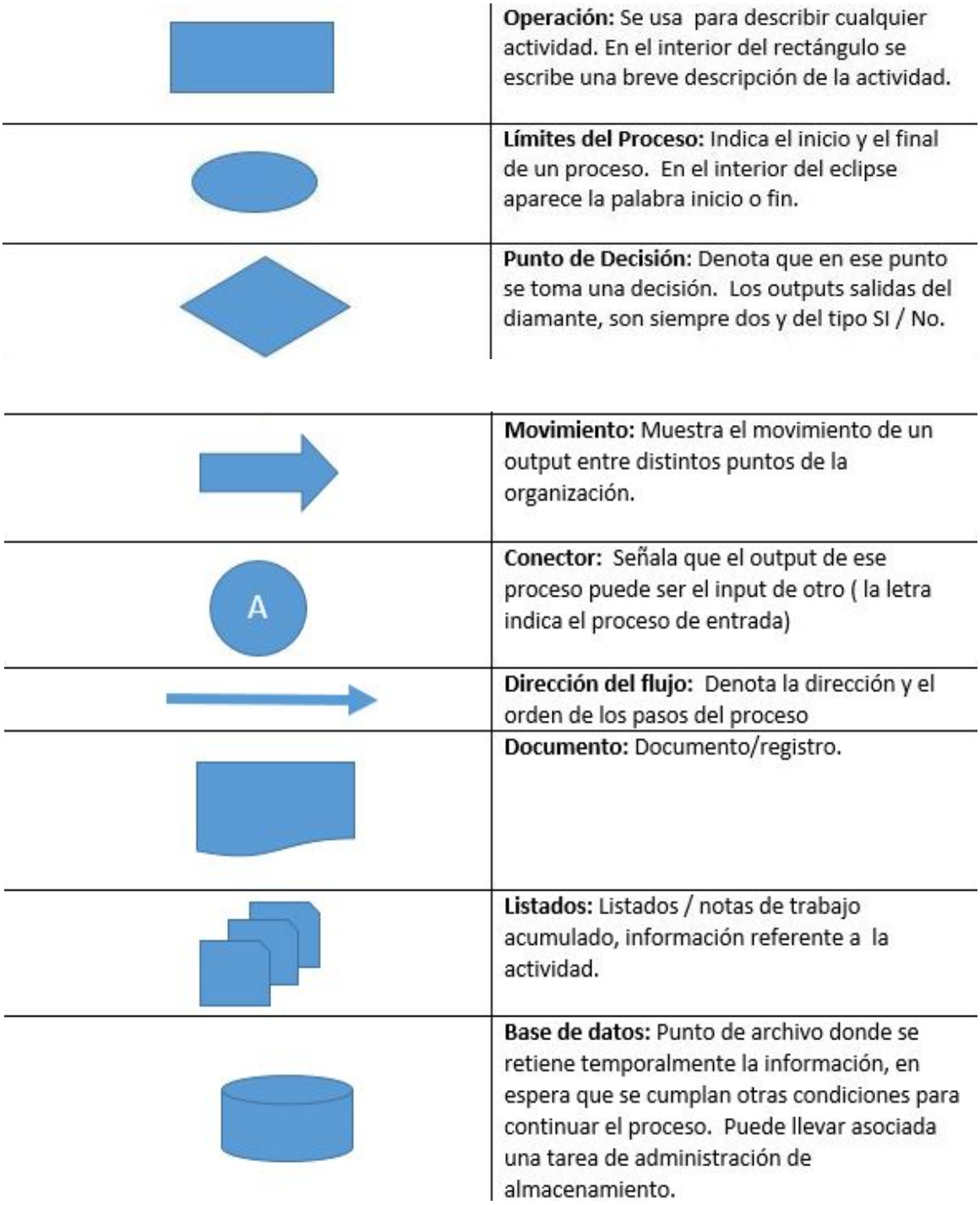
Un diagrama de flujos es una representación gráfica, resumida y ordenada de un proceso. Se utiliza para describir cada paso, sus entradas y salidas, fronteras, qué se hace en cada etapa, tiene un principio y final, una estructura de toma de decisiones, insumos, productos parciales y un producto final terminado. Dentro de los procesos, existen subprocesos los cuales se deben representar por medio de otros diagramas de flujos.

Para efectos este trabajo de investigación. El Diagrama de Flujos será de gran importancia para explicar cómo se desarrolla actualmente el proceso de Monitoreo de Infraestructura de TI. También permitirá explicar cómo debe ser el proceso de la nueva metodología explicando a profundidad cada operación.

Se adjunta una pequeña explicación de cada una de las figuras más utilizadas en los procesos:

**Ilustración 4**

*Figuras Diagrama de Flujo*



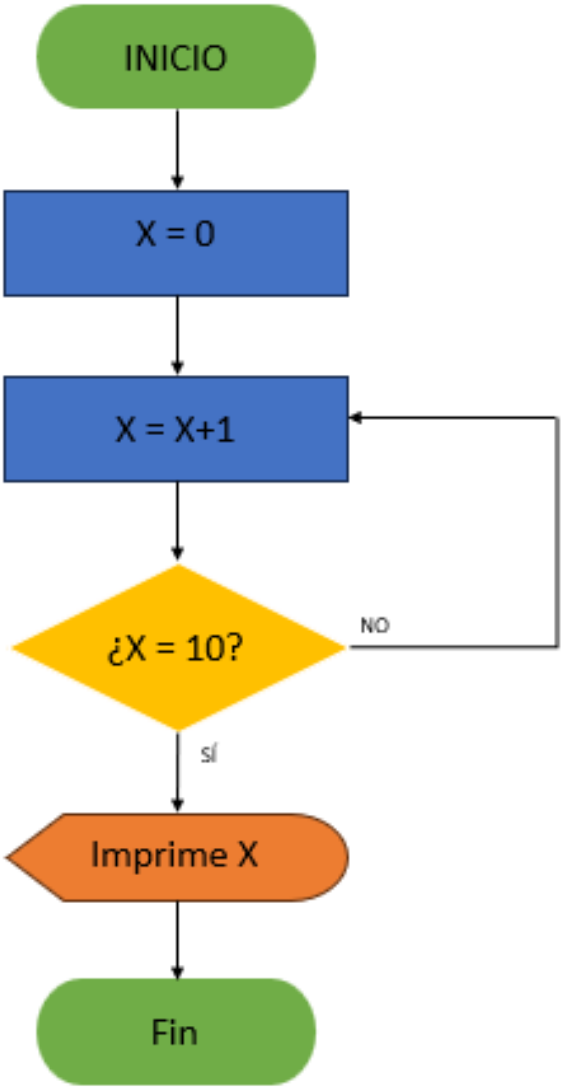

| | |
|---|---|
| | **Operación:** Se usa para describir cualquier actividad. En el interior del rectángulo se escribe una breve descripción de la actividad. |
| | **Límites del Proceso:** Indica el inicio y el final de un proceso. En el interior del eclipse aparece la palabra inicio o fin. |
| | **Punto de Decisión:** Denota que en ese punto se toma una decisión. Los outputs salidas del diamante, son siempre dos y del tipo SI / No. |
| | **Movimiento:** Muestra el movimiento de un output entre distintos puntos de la organización. |
| | **Conector:** Señala que el output de ese proceso puede ser el input de otro ( la letra indica el proceso de entrada) |
| | **Dirección del flujo:** Denota la dirección y el orden de los pasos del proceso |
| | **Documento:** Documento/registro. |
| | **Listados:** Listados / notas de trabajo acumulado, información referente a la actividad. |
| | **Base de datos:** Punto de archivo donde se retiene temporalmente la información, en espera que se cumplan otras condiciones para continuar el proceso. Puede llevar asociada una tarea de administración de almacenamiento. |

Fuente: Torres, Iván. *Diagrama de Flujo, una herramienta infalible para visualizar, esquematizar y mejorar tus procesos.* https://iveconsultores.com/diagrama-de-flujo/

La siguiente imagen representa un pequeño proceso en el que se aumenta el valor de X desde 0 hasta 10, se aumenta en 1 el valor de X. Cuando X llega a 10; finaliza el proceso:

**Ilustración 5**

*Ejemplo de Diagrama de Flujo*



El diagrama de flujo será útil para explicar y comprender cada etapa del proceso de Monitoreo de Infraestructura de TI.

## 2.8. COBIT 5 versión 2019

COBIT por sus siglas en inglés (Control Objectives for Information Systems and related Technology), consiste en los Objetivos de Control para Tecnología de Información y Tecnologías relacionadas.

Cobit es un marco de trabajo para el gobierno y la gestión de la información y la tecnología de la empresa. Define los componentes y los factores de diseño para construir y mantener un sistema de gobierno que se ajuste mejor.

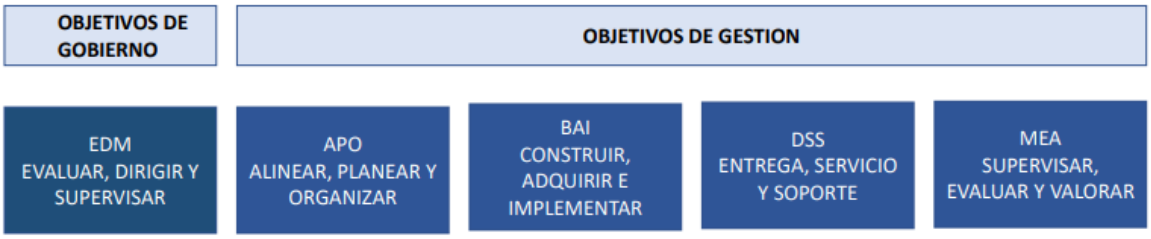
Dicho marco ayuda a mantener una óptima Gobernanza Empresarial de Tecnologías de Información (EGIT) ya que integra eficientemente las mejores prácticas en gobernanza, gestión, soporte, seguridad de la información y gestión de riesgos. A su vez, Proporciona toda una filosofía para la gestión de la seguridad cibernética. Esto por cuanto, reúne las diversas disciplinas de gobierno, riesgo y seguridad. Este proceso lo ayuda a identificar riesgos, priorizarlos y desarrollar planes para abordarlos.

Este framework, está desarrollado por ISACA (Information Systems Audit and Control Association). Una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificación para la realización de actividades de auditoría y control en Tecnologías de Información.

Al igual que en la versión COBIT 5 en COBIT 2019 los objetivos de Gobierno y los objetivos de Gestión están agrupados en cinco Dominios. Los Dominios expresan el propósito de los objetivos que contienen.

**Ilustración 6**

*Dominios Cobit 2019* [5]




Fuente: Ritegno, Eduardo. *COBIT 2019*. Pag 17. https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

Para efectos de aplicación en este trabajo, se debe tener presente los siguientes dominios específicos:

- DSS01: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externos, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

[5] En anexos 8 y 9, se presenta con mayor detalle las actividades de los dominios Cobit 2019.

- DSS02: Gestionar Peticiones e Incidentes de Servicio: Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes. Su propósito es lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.
- DSS03: Gestionar Problemas: Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora. Su objetivo consiste en incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.
- DSS04: Gestionar la Continuidad: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa. Su finalidad es asegurar la continuidad de las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.
- MEA01: Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad: Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada. Con este dominio

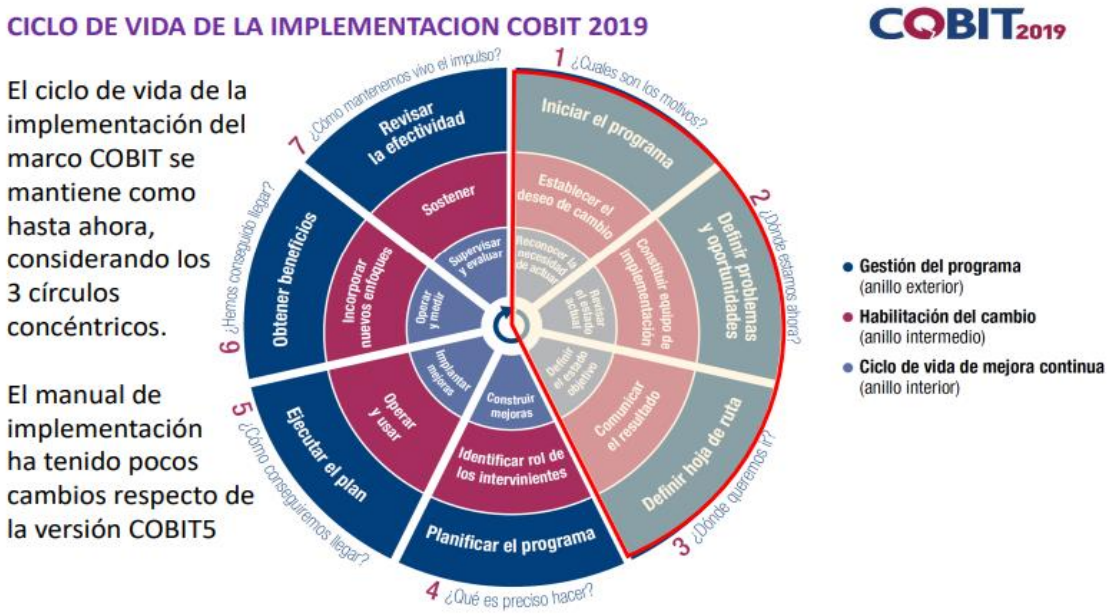
se desea proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.

Todos estos dominios del marco referencial COBIT 2019, atañen directamente a la temática que concierne al proceso de Monitoreo de Infraestructura de TI. Son guía fundamental para el diseño y creación de políticas, normativas y manuales que sirvan para una óptima gestión servicio de Monitoreo de Infraestructuras de TI, ofrecido por la empresa Gosys Pro.

La siguiente gráfica es una guía de implementación del marco referencial Cobit 2019:

**Ilustración 7**

*Ciclo de Vida de Implementación Cobit 2019*




Fuente: Ritegno, Eduardo. *COBIT 2019*. Pag 17. https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

## 2.9. Excelencia Operativa

Antes de presentar la definición y descripción de Excelencia Operativa, es importante poseer al menos una noción básica del modelo de Excelencia Operacional.

Excelencia Operacional:

De acuerdo con PMM Innovation Group, se adjunta la siguiente definición de Excelencia Operacional:

> La Excelencia Operacional se ha definido de muchas maneras. Todas las definiciones tienen en común que la excelencia operacional conduce a una alta calidad y productividad y a la entrega puntual de bienes y servicios competitivos a los clientes (gestión de activos físicos, innovación tecnológica, externalización y competencia global). [6]

El modelo de Excelencia Operacional consta de 5 pilares enfocados en el negocio, la tecnología y la gente. Propone acciones que buscan la excelencia de los procesos, negocios, activos, personas, así como una gestión empresarial verde y sostenible. A continuación, se presenta una imagen que ilustra cada uno de esos 5 ejes mencionados:

---

[6] Amendola, Luigi. *Excelencia Operacional y Mejora Continua. ¿Cómo implementar?* https://www.youtube.com/watch?v=TdMXAcYivmw. Minuto 13:25

**Ilustración 8**

*Ejes del Modelo de Excelencia Operacional*


Fuente: Amendola, Luigi. Excelencia Operacional y Mejora Continua. ¿Cómo implementar? https://www.youtube.com/watch?v=TdMXAcYivmw. Minuto 14:28

La excelencia operacional abarca no solo los procesos de la organización, sino que todos los elementos internos y externos, clientes, proveedores, activos, cultura organizacional, estrategias de negocios, comunicación asertiva entre todas las partes.

El modelo de Excelencia Operacional (incluyendo la Excelencia Operativa), se desarrolla en 7 pasos, los cuales tienen una gran similitud con el modelo DMAIC.

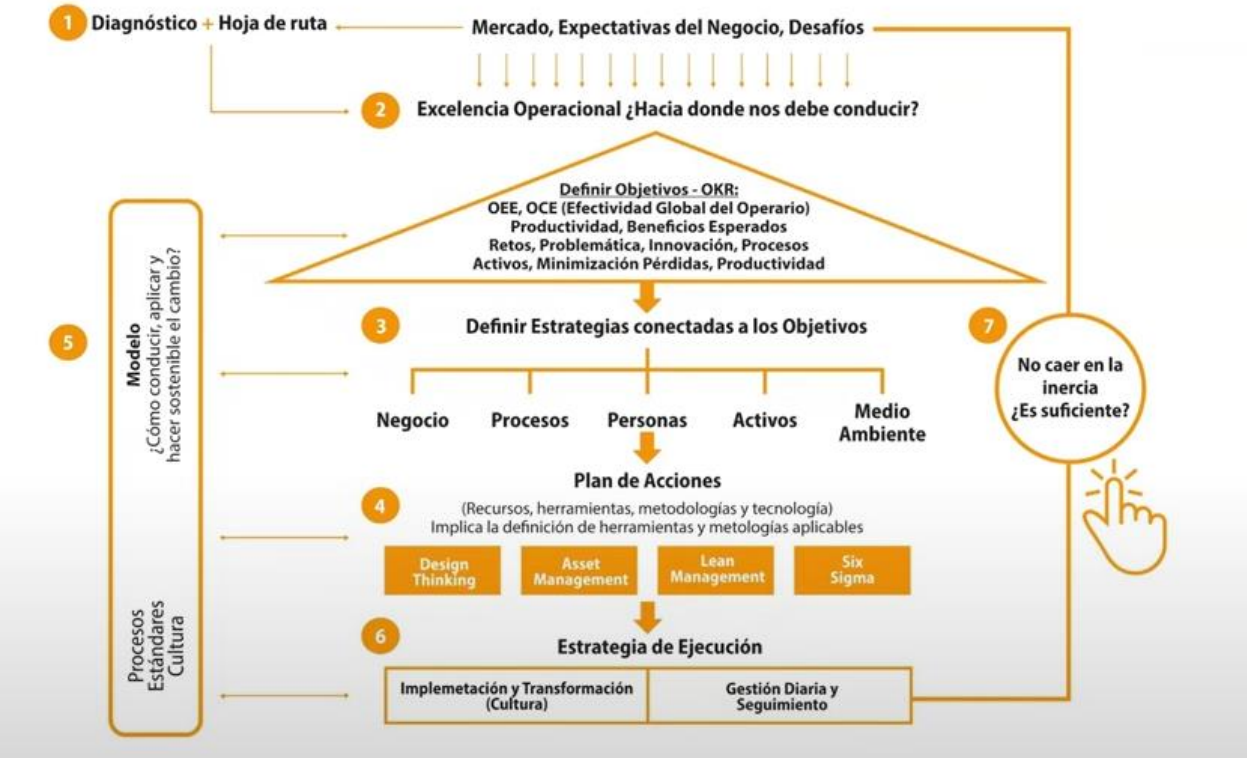
A continuación, una breve descripción de estos:

1. ¿Qué nos falta?: Evaluar qué tan lejos estamos de la excelencia operacional relacionada con las expectativas que el negocio tiene de ésta.
2. ¿Hacia dónde nos debe conducir?: Definición de objetivos claros operativos, tácticos y estratégicos.
3. Definir estrategias conectadas con los objetivos.
4. Desarrollo de los planes: Desarrollo del plan de acciones para desarrollar las estrategias. Asignación de tiempo y recursos. Planificación de seguimiento y control.
5. Construcción del modelo: Guiado a generar un cambio sostenible de cultura de la organización.
6. Estrategia de ejecución: Ejecución de la implementación y transformación cultural. Gestión diaria de seguimiento.
7. No caer en zonas de confort y hacer el proceso de mejora continua.

El siguiente gráfico presenta la secuencia de cómo se debe ejecutar los pasos mencionados anteriormente teniendo en cuenta los 5 ejes de la excelencia operacional:

**Ilustración 9**

*Pasos Para Alcanzar La Excelencia Operacional*




Fuente: Amendola, Luigi. *Excelencia Operacional y Mejora Continua. ¿Cómo implementar?* https://www.youtube.com/watch?v=TdMXAcYivmw. Minuto 24:25

Excelencia Operativa.

Como se expresó en párrafos anteriores; la excelencia operativa es una parte fundamental de la Excelencia Operacional, con la diferencia de que la misma tiene su enfoque a lo interno de la organización. De acuerdo con el Amendola, Luigi (2021)[7], se adjunta la siguiente definición de Excelencia Operativa:

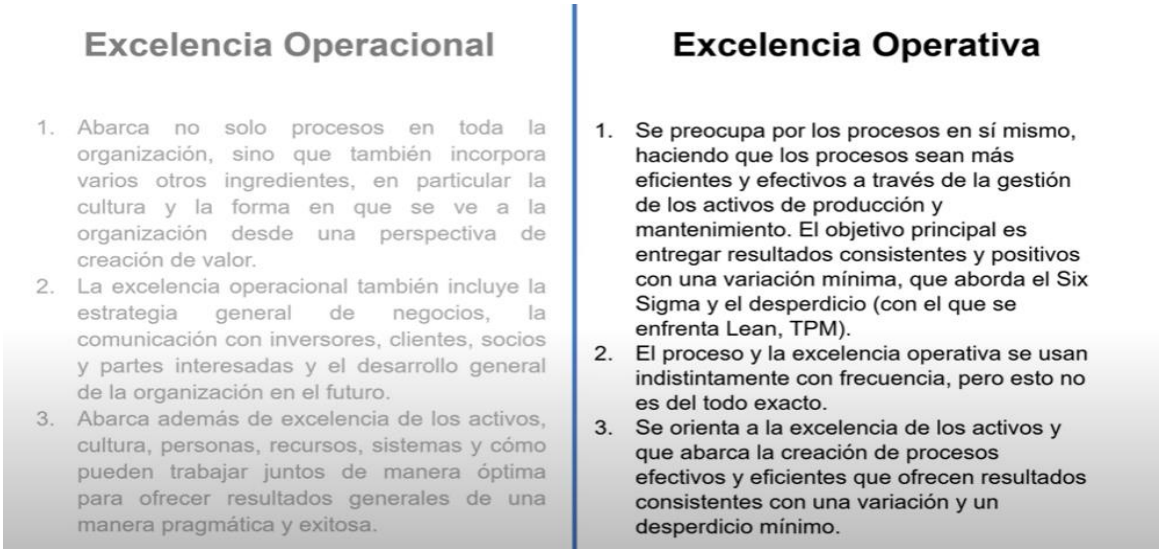
1. Se preocupa por los procesos en sí mismo, haciendo que los procesos sean más eficientes y efectivos a través de la gestión de los activos de producción y mantenimiento. El objetivo principal es entregar resultados consistentes y positivos con una variación mínima, que aborda el Lean Six Sigma y el desperdicio.
2. El proceso y la excelencia operativa se utilizan indistintamente con frecuencia, pero esto no es del todo exacto.
3. Se orienta a la excelencia de los activos y que abarca la creación de procesos efectivos y eficientes que ofrecen resultados consistentes con una variación y un desperdicio mínimo.

