UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

IMPLEMENTACION DE HERRAMIENTA DE MONITOREO EN SMU Y PLAN PILOTO DE CHEQUEOS A SUPERMERCADOS UNIMARC ORIENTE, UNIMARC LOS MILITARES Y UNIMARC LA RECOVA

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Carlos Alejandro Rodríguez Araya
Profesor Guía : Roberto Carú Cisternas
Profesor Integrante : Jorge Tapia Castro

Santiago – Chile
Diciembre, 2017

AGRADECIMIENTOS

Este ha sido un largo camino que comenzó aquel primer día de clases con la incertidumbre sobre qué era lo que se nos venía. Trabajar, estudiar, familia, grandes desafíos, grandes compromisos.

Nada de esto se pudo haber realizado si no es con el apoyo incondicional de mi esposa María Inés y mis hijos, los amo y no me imagino caminando en la vida sin ustedes. Las disculpas a ellos por hacerlos dormir tarde, por los trasnoches, por arrebatarles la pieza o el living del departamento para estudiar.

A mi madre Catalina que ya no está y quien siempre tuvo fe ciega en mí y en lo que podría llegar a lograr*. "Tú puedes".*

A los compañeros de Universidad que siempre tuvieron el ánimo y entregaron su esfuerzo para compartir los conocimientos, para entregar esa ayuda necesaria para resolver ese problema.

Gracias a todos.

Mamá, sí pude.

INDICE

TABLA DE FIGURAS

I. INTRODUCCION

El Holding SMU es la cadena de supermercados con mayor cobertura geográfica del país y que con más de 500 locales y 2.000 puntos de ventas (cajas), se posiciona de esta forma como el tercer actor de retail supermercadista en Chile. El Holding está compuesto por distintos formatos de tiendas los que se caracterizan por el público objetivo al que se encuentran dirigidos. Estos formatos son: supermercados Unimarc, tiendas de conveniencia OKMarket, Supermercados Alvi, Mayorista10 y venta online Telemercados.

Es primordial para una empresa de esta envergadura tener sistemas computacionales robustos y confiables que permitan entregar el mejor servicio a sus clientes durante los 7 días de la semana, sobre todo en una industria tan competitiva como es el retail. Por ello, es tarea fundamental del área de Sistemas entregar un soporte eficaz y eficiente a los diferentes sistemas que operan en la compañía y que, en lo específico, permitan al local continuar operando lo antes posible ante un problema o mejor aún, que permita anticiparse a ellos para evitar su ocurrencia.

En la actualidad, SMU no cuenta con un área dedicada a realizar un monitoreo de los sistemas, tampoco posee las herramientas apropiadas que le permitan anticiparse a un problema o falla en los sistemas de los locales, solo se actúa luego que estos incidentes han ocurrido, es decir, de forma reactiva, cuando el usuario afectado lo reporta.

La Gerencia de TI Operaciones y Formatos ha encargado al área de Soporte Nivel 2 la investigación, desarrollo e implementación de la o las herramientas que permitan monitorear los sistemas computacionales de los locales, que entregue la información necesaria para anticiparse a los incidentes. Que esta herramienta no solo sirva para monitorear estados de hardware o enlaces de comunicaciones, sino que sea un real aporte al negocio mediante el monitoreo de los distintos procesos existentes en el local,

como por ejemplo, la actualización de precios, la activación de promociones, el envío de los precios a las cajas y balanzas del local, entre otros.

Luego de revisar las herramientas existentes en el mercado, se determinó que el software Nagios Core puede cumplir con lo solicitado. Nagios es un sistema de monitorización de redes de código abierto que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Durante la presente Memoria, se explicarán las diferentes etapas que fueron ejecutadas para la implementación de la plataforma Nagios y cómo esta herramienta fue el apoyo necesario para lograr el éxito de los objetivos planteados por la Gerencia de TI.

1.1 Motivación

Desarrollar e implementar una plataforma de monitoreo que permita a la empresa anticiparse a los incidentes, notificar rápida y acertadamente a los profesionales destinados para su corrección, con el fin de ser un real apoyo a la gestión del local. Cambiar la reactividad actual por proactividad, permitiendo de esta forma mantener la continuidad operacional de los locales en su principal función que es la atención de los clientes.