Seguidamente, se adjunta un pequeño cuadro comparativo que muestra la diferencia entre los conceptos de Excelencia Operacional y Excelencia Operativa:

[7] Amendola, Luigi. *Excelencia Operacional y Mejora Continua. ¿Cómo implementar?* https://www.youtube.com/watch?v=TdMXAcYivmw.

**Ilustración 10**

*Diferencia entre Excelencia Operacional y Excelencia Operativa*




Fuente: Amendola, Luigi. *Excelencia Operacional y Mejora Continua. ¿Cómo implementar?* https://www.youtube.com/watch?v=TdMXAcYivmw. Minuto 18:26

# Capítulo III: MARCO METODOLÓGICO

## 3.1. Tipo y enfoque de la Investigación

### 3.1.1. Tipo de Investigación

Éste trabajo posee un híbrido entre investigación de campo y aplicación de acuerdo con los objetivos del Trabajo Final de Graduación.

En primera instancia, se debe realizar consulta en diversas fuentes bibliográficas tales como libros, vídeos, páginas de internet, fuentes primarias y secundarias. Esto con el fin de obtener el conocimiento y la guía de cómo se debe realizar este trabajo. Con el propósito de aprender algunas técnicas de estudio y aplicación, comprensión de las metodologías de investigación, herramientas para recabar, procesar analizar y comprender la información. Este es un proceso investigativo.

Seguidamente, se debe ejecutar el proceso de recolección de datos, realizar observación de campo en las oficinas de Gosys Pro. Se debe realizar visitas, conversar con el personal, conocer cómo se realiza el proceso general de monitoreo, entradas, salidas y tareas. Conocer los sistemas y equipos utilizados. También se debe realizar medición de tiempos, SLA’s y OLAs, KPI. Todo esto con herramientas que se describirán más adelante. Este también es un proceso investigativo.

El propósito final de este trabajo consiste en que la firma Gosys Pro pueda aplicar mejoras a sus procesos. Esto por cuanto, existe la pretensión de establecer mejoras a los procesos de monitoreo en Infraestructura de TI. A luz del marco referencial Cobit 2019, se planteará la sugerencia de las acciones a realizar por parte del patrocinador. Consiste en aplicación como tal.

Aunado a lo anterior, el último objetivo de esta investigación será de gran ayuda para iniciar un nuevo ciclo DMAIC, el cual podrá medir el efecto de las mejoras planteadas en éste o bien descubrir nuevas brechas. Consiste en aplicación como tal.

### 3.1.2. Enfoque Explicativo:

El enfoque de esta tesis es altamente explicativo. No se omite recordar que un enfoque explicativo lleva implícito un enfoque descriptivo.

Si bien es cierto que se debe realizar una descripción general de los problemas que afectan al proceso de monitoreo de TI, tanto internos como externos según diagramas de causa y efecto; el propósito de este trabajo radica en tratar de explicar cómo deben realizarse los procesos de monitoreo y observabilidad según Cobit 2019. En adición a lo anterior; se pretende que el lector pueda comprender la diferencia entre la situación actual y la situación deseada por medio de la visualización de las brechas encontradas.

En vista de que se está trabajando bajo la metodología DMAIC, propiciada por Lean Six Sigma; las evidencias, conclusiones y recomendaciones serán la primera piedra para construir un nuevo ciclo de trabajo de investigación con la finalidad de generar un proceso de mejora continua y llegar a una excelencia operativa.

### 3.1.3. Ruta cualitativa

Hernández Sampieri, Roberto (2018), indica lo siguiente con respecto a la Ruta Cualitativa de la Investigación:

Ruta cualitativa: Definimos un rumbo (planteamiento del problema), pero no es el camino en línea recta. Actúa como la actualización de tráfico y navegación Waze u otros sistemas similares (va reposicionando o recalculando la mejor ruta de cuerdo a las circunstancias para arribar al lugar

que deseamos). Nuestro equipaje incluye análisis temático e interpretación de significados pues lidiaremos con narrativas.[8]

Al desconocer cómo la compañía Gosys Pro ejecuta el proceso de monitoreo de TI, sus pasos, variables, características, elementos. Ser debe comenzar por explorar el campo, ir capturando datos, tomar apuntes, observar, preguntar. En fin; ir aprendiendo, y a la vez analizando la información para finalmente tener una noción de dicho proceso. Esto justifica por qué la ruta debe ser cualitativa.

Sumado a lo anterior, la ruta cualitativa permitirá obtener una mayor flexibilidad en cuanto al proceso de indagación y tratamiento de la información ya que existe un sometimiento a la rigurosidad del método científico tal como se realiza por ruta cuantitativa.

[8] Hernández Sampieri, Roberto. 2018. *Metodología de la Investigación*. México. Editorial McGraw Hill. P.10

## 3.2. Fuentes y sujetos de información

### 3.2.1. Fuentes primarias

Ulate y Vargas (2012) menciona que "las primarias son aquellas fuentes que propician datos de primera mano, es decir, información obtenida directamente quien la produjo, el autor original." (pág. 44) [9]

De acuerdo con lo mencionado anteriormente, se identifica dos fuentes primarias a saber:

a. Registros, bitácoras, reportes y demás datos arrojados por los sistemas de Monitoreo de TI.
b. El personal de Gosys Pro que puedan suministrar información importante para dar sustento al desarrollo de este proyecto.

### 3.2.2. Fuentes Secundarias

De acuerdo con Ulate y Vargas (2012), "las fuentes secundarias son resúmenes de fuentes primarias, compilaciones, comentarios de artículos, de libros o tesis. También pueden ser libros que desarrollan un tema a partir de su propia recopilación de información." [10]

Para efectos de esta tesis, se considerará como fuentes secundarias todos los trabajos, tesis, literaturas, libros, vídeos y demás información que sea útil para dar soporte y sustento al desarrollo de este trabajo. Las mismas se citan en el apartado de Bibliografía.

---

[9] Ulate, I. y Vargas, E. (2012). *Metodología para elaborar una tesis como trabajo final de graduación.* (1ª. Ed.). Costa Rica San José, Editorial Universidad Estatal a Distancia. P.44

[10] Ibid., p.44

### 3.2.3. Sujetos de información

Los sujetos que estarán cubiertos por esta investigación serán el CEO de la firma Gosys Pro, así como el personal involucrado en el proceso de Monitoreo de TI.

A continuación, se presenta una pequeña una tabla que permite definir los sujetos de información:

**Tabla 3**

*Sujetos de Información*

| **PUESTO LABORAL** | **PROFESIÓN** | **EXPERIENCIA** | **RELACIÓN CON EL TEMA** |
|---|---|---|---|
| CEO de Gosys Pro | Ingeniero en Informática | Más de 14 años | Fundador de la empresa, experto en Monitoreo y Observabilidad de TI. |
| Personal de GosysPro | Operadores de Monitoreo | 5 años | Quienes realizan a diario el proceso de Monitoreo de TI. |

## 3.3. Técnicas y herramientas de recolección de datos

Tal como lo menciona Hernández Sampieri, Roberto (2018)., "Recolección de datos cualitativos es el acopio de datos narrativos en los ambientes naturales y cotidianos de los participantes o unidades de muestreo." (Pag 443).[11]

[11] Hernández Sampieri, Roberto. 2018. *Metodología de la Investigación*. México. Editorial McGraw Hill. P.443

Todos los días se recolectan datos de forma consciente e inconsciente. Los mismos se miden y analizan utilizando múltiples técnicas y herramientas. Ese proceso de captura de información puede realizarse de forma empírica o bien bajo métodos científicos y más sofisticados.

Con respecto a los instrumentos de recolección de datos. Hernández Sampieri, Roberto (2018), menciona lo siguiente: "Instrumento de recolección de datos cualitativos es el investigador auxiliándose de diversas herramientas como las entrevistas, observación y sesiones grupales." (Pag 443).[12]

Por lo tanto, emplear herramientas tales como cuestionarios, encuestas, entrevistas, observación, gráficos, medición de KPI's, SLA's y OLA's, variables, medición de procesos, diagrama de flujos son ejemplos de algunos métodos de captura de información.

Los autores Rowlands, David; George, Michael L; Price, Mark; Maxey, John (2005) presentan en el libro "Lean Six Sigma Pocket Tookbook" una nutrida serie de herramientas que serán de gran utilidad para capturar, interpretar, analizar y presentar la información requerida para el desarrollo de este trabajo. También son una guía para en el proceso general de diagnóstico, presentación de situación deseada, proposición de mejoras y los controles para sostenerlas en el tiempo.

Se ha elegido utilizar las siguientes herramientas para capturar la información requerida:

[12] Ibid., p.443

### 3.3.1. Entrevista con cuestionario y conversaciones con el CEO de Gosys Pro

Se debe efectuar una entrevista al CEO de la firma Gosys Pro. Dicha entrevista consistirá en una explicación profunda y paso a paso de cómo se desarrolla el proceso de monitoreo y observabilidad. Esto brindará un panorama general de dicho proceso y permitirá conocer los tipos de alertas y eventos que ocurren y se documentan.

Dentro del proceso de entrevista, se aplicará un cuestionario que contiene algunas preguntas útiles para crear la matriz de datos que permitirá realizar el análisis estadístico.

### 3.3.2. Observación en sitio

El proceso de observación en sitio consistirá en un simulacro de una capacitación a un nuevo colaborador de la unidad de monitoreo de TI. De forma que el patrocinador explique paso a paso cómo se efectuara el proceso de monitoreo, indique los tipos de entradas, qué tipos de eventos se generan, clasificación de alertas e incidencias, el proceso general de gestión de cada una de ellas.

Por medio de la observación en sitio, se obtendrá el conocimiento, las variables y demás elementos que serán útiles para ir trabajando en las mediciones y análisis.

Este proceso de observación en sitio proporcionará la información requerida para completar el análisis SIPOC y Mapa de flujo de valor de alto nivel.

### 3.3.3. Confección de Diagrama de Flujo

La información recabada durante los dos procesos anteriores servirá para confeccionar un diagrama de flujos que permita visualizar de una forma esquemática y ordenada cada uno de los pasos del proceso de monitoreo de TI.

Salas, Ronaldo (2023), indica que en general el proceso de monitoreo y observabilidad es el mismo para todas las alertas. Lo que variará son algunos valores, medidas, parámetros, canalizaciones.

### 3.3.4. Revisión de bitácoras y logs

Cada una de las alertas y eventos generados en el proceso de monitoreo debe ser debidamente documentado, lo cual arrojará datos tales como hora de inicio, hora final, fechas, duración, severidad de la incidencia, causas, consecuencias, personal involucrado en solventar la incidencia, cantidad de veces que se repite la incidencia, franja horaria en que ocurren y otros datos.

Se solicitará al patrocinador una lista de bitácoras, las cuales servirán para efectuar los procesos de medición. Esta muestra será lo suficientemente amplia como para obtener diversidad de resultados. Comprenden un rango cronológico de 4 meses, entre junio y septiembre del año 2023.

De ser necesario, se ampliará la muestra y en proporciones iguales los rangos y filtros mencionados en el párrafo anterior.

Con estos datos, se construirá el Mapa de Cadena de Valor. De este proceso, se obtendrán algunas variables útiles para detectar las brechas y compararlas con los estándares de Cobit 2019. Los datos obtenidos deben ser los insumos para la aplicación de procesos estadísticos que generen gráficas con el fin de obtener patrones, tendencias, comportamientos. Se llegará al proceso de análisis con el fin de plantear las mejoras correspondientes.

De esta medición se pretende obtener como resultado la relación Calidad – Velocidad – costo.

## 3.4. Variables de investigación

La Matriz que se presenta a continuación contiene una correlación entre los objetivos, variables, herramientas a utilizar y entregables de cada objetivo.

**Tabla 4**

*Variables de Investigación*

| OBJETIVO | VARIABLES ASOCIADAS | HERRAMIENTAS | ENTREGABLES |
|---|---|---|---|
| Diagnosticar el estado del proceso de monitoreo de infraestructura de TI para el establecimiento de la situación actual con respecto a las mejores prácticas de Cobit 2019. | Situación actual con base en la voz de la cliente obtenida de entrevistas y reuniones.<br><br>Situación Actual obtenida del diagrama SIPOC<br><br>Cadena de valor de la situación actual resultado del análisis del Mapa de cadena de valor (VSM) | Entrevistas y reuniones<br><br>SIPOC situación actual<br><br>Mapa de cadena de valor de alto nivel situación actual (VSM) | Documento diagnóstico de situación actual |

| | | | |
|---|---|---|---|
| | Flujo de procesos de la situación actual consecuencia del diagrama de flujo. | Diagrama de flujo de la situación actual | |
| Identificar la situación deseada del proceso de Monitoreo de Infraestructura Tecnológica para la identificación de las brechas. | Situación deseada con base en la voz de la cliente obtenida de entrevistas y reuniones.<br><br>Situación Deseada obtenida del diagrama SIPOC:<br><br>Cadena de valor de la situación deseada resultado del análisis del Mapa de cadena de valor (VSM)<br><br>Flujo de procesos de la situación deseada consecuencia del diagrama de flujo. | Entrevistas y reuniones<br><br>SIPOC situación deseada<br><br>Mapa de cadena de valor de alto nivel situación deseada (VSM)<br><br>Diagrama de flujo de la situación deseada<br><br>Matriz RACI | Documento diagnóstico de situación deseada |
| Rediseñar el proceso de Monitoreo de Infraestructura de TI para el cierre de las brechas identificadas, mediante la aplicación del ciclo DMAIC. | Proceso rediseñado consecuencia de aplicar un ciclo DMAIC | SIPOC situación deseada<br><br>Mapa de cadena de valor de alto nivel situación deseada (VSM)<br><br>Diagrama de flujo de la situación deseada.<br><br>Diagramas de flujo por carriles<br><br>Matriz RACI<br><br>Procedimientos operativos estandarizados SOP’s | Documento de proceso desarrollado rediseñado después de un ciclo DMAIC. |
| Transferir el conocimiento del nuevo proceso de infraestructura para que el departamento de informática adopte de forma adecuada la nueva metodología. | Presentación del proceso rediseñado<br><br>Transferencia de conocimiento de los SOP’s | Documento de proceso desarrollado rediseñado después de un ciclo DMAIC.<br><br>Documentos generados en objetivos anteriores.<br><br>Presentaciones | Procedimientos operativos estandarizados SOP’s<br><br>Presentación de SOP’s al cliente |

| | | | |
|---|---|---|---|
| | Transferencia de conocimiento de los métodos de control del nuevo proceso | | |
| Esbozar las recomendaciones para el siguiente ciclo de aplicación DMAIC, mediante la inducción de las herramientas desarrolladas para el nuevo proceso. | Generar las lecciones aprendidas y recomendaciones generales | Análisis retrospectivo<br><br>Formulario lecciones aprendidas<br><br>Documento de recomendaciones. | Informe conclusión de consultoría |
| **OBJETIVO GENERAL** | Rediseñar el proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma. | | |

## 3.5. Diseño de la Investigación

A continuación, se muestra un cuadro que resume las fases de este proyecto:

**Tabla 5**

*Diseño de la Investigación*

| OBJETIVO | FASE | ACTIVIDAD | RESULTADO | HERRAMIENTA |
|---|---|---|---|---|
| 1. Diagnosticar el estado del proceso de monitoreo de infraestructura de TI para el establecimiento de la situación actual con respecto a las mejores prácticas de Cobit 2019. | Análisis de situación | Análisis de situación actual<br>• Entrevistas y reuniones (la voz del cliente)<br>• SIPOC<br>• Mapa de procesos de alto nivel<br>• Mapa de Cadena de Valor | Análisis de situación del proceso de monitoreo | Entrevistas y reuniones<br><br>SIPOC situación actual<br><br>Mapa de cadena de valor de alto nivel situación actual (VSM)<br><br>Diagrama de flujo de la situación actual |
| 2. Identificar la situación deseada del | | Análisis de situación deseada | | Entrevistas y reuniones |

| | | | | |
|---|---|---|---|---|
| proceso de Monitoreo de Infraestructura Tecnológica para la identificación de las brechas. | | Identificación de brechas<br><br>Creación de Plan de acción | | SIPOC situación deseada<br><br>Mapa de cadena de valor de alto nivel situación deseada (VSM)<br><br>Diagrama de flujo de la situación deseada<br><br>Matriz RACI |
| 3. Rediseñar el proceso de Monitoreo de Infraestructura de TI para el cierre de las brechas identificadas, mediante la aplicación del ciclo DMAIC. | Fase de implementación | Aplicar con base en un ciclo DMAIC el rediseño del proceso considerando las buenas prácticas consideradas por Cobit 2019. | Proceso rediseñado | SIPOC situación deseada<br><br>Mapa de cadena de valor de alto nivel situación deseada (VSM)<br><br>Diagrama de flujo de la situación deseada.<br><br>Diagrama de flujo por carriles<br><br>SOP's<br><br>Matriz RACI |
| 4. Transferir el conocimiento del nuevo proceso de infraestructura para que el departamento de informática adopte de forma adecuada la nueva metodología. | | Creación de material necesario relacionado con el objetivo 3 para que en sesiones programadas después de la entrega de este proyecto se ejecute la transferencia de conocimiento | Material de transferencia de conocimiento entregado | Documento de proceso desarrollado rediseñado después de un ciclo DMAIC.<br><br>Documentos generados en objetivos anteriores.<br><br>Presentaciones |
| 5. Esbozar las recomendaciones para el siguiente ciclo de aplicación DMAIC, mediante la inducción de las herramientas desarrolladas para el nuevo proceso. | | Mediante un análisis retrospectivo y la recolección de las lecciones aprendidas se crea un informe de los aprendizajes de este rediseño. | Aprendizajes del primer rediseño para análisis de la organización en ciclos subsecuentes de mejora del proceso. | Análisis retrospectivo<br><br>Formulario lecciones aprendidas (conclusiones)<br><br>Documento de recomendaciones. |

## 3.6. Matriz de coherencia

Seguidamente. Se presenta un cuadro que sirve para crear una relación entre objetivos, herramientas de captura de datos, teorías y entregables:

**Tabla 6**

*Matriz de Coherencia*

| OBJETIVO | ENTREGABLE | FASE O ETAPA | TECNICAS DE RECOLECCION | INSTRUMENTOS | TEMAS RELACIONADOS PARA MARCO TEORICO |
|---|---|---|---|---|---|
| 1. Diagnosticar el estado del proceso de monitoreo de infraestructura de TI para el establecimiento de la situación actual con respecto a las mejores prácticas de Cobit 2019. | Documento diagnóstico de situación actual | Análisis de situación | Entrevistas y reuniones (Voz del cliente)<br><br>Observación en sitio (SIPOC / High Level Flow Chart)<br><br>Aplicación de herramientas de un ciclo DMAIC<br><br>Revisión de logs y bitácoras (Value Stream Map) | Formulario de entrevistas (Anexo 2)<br><br>Resumen de la observación en sitio<br><br>SIPOC situación actual<br><br>Mapa de cadena de valor de alto nivel situación actual (VSM)<br><br>Diagrama de flujo de la situación actual | Monitoreo de Infraestructura de TI<br><br>Lean 6 Sigma |
| 2. Identificar la situación deseada del proceso de Monitoreo de Infraestructura Tecnológica para la identificación de las brechas. | Documento diagnóstico de situación deseada | | Datos recolectados en objetivo 1<br><br>Aplicación de herramientas de un ciclo DMAIC | Entrevistas y reuniones<br><br>SIPOC situación deseada<br><br>Mapa de cadena de valor de alto nivel situación deseada (VSM)<br><br>Diagrama de flujo de la situación deseada<br><br>Matriz RACI | Monitoreo de Infraestructura de TI<br><br>Lean 6 Sigma |

| | | | | | |
|---|---|---|---|---|---|
| 3. Rediseñar el proceso de Monitoreo de Infraestructura de TI para el cierre de las brechas identificadas, mediante la aplicación del ciclo DMAIC. | Documento de proceso desarrollado rediseñado después de un ciclo DMAIC. | Fase de implementación | Aplicación de SIPOC situación deseada<br><br>Aplicación de Diagramas de flujo situación deseada<br><br>Aplicación de Diagrama de flujos por carriles situación deseada<br><br>Aplicación de Mapa de cadena de valor situación deseada<br><br>Presentación | SIPOC situación deseada<br><br>Mapa de cadena de valor de alto nivel situación deseada (VSM)<br><br>Diagrama de flujo de la situación deseada.<br><br>Diagrama de flujos por carriles<br><br>SOP's<br><br>Matriz RACI | Monitoreo de Infraestructura de TI<br><br>Lean 6 Sigma<br><br>Cobit 2019<br><br>Excelencia Operativa |
| 4. Transferir el conocimiento del nuevo proceso de infraestructura para que el departamento de informática adopte de forma adecuada la nueva metodología. | SOPS<br><br>Presentación de SOPS al cliente | | Presentación del proceso rediseñado<br><br>Transferencia de conocimiento de los SOP's<br><br>Transferencia de conocimiento de los métodos de control del nuevo proceso | Presentación del proceso rediseñado<br><br>Transferencia de conocimiento de los SOP's<br><br>Transferencia de conocimiento de los métodos de control del nuevo proceso | Monitoreo de Infraestructura de TI<br><br>Lean 6 Sigma<br><br>Cobit 2019<br><br>Excelencia Operativa |
| 5. Esbozar las recomendaciones para el siguiente ciclo de aplicación DMAIC, mediante la inducción de las herramientas desarrolladas para el nuevo proceso. | Informe conclusión de consultoría | | Generar las lecciones aprendidas y recomendaciones generales (Conclusiones y Recomendaciones) | Análisis retrospectivo<br><br>Formulario lecciones aprendidas<br><br>Documento de recomendaciones. | Monitoreo de Infraestructura de TI<br><br>Lean 6 Sigma<br><br>Cobit 2019<br><br>Excelencia Operativa |

# Capítulo IV: DIAGNÓSTICO DE SITUACIÓN ACTUAL

El objetivo de este capítulo consiste en identificar la situación actual en que se encuentra el proceso de Monitoreo de TI ofrecido por el NOC de Gosys Pro.

Gracias a las facilidades proporcionadas por el marco referencial Lean Six Sigma, existen algunas herramientas sencillas pero muy poderosas, las cuales permiten no solo brindar un diagnóstico detallado con suficiente precisión, sino proponer las pautas para establecer la situación deseada, así como el seguimiento a las correcciones requeridas.

Ahora bien; Se presenta a continuación algunos hallazgos interesantes que serán muy útiles para comprender cómo se está realizando en la actualidad el proceso de Monitoreo de Infraestructura de TI.

## 4.1. Análisis SIPOC

El diagrama SIPOC (supplier, input, process, output, client, por sus siglas en inglés), es una herramienta muy útil y sencilla que sirve para visualizar de una forma global los procesos, quién los provee, sus entradas, salidas y clientes o destinatarios.

El proceso de Monitoreo de infraestructura TI, se encarga de mantener una activa y constante vigilancia sobre los servicios de TI. Garantizando la disponibilidad y continuidad de este. Cualquier evento que pueda interferir contra dicha continuidad, generará una alerta.

Las alertas por incidencias en infraestructura de TI son el insumo principal con el que trabajan las unidades de monitoreo de TI. El proceso a nivel general sería gestionar su resolución, para finalmente documentarla y resolverla.

**Tabla 7**

*Análisis SIPOC Situación Actual*

| SUPPLIER | INPUT | PROCCESS | OUTPUT | CUSTOMER |
|---|---|---|---|---|
| Servidores FTP<br><br>Switches de red<br><br>Servidor de monitoreo<br><br>Servidores de bases de datos<br><br>Otros servidores y dispositivos de infraestructura | Datos de eventos | Ingesta y recopilación de datos | Datos recolectados | Agente |
| Agente | Datos recolectados | Asignación de métricas | Datos con métricas | App de monitoreo |
| App de monitoreo | Datos con métricas | Procesamiento de Información | Datos procesados | Alert Manager |
| Alert manager | Datos procesados | Generación de alerta | Alerta generada | Dashboard de monitoreo |
| Dashboard de monitoreo | Alerta generada | Presentación de alertas | Alerta para resolver automáticamente<br><br>Alerta escalada a operador | Programa de solución automática de alertas<br><br>Operador de monitoreo |
| Operador | Alerta asignada a operador | Escalamiento de alerta | Alerta escalada a segundo o tercer nivel | Niveles expertos (DBA, redes, soporte, programación) |
| Niveles expertos (DBA, redes, soporte, programación) | Alerta escalada a segundo o tercer nivel | Resolución de incidencia | Alerta resuelta | Operador |
| Operador | Alerta resuelta | Seguimiento de Alerta | Alerta no solventada<br><br>Alerta solventada | Vuelve a escalar<br><br>Cierre de alerta |
| Operador | Alerta cerrada | Cierre y documentación de alerta | Alerta documentada | Informa a unidades usuarias<br><br>Informa a niveles expertos |

Como se puede observar en el cuadro anterior, la unidad de monitoreo, en algunas ocasiones, requiere de los servicios de una unidad experta (infraestructura de TI, Redes, Soporte, Administración de bases de datos), para gestionar la resolución de los eventos por lo que también se convierte en cliente.

Es importante tener presente que, en algunos casos, las unidades expertas pueden tardar más de lo esperado en la resolución de los problemas.

El proceso de Monitoreo de infraestructura de TI es muy sencillo. Consta de nueve subprocesos identificados sucesivos el uno del otro. Este proceso corresponde a cada alerta. Más adelante se presenta un cuadro que muestra la cantidad de alertas procesadas y un pequeño análisis estadístico.

Entre los eventos más comunes que generan alertas, se menciona los fallos en procesos, fallos de memoria, desconexiones de nodos de la red, caída de algún proceso o servicio. Caídas de bases de datos entre otros.

1. Los componentes de infraestructura (servidores, switches, routers, bases de datos, servidores FTP) generan y envían información general. Dicha información corresponde a bitácoras que registran datos sobre procesos, uso de memoria, ancho de banda, disponibilidad de red y servicios, resultados y otros. Dicha información se almacena en logs.
2. El agente, que está instalado en cada componente de la infraestructura; ejecuta una asignación de métricas a los datos capturados anteriormente. Posteriormente, dicha información ya con métricas es trasladada a la aplicación de monitoreo. Las alertas se generan gracias a las métricas capturadas por al agente, el cual utiliza de protocolos, http, ftp, sms, smmp y otros.

3. La aplicación de monitoreo procede con el procesamiento general de la información la cual ya contiene métricas, priorización y criticidad y la traslada a los “Dashboard” de Monitoreo. Algunas de las incidencias reportadas se resuelven de forma rápida (menos de 1 minuto) y automática. Por ejemplo “pings” fallidos, caídas temporales de enlaces con puntos de ventas.
4. El resto de las alertas (la mayoría), quedan en el “Dashboard” de monitoreo y se le envía notificación al operador de monitoreo ya sea por SMS, correo o cualquier otro medio.
5. El operador utiliza el “Dashboard” para analizar la información y proceder con el escalamiento respectivo para que los expertos en cada una de las áreas de TI.
6. Los usuarios expertos de segundo o tercer nivel (Administrador de bases de datos, encargados de red, técnicos expertos), son quienes realizan las acciones correctivas en un plazo establecido. Mientras tanto, el operador de monitoreo da seguimiento.
7. Una vez que el usuario experto resuelva la incidencia, procede a notificar al operador de monitoreo quien debe corroborar la pertinencia de la solución.
8. En caso de que la incidencia sea resuelta con buen suceso; el operador ejecuta el cierre del “ticket”. En caso de que el problema persista, procede con un nuevo escalamiento del caso a los segundos niveles para una segunda revisión y su respectiva corrección. En esto consiste el proceso de seguimiento.
9. Ya cerrado el caso, finalmente se documenta en el repositorio de conocimiento de manera que se pueda identificar patrones, conductas, comportamientos y a su vez, ir trabajando en acciones integrales que permitan evitar de forma permanente la ocurrencia de esa incidencia.

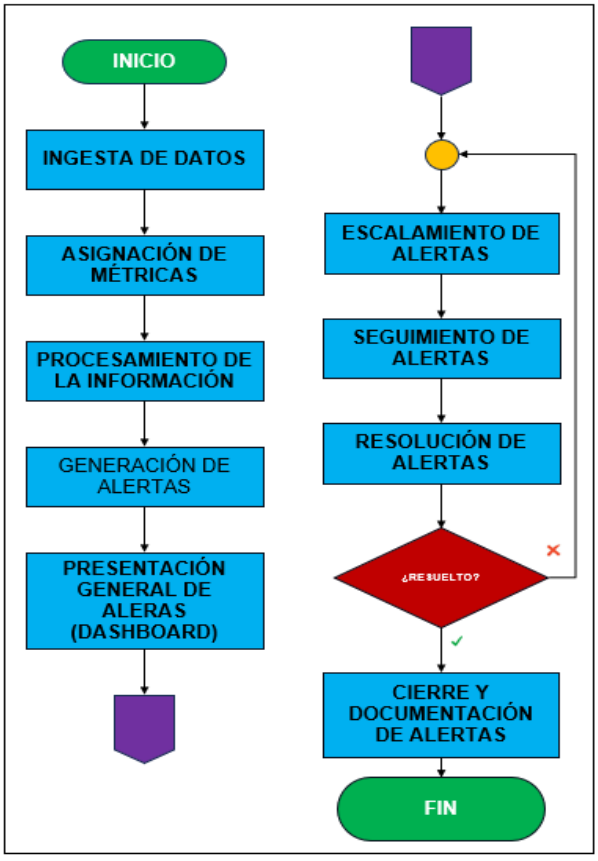
## 4.2. Mapa de proceso de alto nivel

Ya en el diagrama SIPOC, se pudo observar elementos importantes tales como proveedores, entradas, salidas y clientes del proceso de monitoreo de una manera superficial. También presentó una descripción general de cada uno de los nueve procesos. Cinco se realizan de forma automática y cuatro por los operadores de monitoreo.

Por medio de este diagrama de flujo de alto nivel, se observa de una forma más sencilla y resumida cómo se ejecuta el proceso de Monitoreo de TI por parte de la empresa Gosys Pro.

**Ilustración 11**

*Diagrama de Flujo General*



Como se puede apreciar, el proceso general de monitoreo de TI es muy sencillo. Es un ciclo general de atención de alertas que se repite tantas veces como ocurra incidencias en los servicios de Infraestructura de TI.

### 4.3. Análisis estadístico del proceso de monitoreo de TI

Para efectos de realizar un análisis más fidedigno, Se obtuvo por parte de la compañía Gosys Pro un amplio listado de bitácoras. Se trata de un total de 67444 eventos registrados entre el 01 de junio de 2023 y el 30 de septiembre del 2023. Se encontraron 33 tipos diferentes de eventos. En el apartado de Anexos 5 al 7, se adjunta toda la información procesada.

El siguiente cuadro muestra la cantidad de eventos ocurridos durante cada mes y en total, también muestra al final la cantidad total de incidencias. Las mismas han sido ordenadas de menor a mayor frecuencia:

**Tabla 8**

*Tabulación Total de Eventos*

| TIPO | JUN | JUL | AUG | SEP | TOTALES |
|---|---|---|---|---|---|
| ADQ_RELAY | 2 | 0 | 0 | 0 | 2 |
| OriginationRule | 2 | 0 | 0 | 2 | 4 |
| PrometheusAlertmanagerJobMissing | 5 | 0 | 0 | 0 | 5 |
| TotalProcesses | 2 | 0 | 9 | 5 | 16 |
| PrometheusAllTargets | 34 | 0 | 0 | 6 | 40 |
| Swap | 13 | 0 | 14 | 16 | 43 |
| ncpalistener | 22 | 7 | 26 | 44 | 99 |
| ncpapassive | 28 | 7 | 27 | 44 | 106 |
| ProccessCMD | 49 | 8 | 22 | 39 | 118 |
| HostDown | 34 | 40 | 23 | 58 | 155 |
| CheckSystemLog | 49 | 9 | 61 | 59 | 178 |
| ReadTime | 64 | 32 | 76 | 84 | 256 |
| WriteTime | 81 | 33 | 73 | 84 | 271 |
| CheckService | 71 | 28 | 81 | 109 | 289 |
| WindowsServerDiskSpace | 95 | 54 | 96 | 84 | 329 |
| ProcessCount | 97 | 15 | 171 | 65 | 348 |
| WriteBytes | 151 | 118 | 135 | 165 | 569 |
| Check_Failed_Jobs | 181 | 142 | 144 | 168 | 635 |
| AppPool | 3 | 204 | 190 | 250 | 647 |
| ReadBytes | 180 | 172 | 168 | 194 | 714 |
| IIS | 168 | 193 | 184 | 235 | 780 |
| MemoryUsage | 184 | 124 | 264 | 332 | 904 |
| Check_Uptime | 233 | 236 | 227 | 247 | 943 |
| EnlacesDown | 334 | 643 | 364 | 102 | 1443 |
| CheckLogical | 425 | 115 | 567 | 477 | 1584 |
| EnlacesCritical | 366 | 322 | 620 | 415 | 1723 |
| Sophos | 523 | 127 | 609 | 485 | 1744 |
| PingCritical | 438 | 375 | 681 | 423 | 1917 |
| SiteHTTPFailure | 607 | 493 | 706 | 373 | 2179 |
| SQLMessages | 769 | 491 | 889 | 1038 | 3187 |
| WindowsServerMemory | 1740 | 1730 | 1481 | 2422 | 7373 |
| CPUusage | 5642 | 5140 | 3011 | 3143 | 16936 |
| WindowsServerService | 7405 | 8424 | 7388 | 247 | 23464 |
| **Totales** | **19997** | **19282** | **18307** | **11415** | **69001** |
| | | | | | |
| Cantidad del reporte | 19793 | 18982 | 17634 | 11035 | 67444 |
| Diferencia[13] | 204 | 300 | 673 | 380 | 1557 |
| | | | Margen de error.....: | | 2,31% |

Fuente: Corrales, Oscar. *Resultados.xlsx.2023*

[13] Esta diferencia se obtiene debido a que las incidencias tabuladas se obtuvieron directamente de un query. Es posible que algunos datos se hayan duplicado.

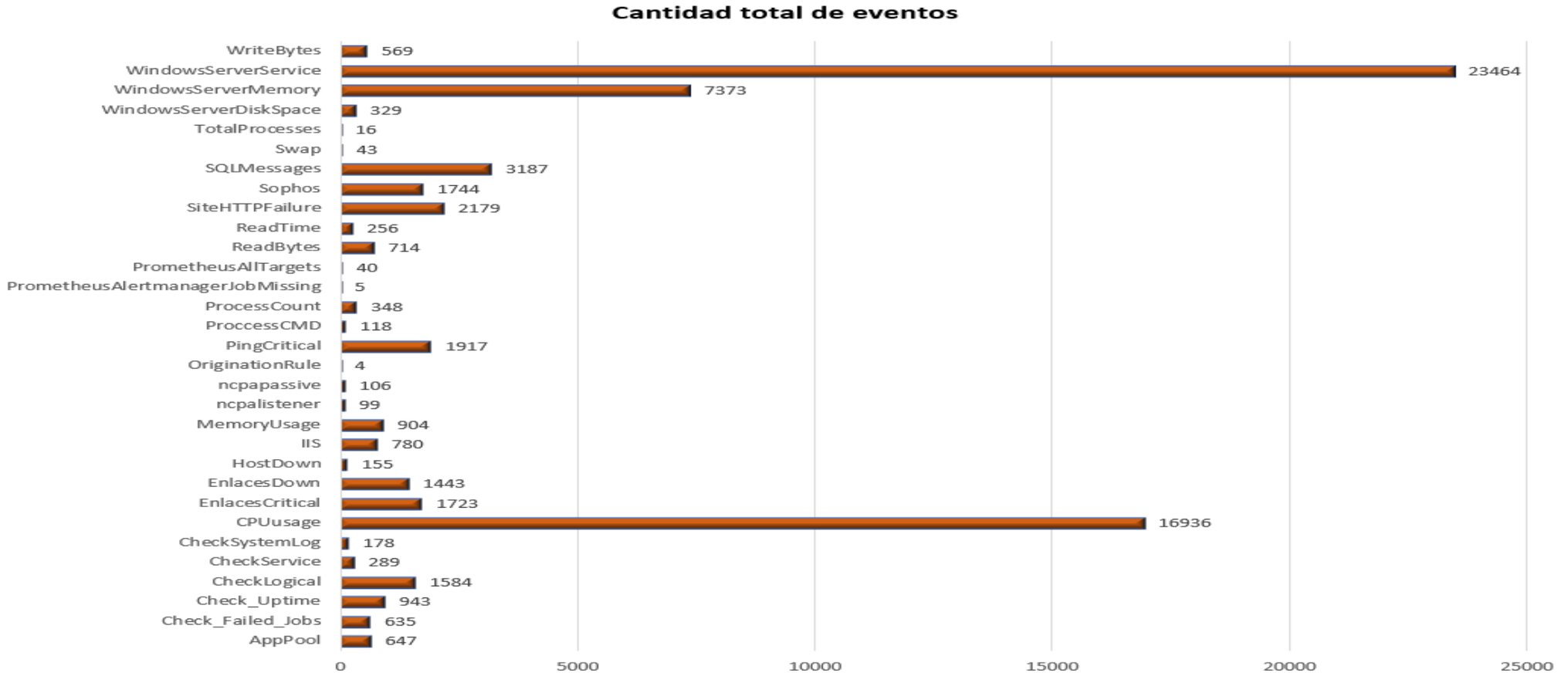
Como puede observarse en el cuadro anterior, existe una lista muy heterogénea en la cantidad de eventos registrados. Mientras que algunos tipos de eventos (por ejemplo: ADQ_RELAY), ocurren muy pocas veces al mes (menos de 10 veces). Otros solamente dos veces en todo el cuatrimestre. Por otro lado, otros eventos que son sumamente frecuentes (ejemplo “WindowsServerService”). A razón de más de 5000 mensuales.

A la hora de agrupar los datos por tipo de evento, se repitieron varios, lo cual generó un sobregiro de 1557 eventos para un total de 69001 alertas. Si se toma esa diferencia y se divide entre la cantidad real de logs, se descubre que el margen de error es de 2.31%.

A modo de gráfico, dicho comportamiento se visualiza de la siguiente manera

**Ilustración 12**

*Cantidad de Eventos por Cuatrimestre*




Fuente: Corrales, Oscar. *Resultados.xlsx.2023*

Para efectos más prácticos, se ha decidido analizar esta información desde tres puntos de vista: costo, criticidad y tiempo de atención

### 4.3.1. Costo

De acuerdo con lo conversado con el patrocinador encargado de Gosys Pro. Debido a que Gosys Pro es una pyme que utiliza licencias de “open source” e infraestructuras alojadas en la nube. Los costos son muy bajos.

El costo total por uso de licencias es de aproximadamente $610 mensuales. El Costo aproximado mensual por salarios de los operadores es de $3 888. La suma de estos dos rubros da como resultado un estimado de US $4 498.00 mensuales por concepto de Costos de Operación.

Cabe recordar que Gosys Pro como tal no tiene un domicilio. Salvo la oficina del CEO ubicada en su casa de habitación. Los operadores de monitoreo se encuentran en teletrabajo y acceden desde sus equipos de forma remota por medio de un VPN a las plataformas de Gosys Pro. Por lo que solo se toma en cuenta el costo por salarios de los operadores. Ellos se encuentran en horarios alternos cubriendo las 24 horas del día. Los 365 días del año.

La resolución de las incidencias reportadas no es competencia de Gosys Pro, sino propiamente del cliente, por lo que se desconoce el costo por segundo y tercer nivel de atención.

El siguiente cuadro estima los costos productivos en rangos inferiores y por último el costo por alerta atendida.

**Tabla 9**

*Costos Promedios*

| **Costos promedios** | |
|---|---|
| Mensual | $4 498.00 |
| Diario | $187.42 |
| Por hora | $3.12 |
| Por Alerta | $3.75 |

*Nota. Los $3.75 por alerta se obtienen por la división del promedio de 16 861 alertas mensuales recibidas entre los $4 498 de costos productivos.

Alertas promedio mensual = 67444 / 4 =

Costo por alerta = 16861 / 4498 = $3.75

Gosys Pro cobra una suma estimada de $6 000 mensuales a la empresa que actualmente goza de sus servicios. No obstante, dicha suma puede variar según se negocie entre las partes.

### 4.3.2. Criticidad

El segundo enfoque con el que se procede a analizar la información obtenida es según su criticidad.

La siguiente tabla muestra de igual forma la cantidad total de eventos ocurridos en el rango de un cuatrimestre (De junio a septiembre 2023), así como una breve mención al tipo de incidencias ocurridas:

**Tabla 10**

*Cantidad de Eventos Según Criticidad*

| CRITICIDAD | TIPO | JUNIO | JULIO | AGOSTO | SEPTIEMBRE | TOTALES |
|---|---|---|---|---|---|---|
| **MODERADO** | • Servidor de monitoreo AlertmanagerJobMissing<br>• HostName<br>• Certificados próximos a caducar | 5 | 8 | 11 | 0 | 24 |
| **ALTO** | • Enlaces punto de venta del cliente ping Critical<br>• CPU Usage<br>• Memory Usage<br>• Check Read<br>• Check Write<br>• Sophos | 9381 | 7397 | 7381 | 7509 | 31668 |
| **CRITICO** | • Enlaces punto de venta caídos. WindowsServerStatus<br>• IIS AppPool<br>• Servidores caídos<br>• SiteHttpFailure, WindowsMemoryUsage | 10407 | 11577 | 10242 | 3526 | 35752 |
| | **Totales** | **19793** | **18982** | **17634** | **11035** | **67444** |

Fuente: Corrales, Oscar. *Criticidad.xlsx.2023*

Las bitácoras revelan una ínfima cantidad de incidentes con criticidad moderada. Por lo general son errores de conexión entre el servidor de monitoreo y el resto de la infraestructura. También errores como hosts no encontrados o certificados próximos a vencer.

Los eventos con criticidad alta, es lo que conocemos como advertencias o “warnings”, a las que se les debe prestar mayor atención con el fin de prevenir la caída del servicio. Generalmente consiste en alertas por saturación en el uso de memoria o CPU, chequeos de lectura y escritura o paquetes extraviados a la hora de hacer “ping” con los puntos de venta.

Los eventos críticos son los más frecuentes y a su vez, representan una evidente afectación a la continuidad del servicio. Nótese que los tipos de alertas indicados corresponden a servidores caídos, enlaces caídos con los puntos de venta del cliente, caída de servicios IIS, o bien colapso de servidores por memoria o uso del CPU.

El siguiente gráfico muestra dicho comportamiento de la siguiente manera:

**Ilustración 13**

*Gráfico Alertas Según Criticidad*


Fuente: Corrales, Oscar. *Criticidad.xlsx.2023*

### 4.3.3. Duración

Con respecto a la duración de las alertas, se procedió con la tabulación de los tiempos de cierre de estas, se obtuvo el siguiente resultado:

**Tabla 11**

*Tiempos de Resolución de Alertas*

| TIEMPO DE RESOLUCIÓN | CANTIDAD | PORCENTAJE |
|---|---|---|
| NULL | 504 | 0,75 |
| MAS DE 1 MES | 41 | 0,06 |
| DE 1 A 31 DIAS | 1020 | 1,51 |
| DE 1 A 24 HORAS | 2931 | 4,35 |
| DE 1 A 59 MINUTOS | 62441 | 92,58 |
| MENOS DE 1 MINUTO | 507 | 0,75 |
| **TOTAL DE REPORTES** | **67444** | **100** |

Fuente: Corrales, Oscar. *Tiempos Totales.xlsx*.2023

Como se puede observar, La gran mayoría de incidencias (92.58%), se logran resolver en menos de 1 hora. Existe un 4,35% se solventan en el transcurso del día en un plazo inferior a 24 horas. Un 1.51% se cierran en un plazo superior a 1 día, pero inferior a un mes.

Por otra parte, la muestra arroja 41 alertas que fueron cerradas en un plazo superior a 1 mes, dos de ellas superando los 4 meses de plazo.