1.2 Hipótesis

La plataforma Nagios nos permitirá monitorear el hardware y servicios que operan sobre ellos en todos los locales de la cadena. Utilizando las características de Nagios como ser software gratuito bajo licencia open source, con excelente nivel de soporte por medio de comunidades en línea, con su robustez y gran flexibilidad, será el complemento correcto

para que el área de Soporte Nivel 2 pueda anticiparse a los incidentes o problemas que impidan entregar el servicio ofrecido a los clientes.

1.3 Objetivo General

Implementar la herramienta Nagios Core y utilizar sus múltiples funcionalidades de monitoreo para disminuir la ocurrencia de incidentes y con sus características de notificación, alertar de aquellos que ocurran con el fin de asegurar la continuidad operacional en los locales.

1.4 Objetivos Específicos

- Identificar el hardware y servicios (software) que deben ser monitoreados con la finalidad de prevenir su degradación o interrupción.

- Crear las alertas o plugins correspondientes a los puntos identificados de hardware y servicios que deben ser monitoreados.

- Creación de notificaciones sobre incidentes o fallas para ser enviadas a personal interno y/o proveedores externos de la empresa, según corresponda.

- Recolectar datos del monitoreo con el fin de crear un historial y generar estadísticas que permitan la anticipación a los incidentes o fallas.

- Cambiar la reactividad existente en las tareas realizadas por el área de Soporte Nivel 2 frente a la ocurrencia de incidentes, por la proactividad sobre ellos.

II. MARCO TEORICO

Los sistemas y las tecnologías de información han cambiado la forma en la que operan las organizaciones actuales. Por medio de estas se automatizan procesos, se entrega la información necesaria para la toma de decisiones logrando con ello importantes beneficios para la empresa.

Las tecnologías de la información han sido definidas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: el factor humano, los contenidos de la información y los mecanismos de intercambio de ellas, el equipamiento, la infraestructura, el software y los recursos financieros asociados a los elementos indicados anteriormente. La forma en la que interactúan estos elementos es mediante los distintos procesos que existen dentro de la empresa.

Una empresa tiene una gran cantidad de procesos de variados tamaños y complejidades que buscan, desde sus objetivos particulares, cumplir aquellos objetivos planteados por la Gerencia. Por eso es importante que los procesos y los elementos que la componen operen correctamente para lograr un eficiente uso de los recursos de TI y que permitan a la empresa cumplir con lo señalado anteriormente.

SMU tiene más de 500 locales entre sus distintos formatos, y si bien el software que se utiliza en los locales es el mismo para ellos, existen algunas particularidades según el tipo de negocio que las hacen diferentes. Esta diferencia es comercial, es la propuesta que se realiza al público, pero sistémicamente esta diferencia es mínima.

Una empresa de retail que atiende público los 7 días de la semana y más de 350 días al año, demanda un alto uso de sistemas informáticos en sus distintos niveles de trabajo.

Algunos de esos sistemas son visibles solo para el personal interno de la compañía y una menor parte, por el cliente que adquiere los productos en los locales. Esto es precisamente lo importante para la empresa, la venta de los productos y que la experiencia del cliente durante este proceso sea la mejor. Esta experiencia comienza desde que el cliente ingresa al local hasta que llega al punto de venta para pagar por los productos escogidos en la sala de ventas. Que en el punto de venta se cobre el precio ofrecido, que en la sala de ventas exista stock del producto que el cliente busca, que pueda pagar con su tarjeta bancaria o de casa comercial en línea, son solo algunos ejemplos de los distintos puntos que abarcan esta experiencia. Estos puntos visibles para los clientes son el resultado de distintos procesos manuales y/o automáticos, administrativos y/o sistémicos.

Basado en el marco de referencia de ITIL, se define como incidente “una interrupción no planificada de un servicio de TI o una reducción de la calidad de un servicio de TI”. El hecho que se dé en forma constante un incidente, o que un único incidente sea de gran impacto, genera lo que se conoce como un problema.

2.1 Sistemas de Monitorización

En todas las organizaciones con infraestructura informática es necesario garantizar la disponibilidad y accesibilidad de los servicios y hardware que los soportan, tanto para los clientes internos (empleados) de la empresa o externos (clientes).

Para esta tarea es que nacen los sistemas de monitoreo con el objetivo claro de ser un apoyo para los encargados de la supervisión de la infraestructura informática.