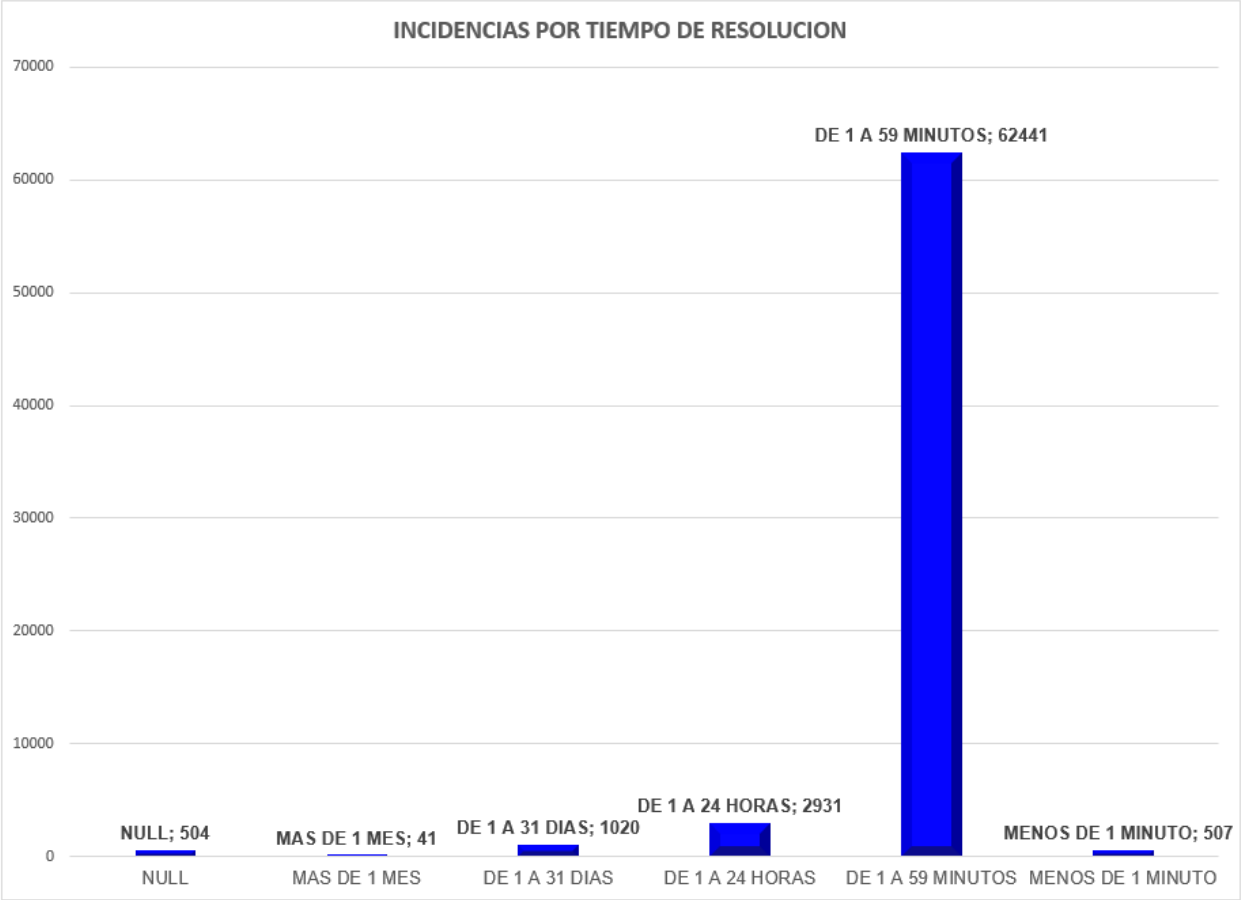
Existe un 0.75 de las incidencias reportadas que no tienen tiempo registrado, por lo que son valores nulos. No se tiene información del motivo que genera esta situación.

Finalmente, un 0.75% de los eventos fueron resueltos en un plazo inferior a 1 minuto. Es posible que esto sea por pequeñas interrupciones en las conexiones de red.

La gráfica que refleja este comportamiento se visualiza de la siguiente manera:

**Ilustración 14**

*Gráfico Alertas por Tiempo de Resolución*




Fuente: Corrales, Oscar. *Tiempos Totales.xlsx*.2023

Si se toma los valores del período analizado (4 meses) y se promedian, se obtiene la siguiente información:

**Tabla 12**

*Tiempo Promedio de Atención de Alertas*

| TIEMPO PROMEDIO DE ATENCIÓN DE ALERTAS | | |
|---|---|---|
| Promedio por mes | 16861 | |
| promedio por día | 562,03 | |
| promedio por hora | 23,42 | |
| promedio por minuto | 0,39 | |
| promedio por segundo | 0,0065 | **(takt Time)** |

Fuente: Corrales, Oscar. *Tiempos Totales.xlsx*.2023

Como se puede notar, se logra resolver un promedio de 23 alertas en 1 hora, el "takt time" se calcula en 0.0065 alertas resueltas por segundo.

De ahora en adelante, se redondeará los valores de promedio diario en 562 alertas diarias y promedio de 23 alertas por hora.

## 4.4. Mapa de valor del flujo del proceso

La información obtenida en el punto anterior es vital para general el Mapa de cadena de valor. A continuación, se adjunta el mapa de valor del proceso el cual trataremos de explicar a continuación de acuerdo con los siguientes elementos:

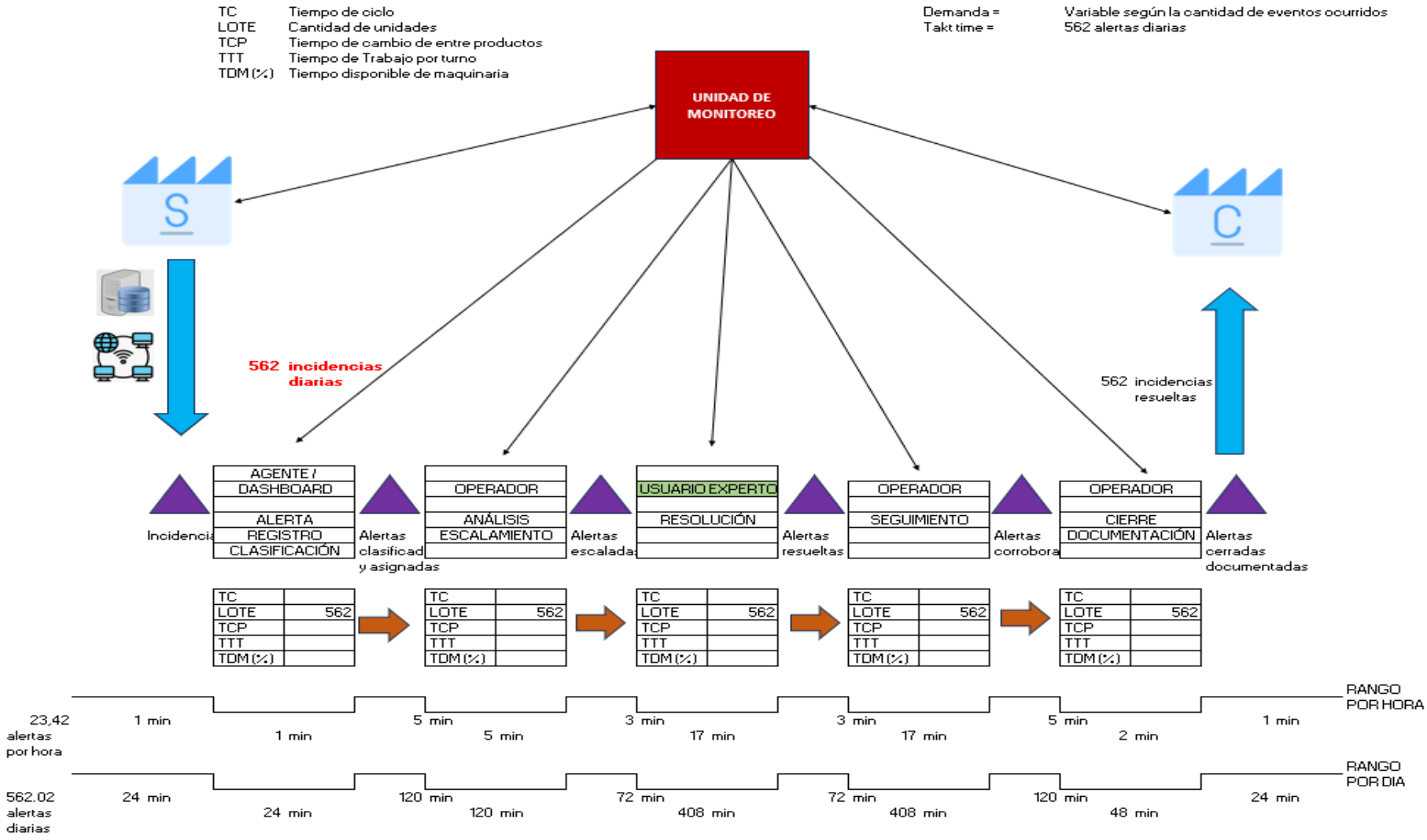
Familia del producto: Alertas por eventos informáticos

Estado actual del proceso: Activo y en producción

Takt Time: 562 alertas diarias.

**Ilustración 15**

*Mapa de Valor del Flujo de Procesos*



Se agrupa los procesos según el Mapa del proceso de alto nivel. Los elementos automáticos se agrupan en la primera caja. Otra caja hace referencia a los procesos de resolución automática de incidencias, Otras dos cajas aluden las tareas ejecutadas por el operador de TI y una más haciendo referencia al especialista segundo nivel.

Por otra parte, se debe tener en cuenta que los tiempos de resolución de las alertas son un promedio de 562 alertas diarias, las cuales se subdividen en los subprocesos ejecutados tanto por hora como por día. Los subprocesos automáticos suelen ser más rápidos, casi que inmediatos. Los que se escalan a segundo nivel son los más lentos.

Tomando en cuenta que existen seis operadores de monitoreo. Si se toma las 562 alertas diarias y se divide entre cada uno de ellos, se obtiene un aproximado de 94 alertas diarias por operador.

Cabe destacar que la mayoría de las alertas (92% aproximadamente), se resuelven en menos de 1 hora. Considerando que la jornada diaria de cada operador de monitoreo es de 8 horas, el operador debería atender en promedio 11.75 alertas cada hora.

## 4.5. Resumen del diagnóstico

Luego de realizar una revisión general del proceso de monitoreo de TI por medio de las herramientas utilizadas anteriormente, es posible indicar las siguientes observaciones a modo de diagnóstico:

### 4.5.1. Observaciones según Cobit 2019

De acuerdo con el marco de sanas prácticas Cobit 2019, el proceso de monitoreo de TI cumple satisfactoriamente con varios de los objetivos planteados en el los dominios MEA01, DSS03, DSS04 (Ver Anexo 5). Esto por cuanto, la unidad de monitoreo de Gosys Pro sí realiza las siguientes acciones:

1. Existe una identificación y correlación de reportes de incidentes, bitácoras de errores y otros problemas.
2. Define niveles de prioridad en coordinación con el negocio para asegurar la identificación de la causa raíz de los problemas y resolverlos a tiempo.
3. Existe una base de datos de conocimiento de los errores más frecuentes y conocidos.
4. Se mantiene un monitoreo constante en tiempo real sobre los procesos y servicios de infraestructura del cliente.
5. Existe una preocupación real por reestablecer los servicios de TI lo más pronto posible.
6. Existe una intención por generar valor en los procesos de monitoreo de TI.
7. Se generan reportes para las partes interesadas.
8. Aseguran que se mantenga una responsabilidad por acciones correctivas.
9. Existe una constante comunicación con otros niveles de TI

Por otra parte, se detectaron brechas con las estipulaciones del marco Cobit 2019. Esto debido las siguientes razones:

1. No existen manuales documentados con indicaciones para atender las alertas.

2. Cada operador de monitoreo realiza las acciones de acuerdo con sus conocimientos. A la hora de capacitarles, los mismos toman sus apuntes y los tienen a mano, el proceso con el tiempo se vuelve mecánico e inconsciente.
3. El operador de monitoreo en general, solamente se limita a escalar tareas a niveles expertos y esperar a que las incidencias sean resueltas. No genera un análisis crítico o diagnóstico del evento ocurrido.
4. La unidad de monitoreo en general es un ente reactivo ante los eventos que ocurren, no asumen un papel protagónico en aras de resolver las incidencias.

### 4.5.2. Observaciones según diagrama de Ishikawa

A continuación, se adjunta un pequeño listado de observaciones tomando en cuenta la causa raíz, la cual provoca que no existe una estandarización en el proceso de Monitoreo de TI. No se omite indicar que el diagrama de Ishikawa evalúa activos y elementos componentes de la organización que, si no están en óptimas condiciones, repercutirán en una afectación real al proceso de Monitoreo de Infraestructura de TI.

#### i. Materias primas

Se considera materias primas al conjunto de alertas generadas por los eventos e incidencias reportadas. Dependen de las métricas aplicadas sobre la información arrojada por los servidores y la infraestructura en general.

ii. Medición

Se entiende como medición los tiempos de resolución de eventos. Los mismos deben ser consecuentes con los SLA's, KPI's y OLA's. Se toma en cuenta otros dos valores importantes como la criticidad de las incidencias, así como el costo por atención de cada alerta.

Ya en líneas anteriores (Mapa de Cadena de Valor y Análisis Estadístico del proceso de Monitoreo), se realizó un análisis un poco más profundo sobre los datos arrojados en la relación costo-tiempo-calidad.

Estos valores son un promedio de 562 alertas diarias (más del 92% resueltas en 1 hora), un costo de $3.75 por alerta o bien $187 diario.

iii. Métodos

En este momento no existe manuales documentados. El conocimiento se transfiere de forma verbal de persona a persona. Se pretende que la información saliente de este documento sirva como insumo para la creación de los manuales correspondientes.

iv. Mano de obra

Además del CEO de Gosys Pro, existen seis operadores de monitoreo, los cuales cubren las 24 horas, los 365 días del año. Se nota que, a nivel general, los operadores de monitoreo sí existen conocimientos suficientes sobre los procesos de monitoreo. Lamentablemente los segundos y terceros niveles (usuarios expertos que resuelven las incidencias reportadas), quedan fuera del alcance de esta investigación.

v. Medio Ambiente

La oficina de Gosys Pro, cuenta con buena ventilación e iluminación. Está localizada dentro de una casa de habitación que, a su vez, tiene su domicilio dentro de un condominio privado, por lo que goza de buena seguridad perimetral. También cuenta una conexión a internet de hasta 100mbs.

vi. Maquinaria

El CEO cuenta con un equipo personal portátil, lo mismo que los operadores. Todos se conectan por medio de VPN a los servidores alojados en la nube. Los servidores por su parte están alojados en contenedores instalados sobre plataformas como AWS, y Qubernetes.

### 4.5.3. Relación costo – calidad – velocidad

La velocidad de atención de requerimientos en general es muy buena, partiendo de que se atiende un promedio aproximado de 562 alertas diarias. A nivel global, más del 92% de las alertas son resueltas en un plazo inferior a 1 hora, lo cual sí demuestra un compromiso real por una atención expedita.

El ciclo del proceso es diario. El aumento o disminución de la cantidad de eventos no depende Gosys Pro, sino del cliente. De hecho, si se retoma la información presentada en la Tabla 8, se puede observar una reducción constante en la cantidad de alertas reportadas desde junio hasta septiembre. Esto pudo ocurrir por dos razones básicas:

1. Se ajustaron los umbrales en los sistemas de monitoreo por parte de Gosys Pro

2. Conforme pasa el tiempo. El cliente invierte en mejoras a su infraestructura.

En relación con los costos. Se calcula un aproximado de $3.75 por alerta. Este monto parece ser muy elevado.

Con respecto a la calidad, con la información obtenida, es imposible determinar la existencia de reprocesos o desperdicios. Sin embargo, sí evidencia las alertas ocurridas con más frecuencia, por lo que puede permitir a Gosys Pro y a los clientes tomar las decisiones correspondientes para buscar una solución radical a las mismas.

# Capítulo V: DISEÑO Y DESARROLLO DE LAS PROPUESTA DEL PROYECTO

En el capítulo anterior, se expuso el diagnóstico de la situación actual del proceso de Monitoreo de Infraestructura de TI. Esto con el fin de revelar y establecer las brechas correspondientes.

Por otra parte. Para este nuevo capítulo, la pretensión principal consiste en proponer una metodología de trabajo que permita alinear el proceso de monitoreo de la firma Gosys Pro con los estándares de la metodología Cobit 2019 mediante un nuevo ciclo DMAIC.

Una vez ejecutado este ciclo, se podrá no solo revelar las brechas en el proceso de monitoreo, sino crear el rediseño que permita eliminarlas. Este rediseño consiste en una visión más profunda y minuciosa de cada paso del proceso general de Monitoreo de TI.

Los entregables de este trabajo de investigación serán de gran ayuda para el patrocinador de este trabajo. El hecho de transferir el conocimiento al CEO de la firma Gosys Pro, le permitirá visualizar las brechas, reflexionar y ejecutar las acciones necesarias para solventar dichas brechas.

Sumado a lo anterior y de forma automática, quedará la puerta abierta para la ejecución de un nuevo ciclo DMAIC lo cual será un gran impulso para que las autoridades de la empresa patrocinadora desarrollen un ciclo de mejora continua y de esta forma, alcanzar la excelencia operativa.

A partir de este momento, se propondrá algunos cambios en algunos nombres:

Unidad de Monitoreo ===> Torre de Observabilidad

Operador de Monitoreo ===> Especialista en observabilidad

Este primer ajuste se plantea gracias a una conversación con el CEO de Gosys Pro (Anexo2), quien explica la diferencia entre cada uno de ellos.

## 5.2. Análisis SIPOC Situación deseada

En el análisis SIPOC presentado en el capítulo 4, se identificaron 9 procesos realizados por la unidad de monitoreo de TI. Esto según observaciones en sitio.

Ya realizando una inmersión en cada una de las actividades realizadas, se identifica 29 procesos más puntuales, de los cuales, 11 son ejecutados manualmente por usuarios de los sistemas. El resto, son tareas automáticas programadas en las herramientas para dicho fin.

**Tabla 13**

*Análisis SIPOC Situación Deseada*

| SUPPLIER | INPUT | PROCCESS | OUTPUT | CUSTOMER |
|---|---|---|---|---|
| Servidores FTP<br><br>Switches de red<br><br>Servidor de monitoreo<br><br>Servidores de bases de datos<br><br>Otros servidores y dispositivos de infraestructura | Información general de procesos y ejecuciones | Ingesta de datos | Datos recolectados | Agentes de monitoreo |
| Agentes de monitoreo | Datos recolectados | Asignación de métricas | Datos con métricas | App de monitoreo |
| App de monitoreo | Datos con métricas | Procesar información<br><br>Generar queries<br><br>Ejecutar reglas | Datos procesados | Alert Manager |
| Alert mánager | Datos procesados | Genera alerta | Alerta generada | Dashboard de monitoreo |
| Dashboard de monitoreo | Alerta generada | Comparación con línea base<br><br>Normalización de datos<br><br>Medición de alertas | Alerta para resolver automáticamente<br><br>Alerta escalada a especialista en observabilidad. | Programa de solución automática de alertas<br><br>Especialista en observabilidad |

| | | | | |
|---|---|---|---|---|
| | | Categorización de alertas<br><br>Priorización de alertas<br><br>Enviar alertas a programa de solución automática de alertas<br><br>Asignación de alertas a especialista de observabilidad<br><br>Presentación de información de alertas en tiempo real | | |
| Programa de solución automática de alertas<br><br>Especialista en observabilidad | Alerta para resolver automáticamente<br><br>Alerta asignada a operador | Ejecuta resolución<br><br>Cierra alerta<br><br>Documenta alerta<br><br>Analiza comportamientos, y eventos que genera alertas<br><br>Escala a nivel 2 (usuarios expertos)<br><br>Da seguimiento a alertas | Alerta resuelta<br><br>Alerta escalada a segundo nivel (nivel experto) | Unidades usuarias<br><br>Niveles expertos (DBA, redes, soporte, programación) |
| Niveles expertos (DBA, redes, soporte, programación) | Alerta escalada a segundo o tercer nivel | Análisis de alerta<br><br>Ejecuta resolución<br><br>Notifica a operador de monitoreo | Alerta resuelta | Operador |
| Operador | Alerta resuelta | Corrobora que se solvente el problema<br><br>Cierre de alerta | Alerta no solventada<br><br>Alerta solventada | Vuelve a escalar<br><br>Cierre de alerta |
| Operador | Alerta cerrada | Notifica a unidad usuaria<br><br>Notifica a unidad experta<br><br>Documenta en repositorio | Alerta documentada | Unidades usuarias<br><br>Unidades expertas |

A continuación, se describe cada una de las acciones realizadas en este nuevo proceso.

1. Se mantiene el primer proceso de ingesta de datos en el cual, los componentes de infraestructura (servidores, switches, routers, bases de datos, servidores FTP) generan y envían información general. Dicha información corresponde a bitácoras que registran datos sobre procesos, uso de memoria, ancho de banda, disponibilidad de red y servicios, resultados y otros. Nos referimos a routers, servidores, switches y otros. Dicha información se almacena en logs.
2. De igual manera, se mantiene el proceso mediante el cual el agente (que está instalado en cada componente de la infraestructura); ejecuta una asignación de métricas a los datos capturados anteriormente. Posteriormente, dicha información ya con métricas es trasladada a la aplicación de monitoreo. Las alertas se generan gracias a las métricas capturadas por al agente, el cual utiliza de protocolos, http, ftp, SMS, SNMP y otros.
3. La aplicación de monitoreo recibe toda la información ya con métricas, procederá con la generación de consultas en bases de datos para ordenar la información.
4. La misma aplicación de monitoreo ejecutará algunas reglas para depurar la información de las alertas
5. Seguidamente, la aplicación de monitoreo procesa y ordena dicha información para trasladarla al “Alert Manager”.
6. El “alert mánager”, con toda la información recibida procede con la generación de la alerta respectiva para trasladarla al “Dashboard” de Monitoreo.
7. El “Dashboard” de monitoreo compara la información con la línea base. Es decir, contra los umbrales.