Si bien no se trata de una herramienta indispensable, y en donde el tamaño de la empresa puede influir en la decisión de utilizarla, sí son de gran utilidad ya que con sus múltiples

funcionalidades no solo nos permiten conocer el estado de la infraestructura, sino que además de alertarnos por diferentes medios si se ha producido algún evento, generar información histórica con la finalidad de predecir la ocurrencia de eventos o alertar de éstos cuando ocurran.

Como todo sistema, estos han ido evolucionando de acuerdo con las necesidades que van surgiendo, así como a las nuevas tecnologías y dispositivos. Esta evolución podría enumerarse de la siguiente forma:

- **1ª Generación – Aplicaciones propietarias para monitorear dispositivos activos o inactivos.**

  El mostrar el estado de los dispositivos en forma clara y en tiempo real ha sido uno de los grandes retos de este tipo de aplicativos. Para ello, las herramientas de monitoreo mostraban este estado a través de un código de colores:

  - En color verde: el dispositivo está funcionando correctamente.
  - En color amarillo: se detectó algún problema temporal que no afecta la disponibilidad.
  - En color rojo: el dispositivo de encuentra fuera de servicio en este momento y requiere acciones inmediatas para su restablecimiento.

- **2ª Generación – Aplicaciones de análisis de parámetros de operación a profundidad.**

  La siguiente generación de herramientas evalúa el estado de los componentes dentro del dispositivo (CPU, memoria, espacio de almacenamiento, etc.) de manera que se puedan buscar los parámetros de ajuste para modificar los

parámetros que sean necesarios para mantener y elevar los niveles de servicio del dispositivo.

- **3ª Generación – Aplicaciones de análisis punta a punta con enfoque a servicio.**

  Esta nueva generación de aplicaciones tiene un enfoque más transaccional ya que captura un flujo de tráfico e identifica las latencias que se producen en las conexiones entre los distintos componentes de un servicio.
  Ya no es sólo el estado de un dispositivo aislado, sino que como es que las conjunciones de varios de ellos afectan el estado final del servicio que se desea entregar.

- **4ª Generación – Personalización de indicadores de desempeño de los procesos de negocio.**

  Esta generación logra representar en forma clara y gráfica los indicadores que el cliente puede crear y personalizar de acuerdo con sus necesidades, son los llamados dashboard.
  Con la madurez que han alcanzado las herramientas de monitoreo, estas permiten entregar información simultánea de la visibilidad de la infraestructura, mediciones de impacto al negocio, predicciones de desempeño, entre otros.

2.2 ITIL

ITIL (Biblioteca de Infraestructura de Tecnologías de Información) cuya finalidad fundamental es orientar a la empresa a organizar su funcionamiento interno y mejorar

continuamente el servicio al cliente, aporta grandes beneficios a pequeñas y grandes empresas gracias a su filosofía de mejora continua. Por ello se centra en tres objetivos que son claves en la Gestión de Servicios TI:

- Alinear los servicios informáticos adaptándose no sólo a las necesidades actuales, sino adelantándose a las futuras.

- Mejorar mediante el análisis de los sucesos y la mejora continua la calidad de los servicios ofrecidos.

- Reducir el coste económico a largo plazo buscando la eficacia en la implementación y mantención de los servicios de TI.

Con la utilización de sistemas de monitorización podemos implementar muchas mejoras que ayuden a la empresa a acercarse a los objetivos mencionados anteriormente.

Dentro del entorno de ITIL podemos encontrar otros aparatos que nos sirven como base para la implementación de una herramienta de monitoreo entregándonos su guía y beneficio.

2.2.1 Gestión de la Continuidad del Servicio

Esta se encarga de prevenir y proteger a la empresa de los efectos que pudiera tener una interrupción de los servicios de TI, ya sea que haya sido ocasionada por alguna falla técnica o por causas naturales, o que haya sido provocada voluntaria o involuntariamente, por alguna persona.

La Gestión de la Continuidad de los Servicios de TI debe combinar equilibradamente procedimientos:

- Preventivos
  Son medidas que buscan eliminar o mitigar los riesgos de interrupción y sus posibles efectos.

  La utilización de una herramienta de monitoreo nos permite cubrir este punto ya que se dispone de un sistema que está vigilando que no se produzca alguna interrupción.

- Reactivos
  Son procedimientos que buscan reanudar el servicio tan pronto como sea posible después de cualquier interrupción.

  Utilizando la funcionalidad de notificaciones de la herramienta de monitoreo podremos informarnos a la brevedad si se ha generado una interrupción del servicio, y dependiendo del caso específico, se puede programar que esta misma herramienta ejecute alguna acción con la finalidad de restaurar el servicio.

2.2.2 Gestión de Eventos

Este proceso de ITIL se asegura que todos los dispositivos y servicios se encuentren constantemente monitoreados con la finalidad de anticiparse a los problemas, resolverlos o incluso prevenirlos. Además, define un proceso para categorizar estos eventos de modo que se puedan tomar las medidas apropiadas para restablecer la normalidad de estos de ser necesario.

Se denomina evento “a todo suceso detectable que tiene importancia para la estructura de la organización TI, para la prestación de un servicio o para la evaluación del mismo”.

Existen 2 tipos de herramientas de monitorización:

- Herramientas de monitorización activa.
  Se comprueban los dispositivos y servicios uno a uno para verificar su estado. Si se detecta una interrupción de la disponibilidad, la herramienta genera una alerta que es enviada al equipo designado para su control.

- Herramientas de monitorización pasiva.
  Detectan alertas operacionales generadas por los propios dispositivos o servicios.

Los eventos no siempre son por la interrupción del servicio entregado, también pueden ser rutinarios o informativos. De esta forma, existen tres tipos básicos de eventos dependiendo de su impacto:

- Evento informativo
  Es aquel que no requiere acción y que indica que el servicio está operando con normalidad.

- Evento de alerta
  Es el que se produce cuando se ha alcanzado un umbral establecido.

- Evento de Excepción
  Se genera cuando el servicio está operando anormalmente o se ha interrumpido.

La Gestión de Eventos, además de detectar y notificar los sucesos, se encarga de clasificarlos y dimensionar su impacto en el servicio. En caso de ser necesario, se ocupa

también de documentar el evento y derivarlo al proceso correspondiente para que tome medidas:

- Gestión de Incidentes
- Gestión de Problemas

2.2.3 Gestión de Incidentes

La Gestión de Incidentes tiene como objetivo resolver, de la manera más rápida y eficaz posible, cualquier incidente que cause una interrupción en el servicio. Su objetivo principal es devolver el servicio de TI a su normalidad lo antes posible.

Un incidente es una interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos o consultas reportadas por los usuarios, el equipo del servicio o por alguna herramienta de monitorización de eventos.

2.2.4 Gestión de Problemas

Las funciones principales de la Gestión de Problemas son:

- Investigar las causas de toda alteración del servicio de TI.
- Determinar las posibles soluciones a estas alteraciones.
- Proponer las peticiones de cambio necesarias para restablecer la calidad del servicio.
- Realizar las revisiones post-implementación para asegurar que los cambios han surtido los efectos buscados sin crear problemas de carácter secundario.

La Gestión de Problemas puede ser:

- Reactiva
  Analiza los incidentes que ocurran con la finalidad de descubrir su causa y proponer soluciones a ellas.

- Proactiva
  Monitoriza la calidad de la infraestructura de TI con el objetivo de prevenir incidentes antes de que éstos ocurran.

Si bien existe similitud entre la palabra incidente y problema, incluso, en las organizaciones se tiende llamar incidente a cualquier suceso anómalo sobre la infraestructura de TI, es importante señalar que existen diferencias en la terminología ITIL.

- Incidente
  Es cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.

- Problema
  Es un incidente recurrente, una situación que está generando incidencias.

De todas formas, es importante recalcar que para ambos casos se debe realizar un registro de la interrupción del servicio y cuáles fueron los pasos o procedimientos que se ejecutaron para su solución. Esto cobra vital importancia cuando se trata de un incidente ya que así el técnico puede utilizar su historial de información para encontrar la solución definitiva al problema.

III. DESARROLLO

Una de las metas propuestas por la Gerencia de TI para este proyecto, es lograr que el desarrollo e implementación de la solución de monitoreo sea realizada por personal técnico interno de la empresa. Este desafío busca que las áreas sean proactivas, generadoras de ideas y que generen confianza en sus propias capacidades. Que la solución a un problema no sea siempre buscarla en los proveedores externos.

Para la implementación de esta solución, se analizaron distintos softwares de monitoreo, tanto privativos como open source. Una vez revisados los requisitos del software de monitoreo seleccionado, nos abocamos en la elección del sistema operativo sobre el cual se instalará dicho software.