8. Los datos deben ser normalizados, es decir: evaluar qué elementos generan valor y qué otros no son importantes para la resolución de los eventos.
9. Las alertas son medidas de forma que se pueda priorizar las mismas.
10. Se categorizan las alertas según su criticidad y afectación.
11. Se ordena las alertas según su prioridad de forma que se atienda primero las más críticas y urgentes.
12. En todo momento, la información de las alertas es presentada en tiempo real
13. Las alertas que sean repetitivas y fáciles de resolver deben ser enviadas a un programa que ejecute de forma automática la resolución de estas.
14. Las alertas más críticas, se deben asignar a un especialista en observabilidad para su debida atención.
15. Por su parte, el programa de resolución de alertas ejecuta la resolución de estas de forma automática.
16. El programa de resolución de alertas ejecuta el cierre del caso.
17. El programa de resolución de alertas ejecuta la documentación del caso en el repositorio del conocimiento.
18. El programa de resolución de alertas notifica a la unidad usuaria que la misma ha sido resuelta.
19. El programa de resolución de alertas notifica al especialista en observabilidad que la misma ha sido resuelta.
20. El especialista en observabilidad realiza un análisis general de comportamientos del evento. Su criticidad, qué afectación pueda propiciar y realiza un diagnóstico de la incidencia.

21. El especialista en observabilidad ejecuta un escalamiento de la alerta diagnosticada al nivel experto el cual se encargará de resolver.
22. Mientras la alerta es tratada por los segundos o terceros niveles, el especialista en observabilidad deberá dar un constante seguimiento.
23. El usuario experto debe realizar un análisis de la situación de acuerdo con el diagnóstico brindado por el especialista en observabilidad.
24. El usuario experto debe ejecutar la resolución de la forma más expedita posible, procurando que la misma sea pertinente y eficaz.
25. El usuario experto notifica al especialista en monitoreo.
26. El especialista en observabilidad notifica a la unidad usuaria para que se realicen pruebas.
27. En caso de que la solución no sea pertinente, se debe escalar nuevamente al experto de segundo nivel. En caso de una resolución satisfactoria, procede a cerrar la alerta.
28. Ya con la alerta cerrada, el especialista en observabilidad notifica a la unidad usuaria.
29. De igual forma, se notifica a la unidad experta.
30. Se documenta alerta en el repositorio correspondiente.

Tal vez, se puede visualizar muchos más pasos que los mencionados en el capítulo anterior. No obstante, la pretensión está en automatizar lo más que se pueda en la resolución de eventos.

De los pasos vistos anteriormente. Los pasos 13 y luego, del 15 al 19, consisten en la novedad. La pretensión es crear los programas, BOT’s, RPA’s y demás elementos que permitan una resolución automática y casi inmediata de eventos. Tanto los pequeños como algunos más complejos.

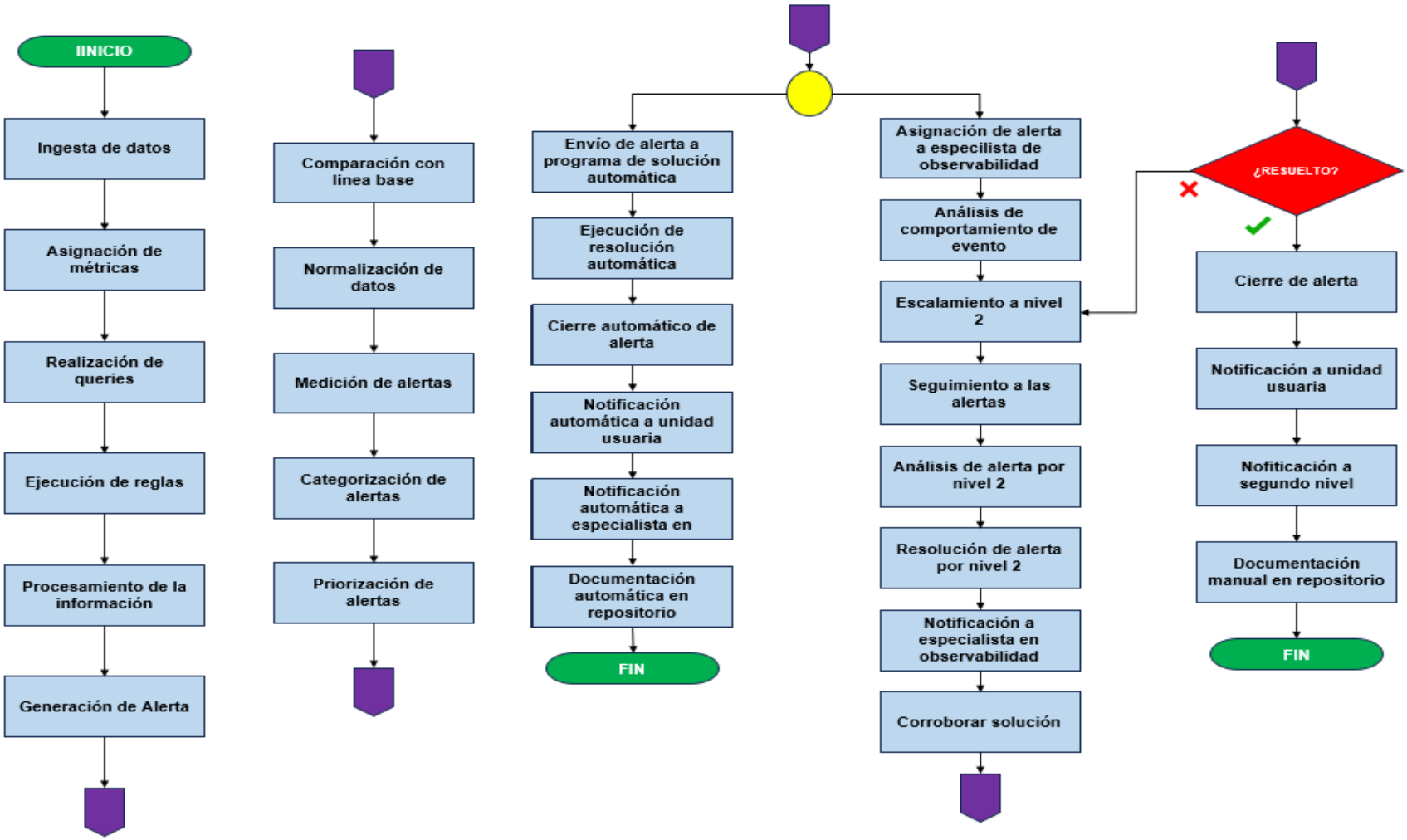
De igual forma, se pretende que el usuario de torre de observabilidad sea mucho más que alguien que recibe y escala casos a segundos niveles. Se pretende que tenga toda la capacidad de analizar, diagnosticar y gestionar la alerta en tiempo y forma.

### 5.3. Mapa de proceso de bajo nivel

Consecuencia de los pasos mencionados en el punto anterior. Se procede con la creación de un Mapa de Proceso de Bajo Nivel. El mismo consiste en una visión mucho más profunda. A continuación, se presenta el mapa de proceso de bajo nivel de la situación deseada. Es mucho más profundo que el expuesto en la situación actual. Esto por cuanto muestra procedimientos más puntuales y específicos

**Ilustración 16**

*Mapa del Proceso de Bajo Nivel*



La principal diferencia entre el mapa de proceso de alto nivel del capítulo anterior y la imagen de marras, radica en la forma en que se le debe dar tratamiento a los eventos por parte de los especialistas en observabilidad, así como los procesos automáticos.

Existe una transformación desde una unidad de monitoreo reactiva, básica, donde el operador de monitoreo es pasivo a la espera de casos, a una torre especializada de observabilidad donde se pueda gestionar dos grandes procesos importantes. A continuación, se explican:

1. Desarrollo de aplicaciones (BOT - RPA), las cuales se pueden conectar por interfaz a la infraestructura de TI y ejecutar algunas resoluciones que sean repetitivas. Por ejemplo, y retomando el análisis estadístico visto en el Análisis Estadístico del Proceso de Monitoreo de la situación actual, se puede observar que la mayor parte de eventos reportados corresponden a alertas por usos de CPU y Memoria. Por tanto, se podría desarrollar un procedimiento que tenga la capacidad de eliminar ciertos procesos identificados. Un ejemplo son sesiones de usuarios que llevan más de 5 minutos inactivas. También es posible automatizar la resolución de otros procesos más complejos.
2. Que la persona usuaria de los sistemas de monitoreo, no se limite a gestionar una alerta como si fuera un simple “pasador” que recibe la alerta y la escala mecánicamente a segundos niveles. El especialista en observabilidad, debe tener la capacidad de analizar bien a profundidad la información de los eventos ocurridos, tener la capacidad de hacer un diagnóstico de la incidencia y escalar a un segundo nivel ya con un amplio criterio. Que el especialista en observabilidad le explique amplia y claramente al usuario experto de segundo nivel la situación, e inclusive tenga la capacidad de sugerirle acciones correctivas con el fin de prevenir que la incidencia se vuelva repetitiva. También que tenga la capacidad de contactar la unidad usuaria y explicarle la situación.

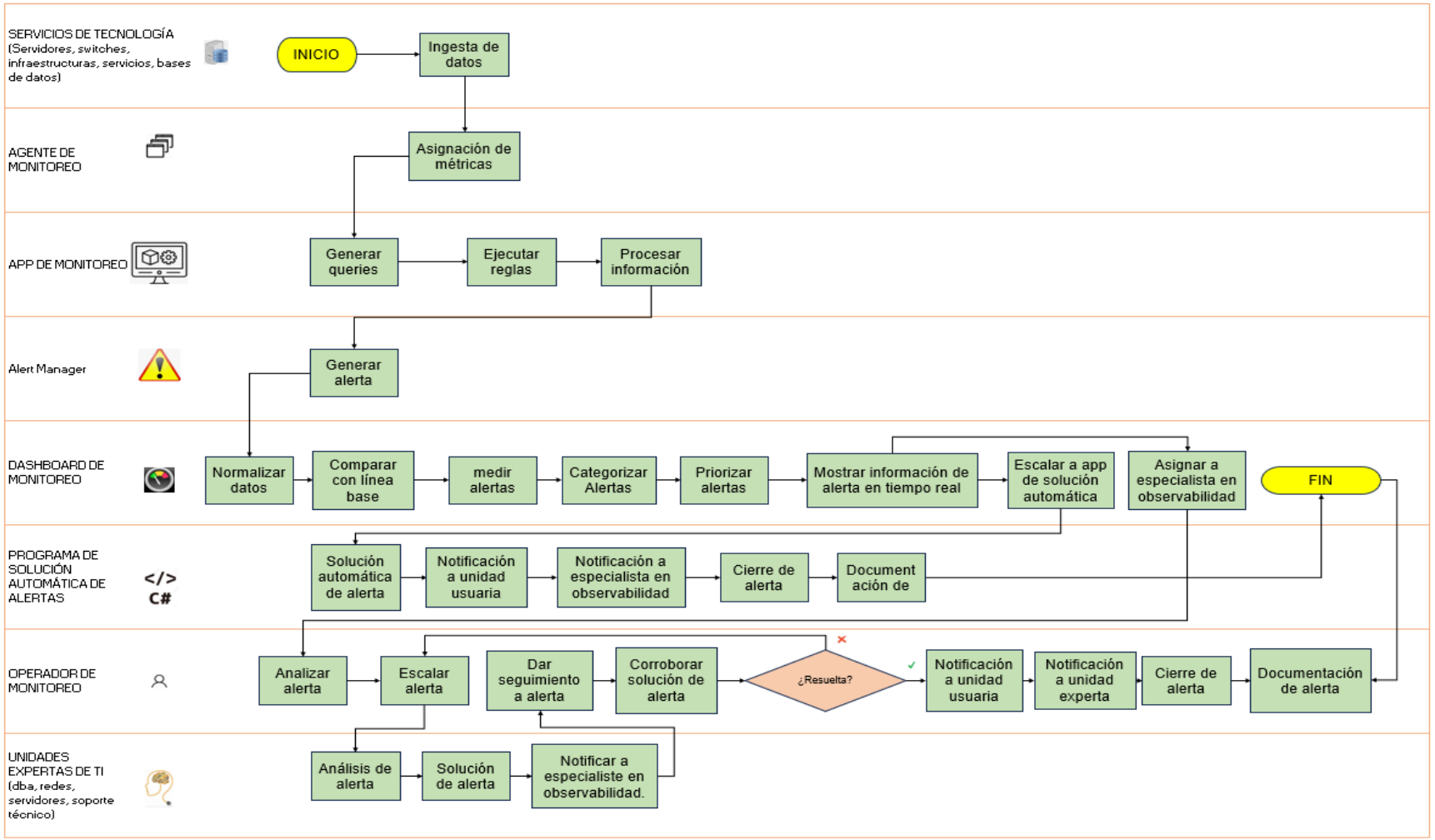
Por su parte, el analista de observabilidad, también deberá tener la capacidad de realizar un amplio análisis estadístico a la información almacenada en los repositorios. De manera que pueda identificar patrones, descubrir nuevos elementos, sugerir la creación de nuevos “BOT’s” capaces de apalear ciertas incidencias.

## 5.4. Diagrama de flujo por carriles

A continuación, se presenta una variante de nuevo el diagrama de flujos de bajo nivel. Esta diferencia radica en que el mismo está separado por carriles. Cada carril alude a las entidades involucradas en la realización de los procesos. Se toma en cuenta elementos automáticos, al especialista en observabilidad, usuarios expertos de segundos niveles.

**Ilustración 17**

*Diagrama de Flujo Por Carriles*



La imagen anterior, refuerza lo presentado en el punto anterior, con la diferencia de que se puede visualizar cada uno de los actores en cada proceso. Nótese que la mayoría de los procesos (19 procesos), son realizados de forma automática por las plataformas de monitoreo. Los 11 restantes, que se muestran a la derecha, corresponden a las acciones ejecutadas por el especialista en observabilidad, así como el experto de Nivel 2.

Nótese también que existe tres tareas ejecutadas por los expertos de segundos niveles. Para este punto, se propone modificar las bitácoras de las alertas, de forma que se documente la cantidad de escalamientos en caso de que un evento no sea solventado de forma integral.

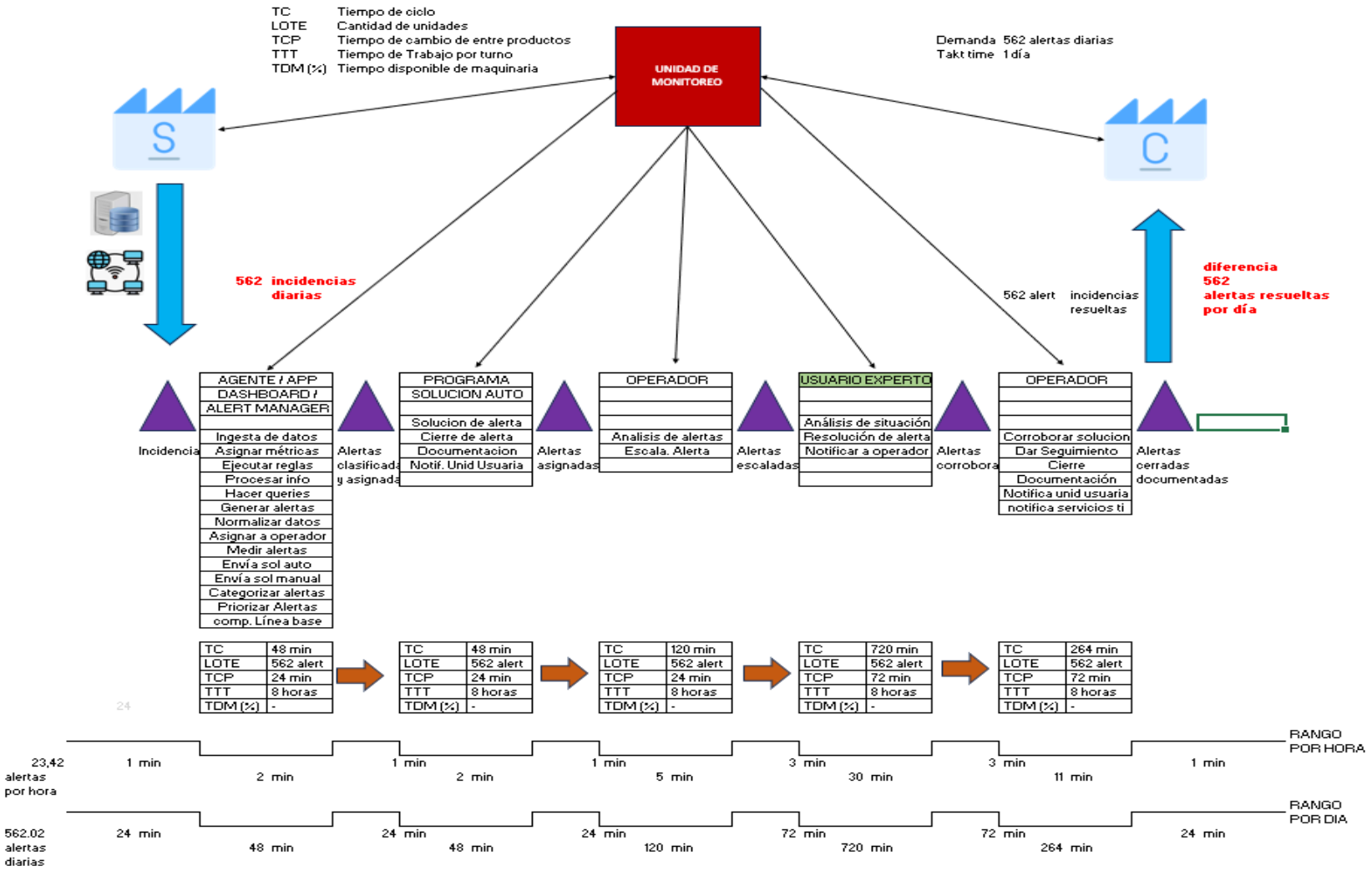
Se propone también una constante comunicación y coordinación entre los especialistas en observabilidad y los expertos de segundos niveles.

### 5.5. Mapa de cadena de valor situación deseada

De igual manera que se expuso en el Mapa de valor del Flujo de Procesos de la situación actual. Se presenta un Mapa de cadena de valor de la situación deseada mediante el cual se agrupa las tareas en cajas según los entes que las ejecutan. Las tareas automáticas están ubicadas en las dos primeras cajas. El resto de las cajas, contienen las tareas que debe ejecutar tanto el especialista en observabilidad, como el experto de segundos niveles. Si bien es cierto, que parece más trabajo, las tareas son puntuales y específicas, de forma que se pueda garantizar la calidad su atención.

**Ilustración 18**

*Mapa de Cadena de Valor Situación Deseada*



Tal como se muestra en la imagen anterior, esta modalidad de trabajo pretende generar valor por medio de la automatización de las resoluciones de los eventos. Se esperaría los siguientes beneficios:

1. Aumentar la capacidad instalada de la Torre de Observabilidad. Esto por cuanto, el especialista en observabilidad podrá tener más libertad y capacidad para atención de alertas.
2. Aumentar la velocidad de atención de incidencias. Gracias a la automatización de soluciones, Muchos eventos podrán solventarse casi de inmediato.
3. Aumentar la calidad y pertinencia de solución de incidencias. Al tratarse de BOT'S – RPA, los mismos se pueden programar según la necesidad.
4. Mejorar el rendimiento de la infraestructura de TI. Ya que muchas alertas serán atendidas de forma automática, muchas situaciones pueden ser corregidas casi de inmediato. Por ejemplo, picos de memoria y CPU en servidores.
5. Reducción considerable de costos. Esto por cuanto, ya no se dependería tanto de los especialistas en observabilidad ni de segundos o terceros niveles para la resolución de eventos.
6. Mejoramiento sustancial en la continuidad del servicio. Esto por cuanto al resolverse las alertas de una forma más expedita, se contribuye a que exista una mejor disponibilidad de las plataformas tecnológicas.
7. Implementar el servicio de la Torre Observabilidad de TI en algunas otras áreas o plataformas que estén descubiertas.

## 5.6. Matriz RACI

A continuación, se presenta una matriz RACI (Responsable, Apoderado, Soporte, Consultado, Informado), mediante la cual se muestra cada tarea y el responsable de ejecutarla.

**Tabla 14**

*Matriz RACI*

| **MANAGER** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **ACTIVIDAD DE CADA PASO DEL PROCESO OPERATIVO** | Infraestructura de TI | Agente de monitoreo | App de monitoreo | Alert Manager | Dashboard de | Aplicación de | Especialistas en observabilidad | Usuario experto |
| **Ingesta de Datos** | R | | | | | | | |
| **Asignación de métricas** | | R | | | | | | |
| **Generación de queries** | | | R | | | | | |
| **Ejecución de reglas** | | | R | | | | | |
| **Procesamiento de información** | | | R | | | | | |
| **Generación de alertas** | | | | R | | | | |
| **Normalización de datos** | | | | | R | | | |
| **Comparación con línea base** | | | | | R | | | |
| **Medición de alertas** | | | | | R | | | |
| **Categorización de alertas** | | | | | R | | | |
| **Priorización de alertas** | | | | | R | | | |
| **Mostrar información en tiempo real** | | | | | R | | | |
| **Escalamiento a aplicación de solución automática** | | | | | R | | I | |
| **Escalamiento a especialista de observabilidad** | | | | | R | | I | |
| **Análisis de alerta** | | | | | | | R/A | |
| **Escalamiento de alerta** | | | | | | | R/A | I |
| **Seguimiento de alerta** | | | | | | | R/A | I |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Corroborar solución** | | | | | | | R/A | C |
| **Notificación a unidad usuaria** | | | | | | | R/A | |
| **Notificación a especialista de nivel 2** | | | | | | | R/A | |
| **Cierre manual de alerta** | | | | | | | R/A | |
| **Documentación manual de alerta** | | | | | | | R/A | |
| **Solución automática de alerta** | | | | | | R | I | |
| **Notificación automática a unidad usuaria** | | | | | | R | I | |
| **Notificación automática a especialista de observabilidad** | | | | | | R | I | |
| **Cierre automático de la alerta** | | | | | | R | I | |
| **Documentación automática de alerta** | | | | | | R | | |
| **Análisis de alerta por parte de especialista de nivel 2** | | | | | | | | R/A |
| **Resolución de alerta por parte de especialista de nivel 2** | | | | | | | | R/A |
| **Notificación a especialista de observabilidad** | | | | | | | I | R/A |

Fuente: Autoría propia

Pareciera que existen muchos responsables para un solo proceso o que existe un cuello de botella ya que cada entidad tiene muchos procesos asignados. Esto hacer referencia específicamente al especialista de observabilidad, quien debe brindar una atención integral a las alertas generadas, así como mantener un seguimiento constante a la evolución de la atención de los incidentes. También el especialista en observabilidad debe asegurarse que el evento suscitado se haya resuelto correctamente.

Todos los especialistas de observabilidad, no solo son responsables por la correcta atención de las alertas, sino que deben apoyar al resto de compañeros del equipo de forma que el proceso general de resolución sea expedito y eficaz. Esto creará el blindaje y la agilidad necesaria para mantener la fluidez en atención de eventos e incidencias por parte del personal de la torre de observabilidad.

Con respecto a los procesos automatizados (primeras 6 columnas). Los mismos son responsables enteros de cada paso efectuado ya que son programas, BOT'S, funciones, disparadores, procedimientos almacenados**. El responsable por el correcto funcionamiento de dichas aplicaciones debe ser el jefe de la Torre de Observabilidad.

El responsable general de toda la torre de observabilidad es el mismo CEO de la firma Gosys Pro quien le da mantenimiento a toda la infraestructura de monitoreo, da soporte a los especialistas de observabilidad (pertenecientes al cliente).

## 5.7. Plantillas SOP

A continuación, se presenta una Plantilla de Procesos Operativos Estandarizados la cual trata de explicar los procesos de Observabilidad de una manera más profunda y detallada. Mencionando cada paso de la atención de alertas por incidencias de TI.

**Tabla 15**

*Procesos Operativos Estandarizados*

| | | |
|---|---|---|
| **Usuario Final**: Gosys Pro | | |
| **Objetivos para Gosys Pro:** | 1. Estandarizar proceso de monitoreo de TI<br>2. Mejorar tiempos de atención de alertas. (KPI, SLA, OLA)<br>3. Colaborar en la reducción de costos por atención de alertas.<br>4. Reducir cantidad de reprocesos. | |
| **Alcance y limitaciones: (straight forward)** | Los procesos en sí son lineales, solamente existe un bucle y pocos procesos heredados. Los mismos se enfocan en el procedimiento de atención de cada alerta. | |
| **Procedimiento** | | **Responsable** |

| | |
|---|---|
| Ingesta de datos<br>a. La infraestructura lanza información en logs de todas las tareas ejecutadas.<br>b. Las tareas se almacenan en un repositorio.<br>c. El repositorio queda para lectura del agente de monitoreo. | Servicios de Infraestructura de TI |
| Asignación de métricas<br>a. Lectura de la información de los repositorios.<br>b. Operaciones aritméticas sobre los datos.<br>c. Se ordena los datos según sus características. | Agente de monitoreo |
| Ejecución de queries<br>a. Se realiza consultas a la información recopilada.<br>b. Se ordena la información.<br>c. Se presenta la información.<br><br>Ejecución de reglas<br>a. Revisión de resultados de queries generados<br>b. En caso de que se cumpla una condición, activa un disparador o “trigger”<br><br>Procesamiento de información<br>a. Se ordena la información obtenida luego de queries y “triggers”<br>b. Se recopila y ordena para generar la alerta | Aplicación de monitoreo |
| Generación de alerta<br>a. Se recibe la información procesada<br>b. Se genera la alerta | Alert Manager |

| | |
|---|---|
| c. Se traslada alerta al Dashboard | |
| Normalización de datos.<br>a. Se excluye datos no importantes.<br>b. Se depura la información de las alertas<br><br>Comparación con línea base<br>a. Se compara la información contra los umbrales predefinidos<br>b. Se revela más información importante<br><br>Medición de alertas<br>a. Se asigna SLA's a las alertas<br>b. Se asigna KPI a las alertas<br>c. Se asigna OLA's a las alertas<br>d. Se asigna nivel de criticidad a las alertas.<br><br>Categorización de alertas<br>a. Se clasifica alerta según su tipo<br>b. Se clasifica alertas según criticidad<br>c. Se ordena las alertas según tipo<br>d. Se ordena alertas según criticidad<br><br>Priorización de alertas<br>a. Se revisa las alertas según tipo<br>b. Se revisa alertas según criticidad<br>c. Se acomodan en una cola según urgencia y prioridad<br>d. Se envían al Dashboard<br><br>Mostrar información de alertas<br>a. Se presenta la información en pantalla en tiempo real. | Dashboard de monitoreo |

| | |
|---|---|
| Escalar a la aplicación de resolución de incidencias<br>a. De acuerdo con ciertas programaciones, se envía la alerta a un programa de resolución automática.<br>b. El programa de resolución recibe la alerta<br><br>Escalar al especialista en observabilidad.<br>a. De acuerdo con ciertas circunstancias, el Dashboard genera un mensaje.<br>b. Se envía el mensaje a los especialistas de observabilidad. | |
| Recibe alerta escalada<br>a. Se recibe alerta escalada.<br>Solución automática de alerta<br>a. Se ejecuta sentencias, SQL y tareas programadas para solventar alerta.<br>Notificación a unidad usuaria<br>a. Si la incidencia es solventada, se procede con la notificación a las unidades usuarias<br>Notificación a unidad experta<br>a. Si la incidencia es solventada, se procede con la notificación a las unidades expertas<br><br>Cierre de alerta<br>a. El proceso de cierre consiste en dar por atendida la incidencia<br>b. Se envía al repositorio para documentación<br>Documentación de alerta<br>a. Se documenta alerta en repositorio. | Programa de solución automática de alertas |
| Análisis de alerta<br>a. Se realiza una revisión general del evento.<br>b. Se realiza un diagnóstico de la situación. | Especialista en observabilidad |

| | |
|---|---|
| c. Se genera un informe para notificar al especialista de segundo nivel<br><br>Escalamiento de alerta<br>a. Con la información recopilada, se crea tarea para especialista de segundo nivel experto.<br>b. Se notifica a especialistas de nivel experto. | |
| Análisis de alerta<br>a. Se realiza una revisión general del evento.<br>b. Se revisa el diagnóstico de la situación.<br><br>Solución de incidencia<br>a. Se ejecuta todas las acciones para solventar la incidencia reportada.<br>b. Se genera un informe para notificar al especialista en observabilidad.<br><br>Notificación a especialistas en observabilidad<br>a. Se envía el informe para notificar al especialista en observabilidad.<br>b. Se documenta en bitácora. | Usuario experto de segundo nivel |
| Seguimiento a alerta<br>a. Mientras la incidencia es resuelta por el experto de segundo nivel, el especialista en observabilidad, se mantiene al tanto y en una constante comunicación.<br><br>Corroborar solución de alerta<br>a. Cuando el usuario experto de segundo nivel responde la tarea, el especialista en observabilidad, debe corroborar con la unidad usuaria que la incidencia haya sido solventada.<br>i. En caso de que sí sea solventada, se procede con los siguientes pasos. | Especialista en observabilidad |

| | |
|---|---|
| ii. En caso de que no sea solventado, se vuelve a escalar a experto de nivel 2.<br><br>Notificación a unidad usuaria<br>a. Si la incidencia es solventada, se procede con la notificación a las unidades usuarias<br><br>Notificación a unidad experta<br>a. Si la incidencia es solventada, se procede con la notificación a las unidades expertas<br><br>Cierre de alerta<br>a. El proceso de cierre consiste en dar por atendida la incidencia<br>b. Se envía al repositorio para documentación<br><br>Documentación de alerta<br>a. Se documenta alerta en repositorio. | |

Nótese que, en la tabla anterior, las tareas se desglosan en pequeños pasos más puntuales y específicos. De esta forma, se podrá detectar cuellos de botella o fallos en el flujo de atención de las incidencias de una forma más precisa y proceder con acciones correctivas de una manera más expedita.

Esta última tabla también se convierte en guía óptima para que el CEO de la firma Gosys Pro, en conjunto con su equipo de trabajo, realicen la introspección correspondiente y procedan con la creación de los manuales estandarizados necesarios para documentar su proceso de observabilidad y por consiguiente, alcanzar un nivel de estandarización.

## 5.8. Beneficios esperados en cumplimiento con el marco Cobit 2019

Si se crea los manuales para los especialistas en observabilidad con base en las herramientas mostradas anteriormente, el personal de Gosys Pro estará en capacidad de:

1. Cumplir con lo estipulado en el dominio DSS01 ya que todo el proceso de atención de alertas estará debidamente documentado y explicado.
2. Una mejora sustancial en el proceso de identificación, clasificación, priorización y atención general de incidentes, lo cual estará acorde con el DSS02.
3. Una resolución más expedita y sencilla de problemas e incidentes ya que se tendrá en todo momento el conocimiento, las trazas y toda la información a la mano. Esto cumplirá con las estipulaciones del DSS03.
4. Permitir un mejor aseguramiento de la continuidad de los servicios de TI ya que la Torre de Observabilidad será proactiva en la prevención de incidentes. Lo cual estará alineado con el DSS04.
5. Permitirá propiciar a que el cliente invierta en la mejora de sus infraestructuras y servicios, lo cual indiscutiblemente mejorará su rendimiento. (MEA01)
6. Permitirá mejorar el rendimiento de la Torre de Observabilidad ya que la misma será más proactiva y expedita en la atención de las alertas. (MEA01)
7. Será de gran ayuda para la creación de nuevos procesos paralelos de gran importancia para la atención no solo de alertas, sino de requerimientos de servicio. Por ejemplo, una unidad de soporte remoto. (DSS02)

Todos estos beneficios serán resultado de todas las acciones que se realicen en pro de la tan deseada estandarización de los procesos de Monitoreo y Observabilidad de la organización Gosys Pro.

## 5.9. Recomendaciones para el patrocinador.

A continuación, se presenta una serie de sugerencias y recomendaciones para que el personal de la firma Gosys Pro, pueda tomar las decisiones pertinentes en busca de mejorar sus servicios de Monitoreo y Observabilidad:

1. Crear la mayor cantidad posible de BOT's, RPA's y aplicaciones que puedan resolver incidencias de manera automatizada para aumentar la velocidad y calidad de atención de incidencias.
2. Adoptar modelos de metodologías ágiles y mantener sesiones frecuentes (sprint) que sirvan para estar al día y alineados en el proceso de Observabilidad de TI.
3. Revisar y actualizar la línea base y los umbrales en los sistemas de monitoreo, de forma que se pueda filtrar mejor las incidencias y dar mayor prioridad a las que son verdaderamente importantes.
4. Crear manuales estandarizados basados en los SOP's desarrollados con el fin de documentar los procesos.
5. Evaluar la forma de obtener licencias, hosts y herramientas más económicas, lo cual permita un ahorro sustancial.
6. Revisar y evaluar las políticas de gestión del talento humano.

Tomando en cuenta lo anterior, se logrará una mejora sustancial en la calidad de atención de alertas, reducción de tiempos de resolución de eventos, aprovechamiento máximo de los recursos destinados al proceso de Observabilidad de TI.

# Capítulo VI: CONCLUSIONES Y RECOMENDACIONES

## 6.1. Conclusiones.

Una vez realizado el presente trabajo final de investigación, se presentan las conclusiones, las cuales sirven para dar continuidad al proceso de mejora continua según lo plantea el ciclo DMAIC.

El objetivo principal de este documento consiste en el rediseño del proceso de Monitoreo de Infraestructura de TI ofrecido por la empresa Gosys Pro para propiciar un grado de estandarización según las sanas prácticas del marco Cobit 2019 con base en la metodología Lean Six Sigma. El mismo se logró gracias a la aplicación de las herramientas del ciclo DMAIC, principalmente la Matriz RACI y los Procedimientos Operativos Estandarizados (SOP's), las cuales permitieron construir un nuevo modelo de atención de alertas por eventos.

Se cumplió el objetivo específico de diagnosticar la situación actual del proceso de monitoreo de TI, el cual reveló la inexistencia de manuales y procedimientos estandarizados y ejecución de tareas de forma empírica, y utilización de costosas infraestructuras de monitoreo. Lo cual, se ve reflejado en el alto costo de atención de incidencias ($3.75 por incidencia). No obstante, sí existe un compromiso real por mantener la correcta continuidad del servicio, así como una correcta resolución de incidencias en plazos inferiores a 1 hora (92% de los incidentes).

Se cumplió el objetivo específico de identificar la situación deseada para establecer las brechas y proponer un cambio sustancial en la ejecución de los procesos de Monitoreo de Infraestructura de TI. Se presentó un desglose mucho más profundo de las tareas a realizar (30 tareas más puntuales) de manera que se pueda automatizar al máximo su ejecución. También se propone un cambio de cultura para propiciar que un operador de monitoreo pase a ser un especialista en observabilidad, quien deja de ser un pasador de casos y se convierte en un especialista con capacidades de diagnosticar, evaluar, analiza y hasta resolver incidencias. Se

colocó una Matriz RACI y unos Procedimientos Operativos Estandarizados (SOP's), los cuales permitirán resolver las incidencias de una forma integral, metódica y ordenada.

Se logró el objetivo específico de rediseñar el proceso de Monitoreo de Infraestructura de TI. De forma que exista más proactividad e inteligencia para resolver incidencias. Se propusieron múltiples sugerencias en pro de la automatización de algunas tareas que actualmente se ejecutan de forma manual (Creación de BOT's y RPA's), así como hacer énfasis el repositorio conocimiento para que los operadores de monitoreo puedan prevenir los eventos y evitar que se materialicen los riesgos inherentes a la interrupción de la continuidad de los servicios.

Se alcanzó el objetivo específico de transferir el conocimiento al departamento de Informática de la firma Gosys Pro, ya que el CEO de dicha compañía, ha estado al tanto de todo el proceso de desarrollo de este trabajo. De igual manera, el patrocinador recibirá una copia completa de este documento, lo cual será de utilidad para su análisis retrospectivo y la ejecución de las acciones respectivas con el fin de obtener las mejoras correspondientes y llegar a una excelencia operativa.

Los entregables de este documento, permitieron cumplir con el objetivo de esbozar las recomendaciones para la ejecución de un nuevo ciclo DMAIC. Esto debido a que se desea alcanzar un modelo de excelencia operativa en el proceso de Monitoreo de Infraestructura de TI. Dicha excelencia operativa se obtendrá gracias a un proceso constante de mejora continua y mejoramiento del control interno, según cita la metodología Lean Six Sigma en su apartado de Control y Seguimiento.

## 6.2. Recomendaciones.

En congruencia con las conclusiones anteriores, se procede a brindar las recomendaciones para la corporación Gosys Pro.

Se recomienda a la alta gerencia, crear un plan de acción que permita aplicar las mejoras propuestas en este documento para materializar el rediseño al proceso de Monitoreo de Infraestructura de TI.

Se recomienda a la gerencia comparar la situación actual con la situación deseada, para que se logre neutralizar la causa raíz del problema, identificar las acciones correctivas y priorizar su aplicación.

Se recomienda a la gerencia de TI, estudiar a fondo el apartado de la Situación Deseada, así como las herramientas aplicadas en dicho capítulo. Para calendarizar la aplicación de las correcciones según su priorización. Se recomienda comenzar por la automatización de las tareas más simples y repetitivas.

Se recomienda a las autoridades correspondientes diseñar los manuales operativos para la Unidad de Monitoreo de TI basados en la matriz RACI y los SOP’s. Para obtener la estandarización de los procesos operativos del NOC. Estos serán el pilar fundamental para la creación del conocimiento que será perdurable y transmitible hacia futuros colaboradores.

Se recomienda al personal gestor de Talento Humano crear un programa de capacitación, reuniones y retroalimentación con los manuales estandarizados para que el personal de la unidad de monitoreo trabaje de una manera uniforme y estandarizada.

Se recomienda a todo el personal de Gosys Pro, diseñar un plan de mejora continua (Ciclo DMAIC) y comprometerse con su realización periódica. Para mantener no solo la estandarización de los procesos, sino una excelencia operativa.

Se recomienda a la compañía Gosys Pro, tomar este documento completo como base y parámetro para ejecutar su implementación en otras áreas operativas del negocio y así obtener una Excelencia Operacional que le permita estar alineada no solo con el marco de sanas prácticas Cobit 5, sino con otras metodologías similares de la industria. Por ejemplo, ITIL Normas ISO.

# Capítulo VII: Apéndices

## 7.1. Bibliografía

Alcalde San Miguel, Pablo. *Calidad fundamentos, herramientas y gestión de la calidad para pymes*. 3° Edición.

Amendola, Luigi. *Excelencia Operacional y Mejora Continua. ¿Cómo implementar?* https://www.youtube.com/watch?v=TdMXAcYivmw.

Axelos. *ITIL Foundation EDITION*. https://fliphtml5.com/ensds/cphj/basic

Camacho Villalobos, María Elena, 1954- *Guía para la elaboración y presentación del trabajo final de graduación*. -- 1. ed.-- Heredia, C.R. Universidad Nacional. Centro de Investigación y Docencia en Educación, 2014.

Colegio de Morelos. *Lineamientos para anteproyecto*. http://elcolegiodemorelos.edu.mx/lineamientos-para-anteproyecto/

Cortés, Andrés Alberto. *EVALUACIÓN POR MEDIO DE COBIT 2019, DEL MODELO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA MUNICIPALIDAD DE CARRILLO, PRODUCTO DE LOS PROCESOS DE MIGRACIÓN DE SISTEMAS OPERATIVOS E INFORMÁTICOS*. Tesis 2021

Gutiérrez Pulido, Humberto. *Calidad Total y Productividad*. Cuarta Edición. Editorial Mc Graw Hill. 2014

Hernández Sampieri, Roberto. *Metodologías de la Investigación*. 4ta Edición. Editorial Mc Graw Hill 2019.

MT Solutions. *Monitoreo y Observabilidad TI: conceptos claves para 2023*. https://www.mt2005.com/monitoreo-observabilidad-conceptos-claves-2023/

Mora Tavarez, José Manuel. *Diseño y Evaluación de un Proceso de Monitoreo de Operaciones y Control de Métricas de Servicios de TI*. Tesis. 2014

Navarro, Carlos. *Memoria del Proyecto*. Universidad Oberta de Cataluña.

Parra, Luis Diego. *Desarrollo de una herramienta informática mínima viable que agilice el proceso de extracción de información de la aplicación ETA en la empresa Claro CR Telecomunicaciones S.A*. Tesis. 2022

Pyzdek, Tomas. *SIGMA PROJECT PLANNER*. Pag xvi

Ritegno, Eduardo. *COBIT 2019*. Pag 17. https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

Salas, Ronaldo. *Propuesta Monitoreo*. 2020

Sánchez, Carlos. *Normas APA – 7ma (séptima) edición*. https://normas-apa.org/

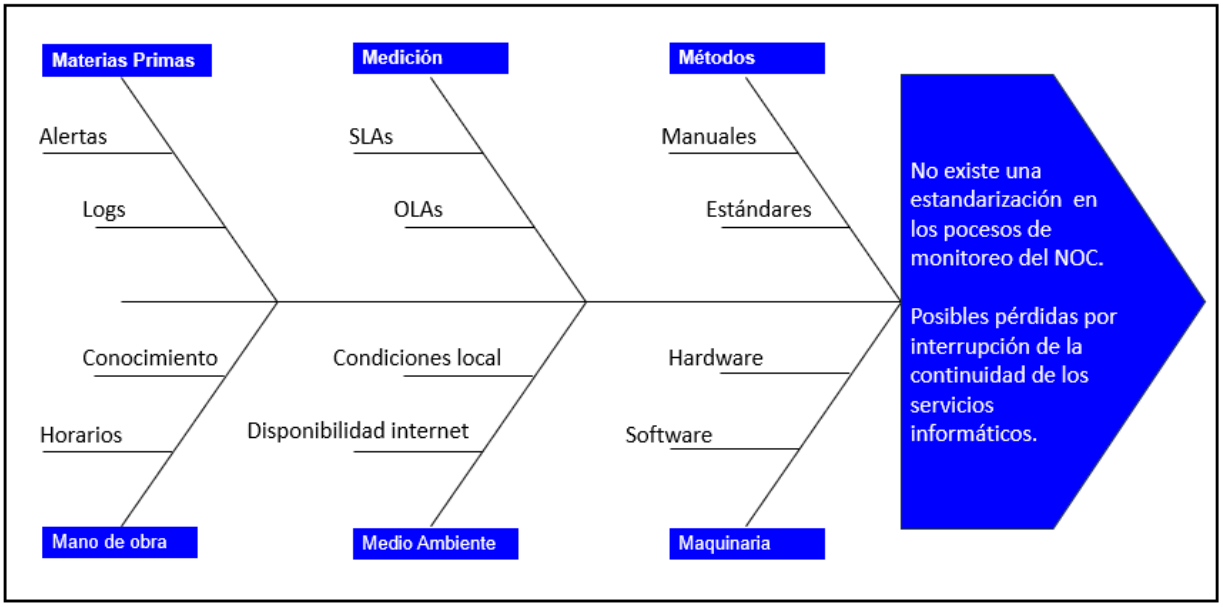
Ulate, I. y Vargas, E. (2012). *Metodología para elaborar una tesis como trabajo final de graduación*. (1ª. Ed.). Costa Rica San José, Editorial Universidad Estatal a Distancia.

Villamizar, Carlos. *¿Qué es COBIT y para qué sirve?* https://www.globalsuitesolutions.com/es/que-es-cobit/

## 7.2. Anexos

### 7.2.1. Anexo 1. Posibles Causas del problema según diagrama de Ishikawa

Se adjunta algunos primeros hallazgos sobre eventuales causas del problema.




Materias primas

Las materias primas son todas las alertas generadas por los eventos e incidencias reportadas.

Medición

La medición básicamente son los SLA’s, KPI’s y OLA’s a la hora de resolver las incidencias. Se miden en unidades de tiempo (horas, minutos, segundos).

Se toma en cuenta otros dos valores importantes como la criticidad de las incidencias, así como el costo por atención de cada alerta.

Métodos

En este momento no existe manuales documentados, se pretende que la información saliente de este documento sirva como insumo para la creación de los manuales correspondientes.

Mano de obra

Además del CEO de Gosys Pro, existen seis operadores de monitoreo, los cuales cubren las 24 horas, los 365 días del año.

Medio Ambiente

Corresponde a las oficinas donde se ubica Gosys Pro, la cual cuenta con buena ventilación e iluminación. Dentro de una casa de habitación que, a su vez, tiene su domicilio dentro de un condominio, por lo que goza de buena seguridad. Tienen una conexión a internet de hasta 100mbs.

Maquinarias

El CEO cuenta con un equipo personal, lo mismo que los operadores. Todos se conectan por medio de VPN a los servidores alojados en la nube.

### 7.2.2. Anexo 2. Entrevista con el CEO de Gosys Pro

El objetivo del presente cuestionario consiste en conocer y describir el proceso de monitoreo de TI y cómo el mismo es desarrollado por parte de la empresa Gosys Pro.