Si bien siempre estuvo presente la prerrogativa de optimizar costos, se evaluó para este proyecto el software privativo y el software open source, siendo el costo monetario uno más de los puntos a considerar en la selección del software realizada.

Los principales puntos que se tuvieron en cuenta para la evaluación de las distintas herramientas de monitoreo se encuentran:

- Comunicación de las alertas.
- Usabilidad y presentación de los datos en el panel.
- Flexibilidad a la hora de adaptarse a herramientas o software particulares.
- Escalabilidad de la herramienta.
- Soporte de distintos protocolos de transmisión de datos.

- Comunidad de usuarios de apoyo a la herramienta.

- Flexibilidad para el diseño de alertas y plugins propios.

- Costo monetario de la herramienta.

Respecto a los puntos que se utilizaron para la elección del sistema operativo sobre el cual se instalaría la herramienta de monitoreo, básicamente se tuvo que esperar a elegir la herramienta ya que algunas usan Windows y otras Linux.

3.1 Revisión de distintos sistemas de monitoreo

Se evaluaron las siguientes herramientas para monitoreo de redes:

- Zabbix
- WhatsUp Gold
- Nagios Core

3.1.1 WhatsUp Gold

WhatsUp Gold es un software propietario de la empresa Ipswitch que opera sobre una plataforma Windows y utiliza la base de datos Microsoft SQL Server para almacenar la información de los monitoreos realizados.

Tiene características como el descubrimiento y creación de mapas automatizados, generación de reportes avanzados, notificaciones de alertas, acciones de autorecuperación en caso de caídas (como levantar un servicio de Windows), tiene interfaz web, entre otros. Puede monitorear equipos con distintos sistemas operativos, como Windows y Linux.

Sin embargo, el software tiene un costo que varía dependiendo de la edición y las funcionalidades de ellas. El valor de las ediciones varía en el intervalo de US$ 1.755 a US$ 4.995. Además, hay un costo adicional por la cantidad de nodos y servicios que serán monitoreados. No debemos olvidar que este software debe ser levantado sobre una máquina que tenga Windows como sistema operativo, lo que hace que el costo total sea aún mayor.

Figura 1: Sistema de monitoreo WhatsUpGold

3.1.2 Zabbix

Es un software open source que cuenta con una interfaz web y usa MySql, PostregSQL, SQLITE, entre otros, como base de datos. Zabbix puede ser levantado sobre una máquina con Linux y tiene agentes para monitorear máquina con Linux y Windows. Realiza chequeos utilizando servicios como SMTP, HTTP, TCP, entre otros. Cuenta con autodescubrimiento, configuración de permisos de usuarios y grupos, sistema flexible de notificación de eventos, entre otros. Permite la generación de reportes y gráficos sin la necesidad de instalar software adicional.

El sistema de gráficos es muy potente pero también es un inconveniente, ya que su vista es fundamentalmente gráfica, y en nuestro caso no aporta mucho valor ya que se monitorearán más de 500 servidores, además, actualmente SMU no dispone de personal dedicado exclusivamente a mirar en pantallas las alertas que se pueden generar por los distintos monitoreos.

Zabbix pertenece a la empresa Zabbix LLC y que, si bien entrega el software en forma gratuita, posee servicios de soporte y entrenamiento a usuarios por un costo adicional.

Como la mayoría de los proyectos open source, Zabbix cuenta con una comunidad de usuarios que contribuyen en el desarrollo de este software y prestan ayuda en distintos foros y comunidades de forma gratuita.

Figura 2: Sistema de monitoreo Zabbix

3.1.3 Nagios Core

Nagios Core es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos y servicios que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH y la posibilidad de programar scripts o plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, genera alertas que pueden ser recibidas por los responsables correspondientes mediante correo electrónico, mensajes SMS, entre otros, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Nagios Core pertenece a la empresa Nagios Enterprise quien provee además entre otros softwares, Nagios XI que es una versión comercial de Nagios Core.

Nagios Core es la herramienta de monitoreo que tiene la mayor comunidad de usuarios y que constantemente está apoyando su desarrollo y con soporte gratuito.

Nagios posee 2 tipos de chequeos:

- Chequeo Activo
  Este tipo de chequeo es realizado por el servidor de Nagios en intervalos regulares o bajo demanda.

- Ventaja
  - No hay que instalar un agente especializado en el cliente.