La información obtenida será utilizada con fines investigativos y académicos por lo que se manejará con la máxima confidencialidad. No se solicitará información de carácter estratégico tal como nombres de servidores, direcciones IP, información financiera, nombre del personal.

Solicito encarecidamente ser lo más amplio posible a la hora de responder, para así poder tener un mayor conocimiento y poder desarrollar un análisis más crítico y objetivo.

En caso de que alguna pregunta pueda ser comprometedora, favor abstenerse de responder.

1. ¿Qué es Gosys Pro?, ¿cuándo nació?, ¿cuál es su nicho de mercado?

Gosys Pro es una empresa nacional dedicada al desarrollo de soluciones de TI principalmente en el área de monitoreo. Fue fundada en el año 2018.

Actualmente contamos con un Gerente-Propietario, dos desarrolladores y una persona encargada del área administrativa. De 6 operadores subcontratados quienes son analistas de observabilidad para el desarrollo de sus labores en el Centro de Operaciones en Monitoreo (NOC).

Nos especializamos en desarrollo de soluciones de monitoreo de infraestructuras de software y hardware, brindamos soporte a empresas del mercado financiero y además trabajamos bajo modelos de proyectos personalizados para grandes y pequeñas empresas.

Gosys Pro es un claro ejemplo del potencial que posee Costa Rica en el impulso a las pequeñas y medianas empresas. Emprendedores que se lanzan al mercado nacional y logran establecer su propio camino.

La historia de Gosys Pro es la historia de una idea que nace en el año 2018, de la mano de un grupo de ingenieros con una visión clara: brindar soluciones tecnológicas de calidad a empresas de toda la región centroamericana. Así nace Mirmecos, una empresa dedicada en un principio al soporte técnico, que pronto se da cuenta de que hay una oportunidad de innovar en el mercado de servicios de monitoreo y observabilidad de sistemas de IT.

Nuestro nicho de mercado se puede establecer en empresas medianas y grandes que cuenten con una infraestructura critica de IT, de igual forma no dejamos fuera las pequeñas empresas que requieran de nuestros servicios.

Además, de la mano de un desarrollador, estamos iniciando un proyecto de gestión de empresas tipo ERP con herramientas de Software libre.

2. ¿Qué es Monitoreo de Infraestructura de TI?

El monitoreo de infraestructura de TI es el proceso de supervisar y registrar continuamente el rendimiento y la disponibilidad de los componentes de la infraestructura de tecnología de la información de una organización. Esto puede incluir servidores, redes, aplicaciones, bases de

datos, dispositivos de almacenamiento y otros recursos de TI críticos. El objetivo principal es detectar problemas y anomalías de manera proactiva para garantizar que los sistemas funcionen de manera eficiente y minimizar el tiempo de inactividad.

El proceso de Monitoreo de Infraestructura de TI comprende los siguientes elementos:

- Uno o varias herramientas de monitoreo de los servicios de TI. Dichas herramientas recopilan y documentan automáticamente y en tiempo real el estado de salud de los sistemas y redes.
- Operadores de Monitoreo son las personas que utilizan dichas herramientas para documentar los eventos y alertar al personal de las áreas competentes para solventar las incidencias ocurridas.
- Hardware, servidores, switches y demás maquinaria que tenga instalados los sistemas de Monitoreo. Pueden ser locales o estar alojados en la nube.
- Un protocolo que contiene las instrucciones y procedimientos para tratar las incidencias ocurridas.
- Un repositorio o bitácora que almacena la información de todas las alertas ocurridas.

Estas son las funciones principales de una unidad de monitoreo:

- Monitorear la red, los servidores y las aplicaciones para la salud y el rendimiento
- Analizar el ancho de banda e identificar proactivamente los cuellos de botella
- Monitorear y analizar continuamente las amenazas y los ataques a la seguridad
- Modificar las configuraciones de la red según las necesidades de la empresa
- Detectar y soluciona rápidamente los fallos para reducir el tiempo medio de reparación.

3. En ocasiones anteriores, usted ha mencionado que más que monitoreo, se trata de Observabilidad. ¿Qué es observabilidad según sus palabras?, ¿Cuál es la diferencia entre Monitoreo y Observabilidad?

La observabilidad es un concepto más amplio que el monitoreo y se refiere a la capacidad de comprender y depurar sistemas complejos y distribuidos. Implica la recopilación de datos detallados y significativos de diferentes partes de un sistema para proporcionar una visibilidad completa de su funcionamiento interno. La observabilidad se enfoca en obtener información detallada y contextualizada que permita a los equipos de operaciones y desarrollo comprender mejor el comportamiento de los sistemas, identificar problemas y tomar medidas correctivas de manera eficaz.

La diferencia clave entre monitoreo y observabilidad radica en el enfoque en la profundidad y la riqueza de los datos recopilados. La observabilidad se centra en proporcionar datos más detallados y contextuales para comprender mejor el sistema, mientras que el monitoreo a menudo se enfoca en alertar sobre métricas específicas o umbrales predefinidos.

4. ¿Podría enumerar y explicar qué tipos de eventos y alertas de monitoreo de TI son atendidas por Gosys Pro?

Cualquier evento o fallo en el sistema puede generar una alerta. Son muchos tipos de alertas que hemos identificado. Principalmente pérdidas de paquetes a la hora de hacer un “ping”, o bien caída de servicios ya sea por fallos en el servidor o fallos de red, suelen ser los más frecuentes.

También se reconocen fallos en procesos ya sea por saturación de memoria o “bugs” en la programación o implementación de los sistemas.

5. ¿Cuáles son los tipos de eventos o alertas más recurrentes?, ¿Con qué frecuencia ocurren?

Por día se registran más de 500 alertas y hay de todo. Sin embargo, las más comunes son las caídas de enlaces de puntos de venta, “overflow” en los procesos, saturación de memorias y CPU, fallos y caída de la página de internet.

6. ¿Cuáles son los tipos de eventos o alertas más críticos?, ¿Con qué frecuencia ocurren?

Casi todos son críticos ya que de ellos depende la continuidad del servicio. Nuestro cliente es una empresa comercial que administra el parque tecnológico a una cadena de tiendas a nivel de américa latina, por lo que cualquier fallo corta dicha continuidad.

De los eventos más críticos que atendemos con mucha frecuencia, puedo enumerar los siguientes:

- Caída de enlaces con puntos de ventas.
- Fallos en aplicaciones IIS.
- Errores en páginas web de cara a los clientes finales.
- Colapsos por picos de uso memoria en los servidores.

7. ¿Bajo qué parámetro se mide la criticidad de las alertas?

Básicamente las pérdidas por interrupciones en la continuidad del servicio, depende de varios factores. Por ejemplo, tiempo que se dura en resolver un evento, cuál es el servidor que falla. No es lo mismo que se caiga el enlace con una tienda a que el mainframe falle.

Es muy relativo y hay muchas razones. La mayoría de las alertas son de alto impacto o críticas. Hay muy pocas de menor intensidad.

8. ¿Existe algún orden de prioridad para la atención de eventos?, ¿Cuáles tipos de eventos son prioritarios?

Siempre se atiende primero las alertas de máxima criticidad y máximo impacto. Por ejemplo, la caída de servidores de facturación, bases de datos de productos, bases de datos de clientes. A grandes rasgos, casi todas las alertas son prioridad, por tratarse de un entorno comercial con servicio a una cadena de tiendas.

9. Con respecto a los eventos o alertas. Mencione los elementos más importantes que comprenden cada alerta, su documentación y tratamiento.

Nos fijamos mucho en la criticidad y el tiempo para resolverlas. Entre más rápido, mejor.

10. ¿Existe algún “machote” o guía que sirva para documentar las alertas?

Las herramientas de monitoreo que utilizamos generan unos logs, en ellos aparece la información general de las incidencias, te voy a pasar una muestra para que la revises. Básicamente

nos fijamos en la hora de inicio, criticidad, servicio afectado, quién se encarga de darle seguimiento o resolver la incidencia y documentar. Como el servicio que ofrecemos es meramente de monitoreo y observabilidad, el cliente es quien debe encargarse por dar mantenimiento a su infraestructura. Nosotros hacemos todo lo posible para coordinar el restablecimiento del servicio afectado.

11. Favor explicar o mencionar algún punto importante concerniente al proceso de monitoreo desarrollado por su organización.

El plus que nosotros ofrecemos es que nuestras herramientas son de mucha calidad, pero de software libre. Por lo tanto, eso abarata mucho los costos para el cliente.

Tenemos mucha experiencia, hemos trabajado en el pasado para compañías como Sonda, GBM, CMA.

12. ¿Usted nos facilitaría una muestra de logs de monitoreo? Si se pudiera en un rango de cuatro meses, mucho mejor. Es con la intención de realizar un análisis general.

Claro, con mucho gusto te puedo bajar el log y pasártelo.

### 7.2.3. Anexo 3. Ejemplo de bitácora de monitoreo

Se extrajo un listado de Excel con más de 67 mil eventos. No obstante, ésta es la estructura general de cada una de las alertas:

INDEX: 9711

Message: ** PROBLEM Host Alert: XX-XXX-XX-XXXXX-XXXXX is DOWN **

Priority: Critical

Tags: XX-XXX-XX-XXXXX-XXXXX

Created At Time: 4/9/2023 21:51

Acknowledged By: ***** *******

Time to acknowledge: 10h 54m 35s

Closed By:

Time to Close:

Status: Acknowledge

Owner:

Source: ********

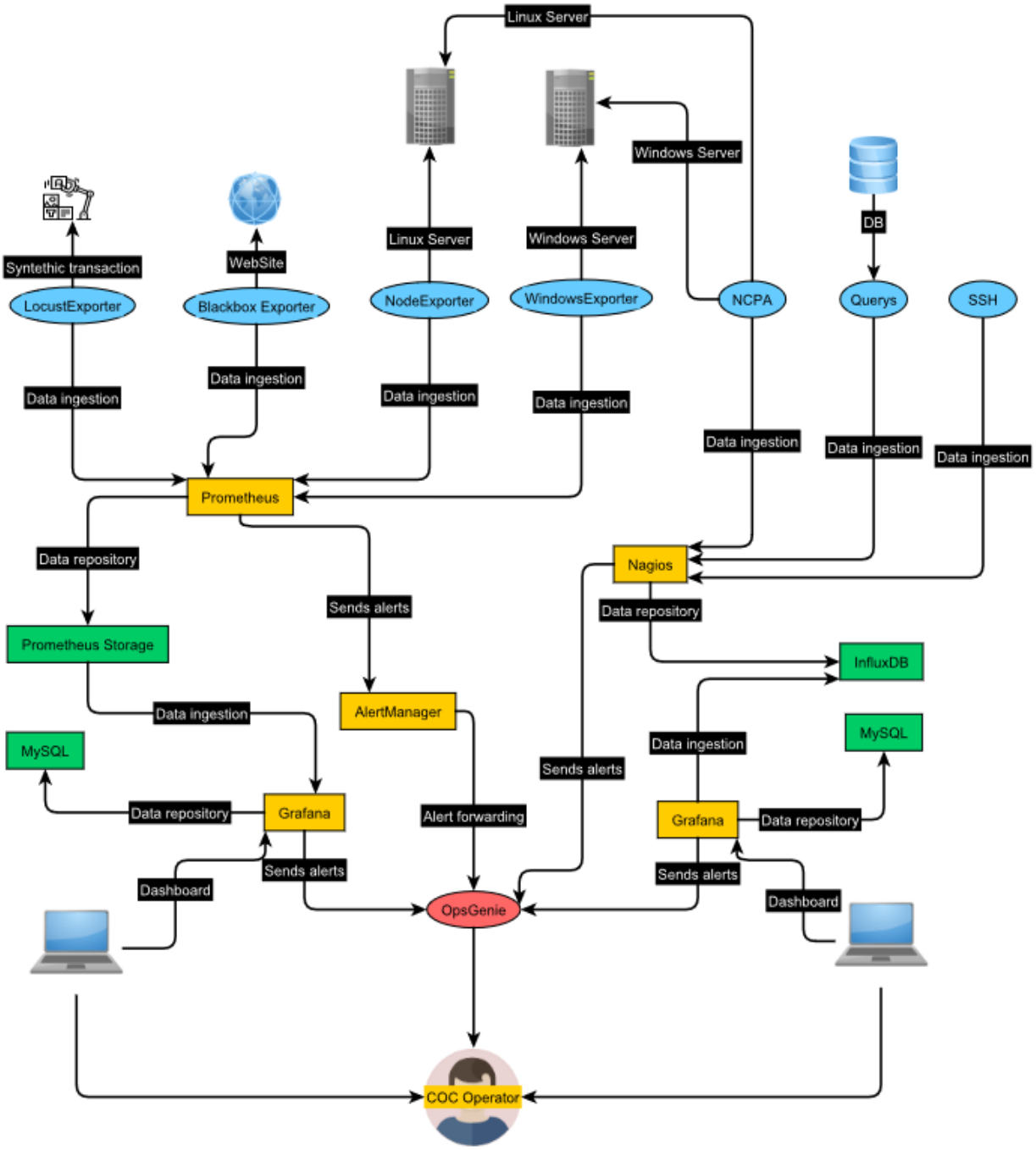
Duplication Count:

ID: a767fbac-b9e3-497f-aa32-18c14631fe58-1693885863709

Teams: CCC

Fuente: Salas, Ronaldo. Servicio de Monitoreo.pdf (2023)

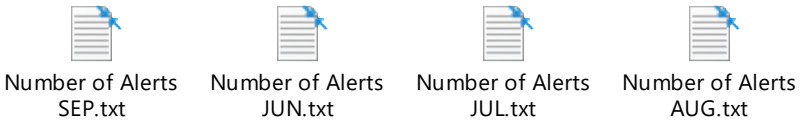
7.2.4. Anexo 4. Estructura general del proceso de monitoreo




Fuente: Salas, Ronaldo. Servicio de Monitoreo.pdf (2023)

### 7.2.5. Anexo 5. Archivos adjuntos con bitácoras

Los siguientes archivos son un compilado de las alertas reportadas durante el cuatrimestre analizado (junio a septiembre 2023).



### 7.2.6. Anexo 6. Consultas SQL sobre las bitácoras analizadas

Las sentencias SQL presentadas a continuación, se utilizaron para la creación del Mapa de Cadena de Valor de la Situación Actual, presentado en el punto 4.3 de este documento.

```
select COUNT(*) WindowsServerService from SEPTEMBER
WHERE
message like '%windowsserverservice%'
```

```
select COUNT(*) IIS from SEPTEMBER
WHERE
message like '%iis%'
```

```
select COUNT(*) WindowsServerMemory from SEPTEMBER
WHERE
message like '%windowsservermemory%'
```

```
select COUNT(*) WindowsServerDiskSpace from SEPTEMBER
WHERE
message like '%WindowsServerDiskSpace%'
```

```
select COUNT(*) SiteHTTPFailure from SEPTEMBER
WHERE
message like '%SiteHTTPFailure%'
```

```
select COUNT(*) PrometheusAlertmanagerJobMissing from SEPTEMBER
WHERE
message like '%PrometheusAlertmanagerJobMissing%'
```

```
select COUNT(*) PrometheusAllTargets from SEPTEMBER
WHERE
message like '%PrometheusAllTargets%'
```

```
select count(*) PingCritical
from SEPTEMBER
WHERE
Message LIKE '%ping is critical%'
```

```
select COUNT(*) Swap
from SEPTEMBER
where
Message like '%swap%'
```

```
select COUNT(*) ncpalistener
from SEPTEMBER
where
Message like '%ncpalistener%'
```

```
select COUNT(*) ncpapassive
from SEPTEMBER
where
Message like '%ncpapassive%'
```

```
select COUNT(*) CheckSystemLog
from SEPTEMBER
where
Message like '%Check System Log%'
```

```
select COUNT(*) ProccessCMD
from SEPTEMBER
where
Message like '%Process cmd%'
and
Message not like '%sophos%'
and
Message like '%sql%'
```

```
select COUNT(*) ProcessCount
from SEPTEMBER
where
```

```
Message like '%process count%'
```

```
SELECT COUNT(*) AppPool FROM SEPTEMBER
where
message like  '%AppPool%'
```

```
select COUNT(*) CPUusage from SEPTEMBER
WHERE
message like '%cpu usage%'
```

```
SELECT COUNT(*) EnlacesDown FROM SEPTEMBER
where
message like '%enlace%'
and
message like '%IS DOWN%'
```

```
SELECT COUNT(*) EnlacesCritical FROM SEPTEMBER
where
message like '%enlace%'
and
message like '%PING IS CRITICAL%'
```

```
SELECT COUNT(*) HostDown FROM SEPTEMBER
where
message like  '%host alert%'
and
message like  '%is down%'
and
message not like '%enlace%'
```

```
select COUNT(*) Sophos
from SEPTEMBER
where
Message not like '%Process cmd%'
and
Message like '%sophos%'
and
Message not like '%sql%'



select COUNT(*) SQLMessages
from SEPTEMBER
where
Message not like '%Process cmd%'
and
Message not like '%sophos%'
and
Message like '%sql%'



select COUNT(*) WriteBytes
from SEPTEMBER
where
Message like '%write_bytes%'


select COUNT(*) WriteTime
from SEPTEMBER
where
Message like '%write_time%'


select COUNT(*) ReadBytes
from SEPTEMBER
where
Message like '%Read_bytes%'


select COUNT(*) ReadTime
from SEPTEMBER
where
Message like '%Read_time%'



select COUNT(*) MemoryUsage
from SEPTEMBER
where
Message like '%memory usage%'



select count(*) CheckLogical from SEPTEMBER
WHERE
MESSAGE LIKE '%Check logical%'
```

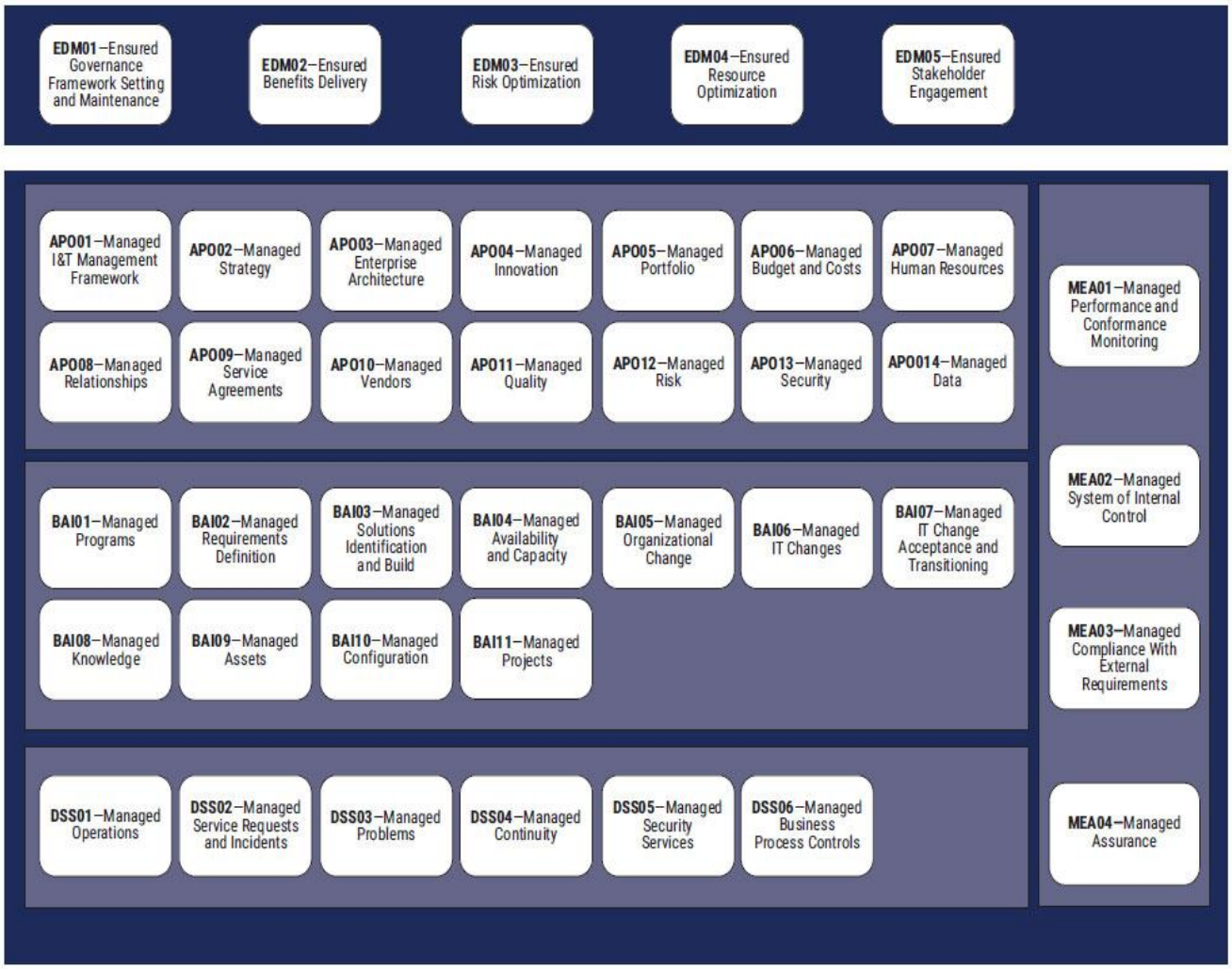
```
select count(*) Check_Uptime from SEPTEMBER
WHERE
MESSAGE LIKE '%Check Uptime%'


select count(*) Check_Failed_Jobs from SEPTEMBER
WHERE
MESSAGE LIKE '%Check_Failed_Jobs%'

select count(*) TotalProcesses from SEPTEMBER
WHERE
MESSAGE LIKE '%Total Processes%'


SELECT COUNT(*) CheckService
FROM SEPTEMBER
WHERE
MESSAGE LIKE '%Check Service%'
and
Message not like '%sop%'
and
Message not like '%sql%'
and
Message not like '%mss%'

select count(*) ADQ_RELAY from SEPTEMBER
WHERE
MESSAGE LIKE '%ADQ relay%'


select count(*) OriginationRule from SEPTEMBER
WHERE
MESSAGE LIKE '%OriginationRule%'
```

### 7.2.7. Anexo 7. Información de alertas procesadas

Luego de procesar la información contenida en el Anexo 5, por medio de las sentencias SQL contenidas en el Anexo 6; se obtuvo los resultados que se presentan en los archivos siguientes:


La información estadística de este apartado es utilizada para crear el Mapa de Flujo de Valor de la Situación Actual, descrita en Capítulo 4.

## 7.2.8. Anexo 8. Objetivos dominios Cobit 2019




Fuente: ISACA (2018)

### 7.2.9. Anexo 9. Actividades Cobit 2019

Listed below are the activities associated with each of the governance and management practices in COBIT® 2019.

The activities are sorted in the order in which they appear in COBIT® 2019 Framework: Governance and Management Objectives.

| Area | Domain | Objective ID | Objective | Practice ID | Practice Name | Activity |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.01 | Perform operational procedures. | 1. Develop and maintain operation procedures and related activities to supp all delivered services. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.01 | Perform operational procedures. | 2. Maintain a schedule of operation activities and perform the activities. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.01 | Perform operational procedures. | 3. Verify that all data expected f processing are received and process completely, accurately and in a time manner. Deliver output in accordance wi enterprise requirements. Support rest and reprocessing needs. Ensure that use are receiving the right outputs in a secu and timely manner. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.01 | Perform operational procedures. | 4. Manage the performance a throughput of the scheduled activities. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.01 | Perform operational procedures. | 5. Monitor incidents and problems deali with operational procedures and ta appropriate action to improve reliability operational tasks performed. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.02 | Manage outsourced I&T services. | 1. Ensure that the enterprise requirements for security of informati processes adhere to contracts and SL with third parties hosting or providi services. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.02 | Manage outsourced I&T services. | 2. Ensure that the enterprise's operation business and IT processing requiremer and priorities for service delivery adhere contracts and SLAs with third parti hosting or providing services. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.02 | Manage outsourced I&T services. | 3. Integrate critical internal management processes with those outsourced service providers. This shou cover, for example, performance a capacity planning, change manageme configuration management, servi request and incident management, proble management, security manageme business continuity, and the monitoring process performance and reporting. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.02 | Manage outsourced I&T services. | 4. Plan for independent audit a assurance of the operational environmer of outsourced providers to confirm th agreed requirements are being adequate addressed. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.03 | Monitor I&T infrastructure. | 1. Log events. Identify the level information to be recorded, based on consideration of risk and performance. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.03 | Monitor I&T infrastructure. | 2. Identify and maintain a list infrastructure assets that need to monitored, based on service criticality a the relationship between configurati items and services that depend on them. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.03 | Monitor I&T infrastructure. | 3. Define and implement rules th identify and record threshold breaches a event conditions. Find a balance betwe generating spurious minor events a significant events so event logs are n overloaded with unnecessary informatio |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.03 | Monitor I&T infrastructure. | 4. Produce event logs and retain them f an appropriate period to assist in futu investigations. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.03 | Monitor I&T infrastructure. | 5. Ensure that incident tickets are creat in a timely manner when monitori identified deviations from defin thresholds. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.03 | Monitor I&T infrastructure. | 6. Establish procedures for monitori event logs. Conduct regular reviews. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 1. Identify natural and man-made disaste that might occur in the area where the facilities are located. Assess the potent effect on the IT facilities. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 2. Identify how I&T equipment, includi mobile and off-site equipment, is protect against environmental threats. Ensure th the policy limits or excludes eatin drinking and smoking in sensitive area and prohibits storage of stationery a other supplies that pose a fire haza within computer rooms. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 3. Keep the IT sites and server rooms cle and in a safe condition at all times (i.e., mess, no paper or cardboard boxes, filled dustbins, no flammable chemicals materials). |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 4. Situate and construct IT facilities minimize and mitigate susceptibility environmental threats (e.g., theft, air, fi smoke, water, vibration, terror, vandalis chemicals, explosives). Consider speci security zones and/or fireproof cells (e. locating production and developme environments/servers away from ea other). |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 5. Compare measures and contingen plans against insurance poli requirements and report results. Addre points of noncompliance in a time manner. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 6. Respond to environmental alarms a other notifications. Document and t procedures, which should inclu prioritization of alarms and contact wi local emergency response authoriti Train personnel in these procedures. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.04 | Manage the environment. | 7. Regularly monitor and maintain devic that proactively detect environmen threats (e.g., fire, water, smoke, humidit |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 1. Examine the IT facilities' requireme for protection against power fluctuatio and outages, in conjunction with oth business continuity planning requiremen Procure suitable uninterruptible supp equipment (e.g., batteries, generators) support business continuity planning. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 2. Regularly test the uninterruptible pow supply's mechanisms. Ensure that pow can be switched to the supply without a significant effect on business operations |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 3. Ensure that the facilities housing t I&T systems have more than one sour for dependent utilities (e.g., pow telecommunications, water, gas). Separa the physical entrance of each utility. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 4. Confirm that cabling external to the site is located underground or has suitab alternative protection. Determine th cabling within the IT site is contain within secured conduits, and access wiring cabinets is restricted to authoriz personnel. Properly protect cabling agai damage caused by fire, smoke, wat interception and interference. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 5. Ensure that cabling and physic patching (data and phone) are structur and organized. Cabling and condu structures should be documented (e. blueprint building plan and wiri diagrams). |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 6. On regular basis, educate personnel health and safety laws, regulations, a relevant guidelines. Educate personnel fire and rescue drills to ensure knowled and actions taken in case of fire or simi incidents. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 7. Ensure that IT sites and equipment a maintained according to the supplie recommended service intervals a specifications. Ensure that maintenance carried out only by authorized personnel |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 8. Analyze the facilities housing's hig availability systems for redundancy a fail-over cabling requirements (extern and internal). |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 9. Ensure that IT sites and facilities are ongoing compliance with relevant hea and safety laws, regulations, guidelin and vendor specifications. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 10. Record, monitor, manage and resol facilities incidents in line with the I& incident management process. Ma available reports on facilities incidents f which disclosure is required by laws a regulations. |
| Management | Deliver, Service and Support | DSS01 | Managed Operations | DSS01.05 | Manage facilities. | 11. Analyze physical alterations to IT sit or premises to reassess the environmen risk (e.g., fire or water damage). Repo results of this analysis to busine continuity and facilities management. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.01 | Define classification schemes for incidents and service requests. | 1. Define incident and service requ classification and prioritization scheme and criteria for problem registration. U this information to ensure consiste approaches for handling and informi users about problems and conducting tre analysis. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.01 | Define classification schemes for incidents and service requests. | 2. Define incident models for know errors to enable efficient and effecti resolution. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.01 | Define classification schemes for incidents and service requests. | 3. Define service request mod according to service request type to enab self-help and efficient service for standa requests. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.01 | Define classification schemes for incidents and service requests. | 4. Define incident escalation rules a procedures, especially for major incide and security incidents. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.01 | Define classification schemes for incidents and service requests. | 5. Define knowledge sources on incider and requests and describe how to use the |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.02 | Record, classify and prioritize requests and incidents. | 1. Log all service requests and inciden recording all relevant information, so th can be handled effectively and a f historical record can be maintained. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.02 | Record, classify and prioritize requests and incidents. | 2. To enable trend analysis, classi service requests and incidents identifying type and category. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.02 | Record, classify and prioritize requests and incidents. | 3. Prioritize service requests and inciden based on the SLA service definition business impact and urgency. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.03 | Verify, approve and fulfill service requests. | 1. Verify entitlement for service reque using, where possible, a predefin process flow and standard changes. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.03 | Verify, approve and fulfill service requests. | 2. Obtain financial and function approval or sign-off, if required, predefined approvals for agreed standa changes. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.03 | Verify, approve and fulfill service requests. | 3. Fulfill the requests by performing t selected request procedure. Whe possible, use self-help automated men and predefined request models f frequently requested items. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.04 | Investigate, diagnose and allocate incidents. | 1. Identify and describe releva symptoms to establish the most probab causes of the incidents. Referen available knowledge resources (includi known errors and problems) to identi possible incident resolutions (tempora workarounds and/or permanent solution |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.04 | Investigate, diagnose and allocate incidents. | 2. If a related problem or known error do not already exist and if the incide satisfies agreed criteria for proble registration, log a new problem. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.04 | Investigate, diagnose and allocate incidents. | 3. Assign incidents to specialist functio if deeper expertise is needed. Engage t appropriate level of management, whe and if needed. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.05 | Resolve and recover from incidents. | 1. Select and apply the most appropria incident resolutions (tempora workaround and/or permanent solution). |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.05 | Resolve and recover from incidents. | 2. Record whether workarounds were us for incident resolution. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.05 | Resolve and recover from incidents. | 3. Perform recovery actions, if required |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.05 | Resolve and recover from incidents. | 4. Document incident resolution a assess if the resolution can be used as future knowledge source. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.06 | Close service requests and incidents. | 1. Verify with the affected users that t service request has been fulfill satisfactorily or the incident has be resolved satisfactorily and within agreed/acceptable period of time. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.06 | Close service requests and incidents. | 2. Close service requests and incidents. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.07 | Track status and produce reports. | 1. Monitor and track incident escalatio and resolutions and request handli procedures to progress toward resoluti or completion. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.07 | Track status and produce reports. | 2. Identify information stakeholders a their needs for data or reports. Identi reporting frequency and medium. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.07 | Track status and produce reports. | 3. Produce and distribute timely reports provide controlled access to online data. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.07 | Track status and produce reports. | 4. Analyze incidents and service reque by category and type. Establish trends a identify patterns of recurring issues, SL breaches or inefficiencies. |
| Management | Deliver, Service and Support | DSS02 | Managed Service Requests and Incidents | DSS02.07 | Track status and produce reports. | 5. Use the information as input continual improvement planning. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.01 | Identify and classify problems. | 1. Identify problems through t correlation of incident reports, error lo and other problem identification resourc |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.01 | Identify and classify problems. | 2. Handle all problems formally w access to all relevant data. Inclu information from the IT chan management system and configuration/asset and incident details. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.01 | Identify and classify problems. | 3. Define appropriate support groups assist with problem identification, ro cause analysis and solution determinati to support problem manageme Determine support groups based predefined categories, such as hardwa network, software, applications a support software. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.01 | Identify and classify problems. | 4. Define priority levels throu consultation with the business to ensu that problem identification and root cau analysis are handled in a timely mann according to the agreed SLAs. Ba priority levels on business impact a urgency. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.01 | Identify and classify problems. | 5. Report the status of identified proble to the service desk so customers and management can be kept informed. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.01 | Identify and classify problems. | 6. Maintain a single problem manageme catalog to register and report proble identified. Use the catalog to establi audit trails of the problem manageme processes, including the status of ea problem (i.e., open, reopen, in progress closed). |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.02 | Investigate and diagnose problems. | 1. Identify problems that may be know errors by comparing incident data with t database of known and suspected erro (e.g., those communicated by extern vendors). Classify problems as know errors. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.02 | Investigate and diagnose problems. | 2. Associate the affected configurati items to the established/known error. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.02 | Investigate and diagnose problems. | 3. Produce reports to communicate t progress in resolving problems and monitor the continuing impact of proble not solved. Monitor the status of t problem-handling process throughout life cycle, including input from IT chan and configuration management. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.03 | Raise known errors. | 1. As soon as the root causes of proble are identified, create known-error recor and develop a suitable workaround. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.03 | Raise known errors. | 2. Identify, evaluate, prioritize and proce (via IT change management) solutions known errors, based on a cost/bene business case and business impact a urgency. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.04 | Resolve and close problems. | 1. Close problem records either aft confirmation of successful elimination the known error or after agreement wi the business on how to alternatively hand the problem. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.04 | Resolve and close problems. | 2. Inform the service desk of the schedu for problem closure (e.g., the schedule f fixing the known errors, the possib workaround or the fact that the proble will remain until the change implemented) and the consequences of t approach taken. Keep affected users a customers informed as appropriate. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.04 | Resolve and close problems. | 3. Throughout the resolution proce obtain regular reports from IT chan management on progress in resolvi problems and errors. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.04 | Resolve and close problems. | 4. Monitor the continuing impact problems and known errors on services. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.04 | Resolve and close problems. | 5. Review and confirm the success resolutions of major problems. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.04 | Resolve and close problems. | 6. Make sure the knowledge learned fro the review is incorporated into a servi review meeting with the busine customer. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.05 | Perform proactive problem management. | 1. Capture problem information related I&T changes and incidents a communicate it to key stakeholde Communicate via reports and period meetings among incident, problem, chan and configuration management proce owners to consider recent problems a potential corrective actions. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.05 | Perform proactive problem management. | 2. Ensure that process owners a managers from incident, problem, chan and configuration management me regularly to discuss known problems a future planned changes. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.05 | Perform proactive problem management. | 3. Identify and initiate sustainab solutions (permanent fixes) addressing t root cause. Raise change requests via t established change manageme processes. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.05 | Perform proactive problem management. | 4. To enable the enterprise to monitor t total costs of problems, capture chan efforts resulting from proble management process activities (e.g., fix to problems and known errors) and repo on them. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.05 | Perform proactive problem management. | 5. Produce reports to monitor proble resolution against the busine requirements and SLAs. Ensure the prop escalation of problems, such as escalati to a higher management level according agreed criteria, contacting extern vendors, or referring to the chan advisory board to increase the priority an urgent request for change (RFC) implement a temporary workaround. |
| Management | Deliver, Service and Support | DSS03 | Managed Problems | DSS03.05 | Perform proactive problem management. | 6. To optimize the use of resources a reduce workarounds, track problem trend |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.01 | Define the business continuity policy, objectives and scope. | |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.01 | Define the business continuity policy, objectives and scope. | 2. Identify key stakeholders and roles a responsibilities for defining and agreei on continuity policy and scope. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.01 | Define the business continuity policy, objectives and scope. | 3. Define and document the agre minimum policy objectives and scope f business resilience. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.01 | Define the business continuity policy, objectives and scope. | 4. Identify essential supporting busine processes and related I&T services. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 1. Identify potential scenarios likely give rise to events that could cau significant disruptive incidents. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 2. Conduct a business impact analysis evaluate the impact over time of disruption to critical business functio and the effect that a disruption would ha on them. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 3. Establish the minimum time required recover a business process and supporti I&T, based on an acceptable length business interruption and maximu tolerable outage. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 4. Determine the conditions and owners key decisions that will cause the continu plans to be invoked. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 5. Assess the likelihood of threats th could cause loss of business continui Identify measures that will reduce t likelihood and impact through improv prevention and increased resilience. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 6. Analyze continuity requirements identify possible strategic business a technical options. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 7. Identify resource requirements a costs for each strategic technical opti and make strategic recommendations. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.02 | Maintain business resilience. | 8. Obtain executive business approval f selected strategic options. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 1. Define the incident response actio and communications to be taken in t event of disruption. Define related rol and responsibilities, includi accountability for policy a implementation. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 2. Ensure that key suppliers and outsour partners have effective continuity plans place. Obtain audited evidence as require |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 3. Define the conditions and recove procedures that would enable resumpti of business processing. Include updati and reconciliation of informati databases to preserve informati integrity. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 4. Develop and maintain operational BC and DRPs that contain the procedures to followed to enable continued operation critical business processes and/ temporary processing arrangemen Include links to plans of outsourc service providers. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 5. Define and document the resourc required to support the continuity a recovery procedures, considering peop facilities and IT infrastructure. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 6. Define and document the informati backup requirements required to supp the plans. Include plans and pap documents as well as data files. Consid the need for security and off-site storage |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 7. Determine required skills f individuals involved in executing the pl and procedures. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.03 | Develop and implement a business continuity response. | 8. Distribute the plans and supporti documentation securely to appropriate authorized interested parties. Make su the plans and documentation are accessib under all disaster scenarios. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). | 1. Define objectives for exercising a testing the business, technical, logistic administrative, procedural and operation systems of the plan to verify completene of the BCP and DRP in meeting busine risk. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). | 2. Define and agree on stakehold exercises that are realistic and valida continuity procedures. Include roles a responsibilities and data retenti arrangements that cause minimu disruption to business processes. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). | 3. Assign roles and responsibilities f performing continuity plan exercises a tests. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). | 4. Schedule exercises and test activities defined in the continuity plans. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). | 5. Conduct a post-exercise debriefing a analysis to consider the achievement. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). | 6. Based on the results of the revie develop recommendations for improvi the current continuity plans. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.05 | Review, maintain and improve the continuity plans. | 1. On a regular basis, review the continu plans and capability against a assumptions made and current busine operational and strategic objectives. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.05 | Review, maintain and improve the continuity plans. | 2. On a regular basis, review the continu plans to consider the impact of new major changes to enterprise organizatio business processes, outsourci arrangements, technologies, infrastructu operating systems and application systen |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.05 | Review, maintain and improve the continuity plans. | 3. Consider whether a revised busine impact assessment may be require depending on the nature of the change. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.05 | Review, maintain and improve the continuity plans. | 4. Recommend changes in policy, plan procedures, infrastructure, and roles a responsibilities. Communicate them appropriate for management approval a processing via the IT change manageme process. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.06 | Conduct continuity plan training. | 1. Roll out BCP and DRP awareness a training. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.06 | Conduct continuity plan training. | 2. Define and maintain traini requirements and plans for tho performing continuity planning, impa assessments, risk assessments, mec communication and incident respons Ensure that the training plans consid frequency of training and training delive mechanisms. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.06 | Conduct continuity plan training. | 3. Develop competencies based practical training, including participati in exercises and tests. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.06 | Conduct continuity plan training. | 4. Based on the exercise and test resul monitor skills and competencies. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.07 | Manage backup arrangements. | 1. Backup systems, applications, data a documentation according to a defin schedule. Consider frequency (month weekly, daily, etc.), mode of backup (e. disk mirroring for real-time backups v DVD-ROM for long-term retention), ty of backup (e.g., full vs. incremental), a type of media. Consider also automat online backups, data types (e.g., voic optical), creation of logs, critical end-us computing data (e.g., spreadsheet physical and logical location of da sources, security and access rights, a encryption. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.07 | Manage backup arrangements. | 2. Define requirements for on-site and o site storage of backup data that meet t business requirements. Consider t accessibility required to back up data. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.07 | Manage backup arrangements. | 3. Periodically test and refresh archiv and backup data. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.07 | Manage backup arrangements. | 4. Ensure that systems, applications, da and documentation maintained processed by third parties are adequate backed up or otherwise secured. Consid requiring return of backups from thi parties. Consider escrow or depo arrangements. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.08 | Conduct post-resumption review. | 1. Assess adherence to the document BCP and DRP. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.08 | Conduct post-resumption review. | 2. Determine the effectiveness of t plans, continuity capabilities, roles a responsibilities, skills and competenci resilience to the incident, technic infrastructure, and organizatior structures and relationships. |
| Management | Deliver, Service and Support | DSS04 | Managed Continuity | DSS04.08 | Conduct post-resumption review. | 3. Identify weaknesses or omissions in t plans and capabilities and ma recommendations for improveme Obtain management approval for a changes to the plans and apply via t enterprise change control process. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 1. Identify stakeholders (e. management, process owners and users) |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 2. Engage with stakeholders a communicate the enterprise requiremer and objectives for monitoring, aggregati and reporting, using common definitio (e.g., business glossary, metadata a taxonomy), baselining and benchmarkin |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 3. Align and continually maintain t monitoring and evaluation approach wi the enterprise approach and the tools to used for data gathering and enterpri reporting (e.g., business intelligen applications). |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 4. Agree on the types of goals and metri (e.g., conformance, performance, valu risk), taxonomy (classification a relationships between goals and metric and data (evidence) retention. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 5. Request, prioritize and alloca resources for monitoring, consid appropriateness, efficiency, effectivene and confidentiality. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 6. Periodically validate the approach us and identify new or changed stakeholde requirements and resources. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.01 | Establish a monitoring approach. | 7. Agree on a life cycle management a change control process for monitoring a reporting. Include improveme opportunities for reporting, metric approach, baselining and benchmarking. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.02 | Set performance and conformance targets. | 1. Define the goals and metric Periodically review them wi stakeholders to identify any significa missing items and define reasonableness targets and tolerances. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.02 | Set performance and conformance targets. | 2. Evaluate whether the goals and metri are adequate, that is, specific, measurab achievable, relevant and time-bou (SMART). |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.02 | Set performance and conformance targets. | 3. Communicate proposed changes performance and conformance targets a tolerances (relating to metrics) with k due diligence stakeholders (e.g., leg audit, HR, ethics, compliance, finance). |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.02 | Set performance and conformance targets. | 4. Publish changed targets and toleranc to users of this information. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.03 | Collect and process performance and conformance data. | 1. Collect data from defined process (automated, where possible). |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.03 | Collect and process performance and conformance data. | 2. Assess efficiency (effort in relation insight provided) and appropriatene (usefulness and meaning) of collected da and validate the data's integrity (accura and completeness). |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.03 | Collect and process performance and conformance data. | 3. Aggregate data to support measureme of agreed metrics. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.03 | Collect and process performance and conformance data. | 4. Align aggregated data to the enterpri reporting approach and objectives. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.03 | Collect and process performance and conformance data. | 5. Use suitable tools and systems for t processing and analysis of data. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 1. Design process performance repo that are concise, easy to understand, a tailored to various management needs a audiences. Facilitate effective, time decision making (e.g., scorecards, traf light reports). Ensure that the cause a effect between goals and metrics a communicated in an understandab manner. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 2. Distribute reports to the releva stakeholders. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 3. Analyze the cause of deviations again targets, initiate remedial actions, assi responsibilities for remediation, a follow up. At appropriate times, review deviations and search for root caus where necessary. Document the issues f further guidance if the problem recu Document results. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 4. Where feasible, integrate performan and compliance into individual sta members' performance objectives and li achievement of performance targets to t organizational reward compensati system. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 5. Compare the performance values internal targets and benchmarks ar where possible, to external benchmar (industry and key competitors). |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 6. Analyze trends in performance a compliance and take appropriate action. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.04 | Analyze and report performance. | 7. Recommend changes to the goals a metrics, where appropriate. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.05 | Ensure the implementation of corrective actions. | 1. Review management responses, optio and recommendations to address issu and major deviations. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.05 | Ensure the implementation of corrective actions. | 2. Ensure that the assignment responsibility for corrective action maintained. |
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.05 | Ensure the implementation of corrective actions. | 3. Track the results of actions committe |

| | | | | | | |
|---|---|---|---|---|---|---|
| Management | Monitor, Evaluate and Assess | MEA01 | Managed Performance and Conformance Monitoring | MEA01.05 | Ensure the implementation of corrective actions. | 4. Report the results to the stakeholders |