- Desventajas
  - Genera un alto uso de recursos del servidor de Nagios el cual aumenta exponencialmente según la cantidad de hosts y servicios a monitorear.
  - Dificultad para monitorear hosts que se encuentran detrás de un firewall.

- Chequeo Pasivo

  Este tipo de chequeo es realizado por aplicaciones o servicios externos y se ejecutan en los equipos que son monitoreados en intervalos regulares o bajo demanda, para después enviar el resultado de éste al servidor de Nagios.

  - Ventajas
    - Ya que este chequeo es ejecutado por el host que está siendo monitoreado, permite liberar de recursos al servidor de Nagios.
    - Servicios de naturaleza asíncrona que no se pueden controlar de manera eficaz por medio de chequeos activos.
    - Dispositivos situados tras firewalls que o pueden ser controlados activamente desde el servidor de Nagios.

  - Desventaja
    - Genera un alto uso de recursos del servidor de Nagios el cual aumenta exponencialmente según la cantidad de hosts y servicios a monitorear.

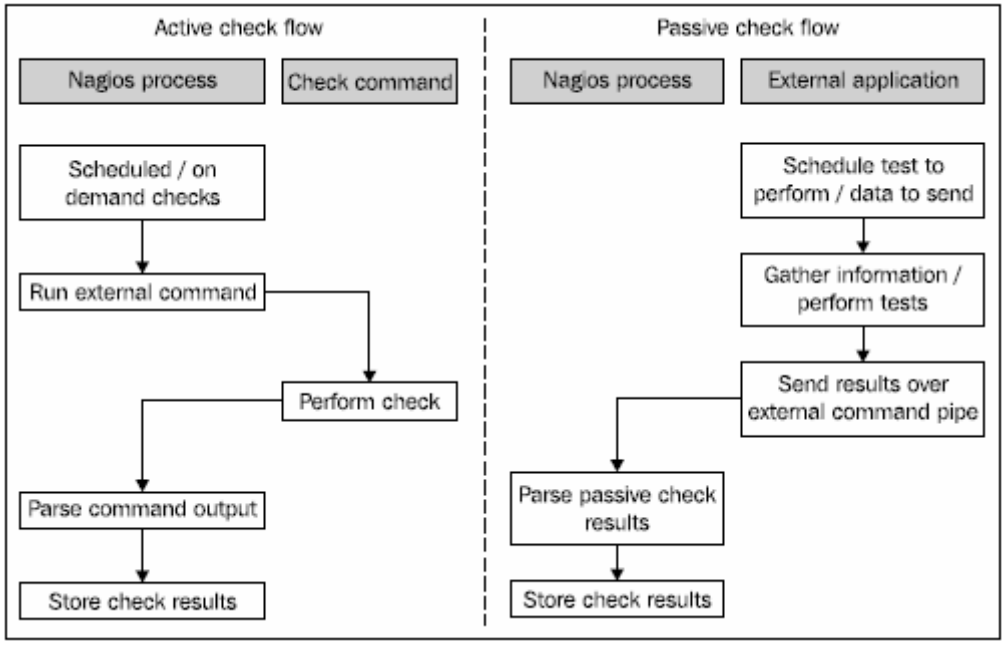

Figura 3: Flujo de procesos entre chequeos activos y pasivos

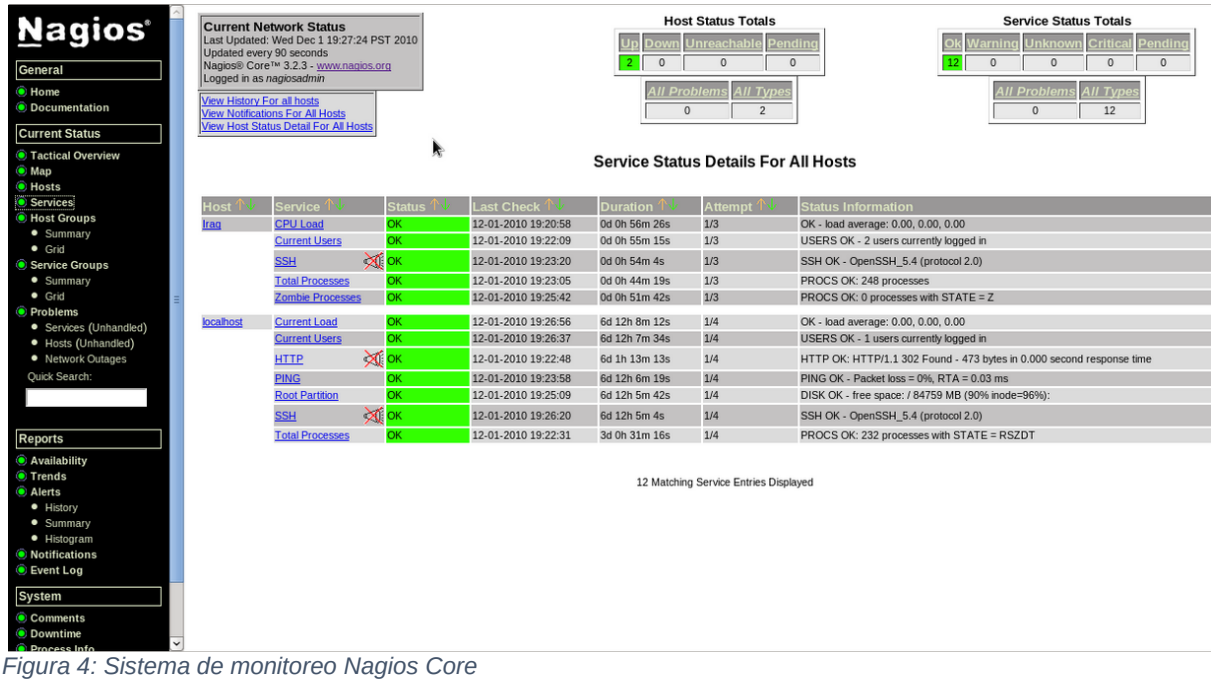

Figura 4: Sistema de monitoreo Nagios Core

3.2 Elección del sistema de monitoreo

Luego del análisis de las herramientas anteriormente mencionadas, se elige Nagios Core como el software open source que nos permitirá lograr los objetivos definidos.

Las principales características que nos llevaron a esta elección fueron:

- Es un sistema de monitoreo que no tiene costo, posee una gran comunidad de usuarios que brindan apoyo tanto con respuestas a problemáticas específicas como en el desarrollo de scripts para monitoreo.

- Es robusto, versátil y personalizable.

- Supervisión de recursos de los servidores como discos duros, memoria, procesos, etc.

- Supervisión de servicios de red como SMTP, HTTP, PING, etc.

- Tiene un sistema de notificaciones altamente potente, que notifica errores cuando existen problemas o alertas que son enviados por correo electrónico.

- Dispone de una interfaz web para la visualización del estado actual de toda la infraestructura de red monitorizada en tiempo real.

- A través de su interfaz web se puede realizar algunas acciones útiles para la gestión del monitoreo como desactivar notificaciones o chequeos si un servidor se encuentra en reparaciones, entre otros.

- Monitoreo de procesos de negocios mediante la consulta directa a base de datos o archivos con el uso de script creados en lenguajes como bash, python, perl, entre otros.

- Flexibilidad en la configuración de los tipos de chequeos permitiendo adecuarlos a nuestra realidad.

3.3 Elección del sistema operativo

Ya que Nagios debe ser instalado sobre una plataforma Linux y luego de revisar las distribuciones disponibles en el mercado, se ha elegido como sistema operativo para el servidor de monitoreo la distribución Linux OpenSuse Leap 42.2.

Esta selección se basa principalmente en los siguientes puntos:

- Es una distribución totalmente gratuita y libre para todo uso ya que se encuentra liberada bajo GNU.

- Utiliza la base de los productos SUSE Linux Enterprise y sigue su mismo calendario de lanzamientos de manera sincronizada con sus Service Packs. Esto asegura tener un sistema operativo estable con una mirada más empresarial. Por otro lado, existe OpenSuse Tumbleweed que es la distribución rolling release y que está orientada para los usuarios que buscan siempre las últimas versiones de todos los softwares.

- OpenSuse Leap permite la instalación del sistema operativo como servidor, ofreciendo de esta forma acelerar el proceso de implementación y elimina

software innecesario como tipos de escritorios, software de ofimática, entre otros.

- Los servidores de los locales de SMU tienen instalados SUSE Linux Enterprise como sistema operativo en sus versiones 10 y 11, además, los puntos de ventas tienen una versión especializada llamada SUSE Linux Enterprise Point of Service. De esta forma se aprovechará el know-how existente del personal técnico de la empresa en el uso de esta distribución Linux.

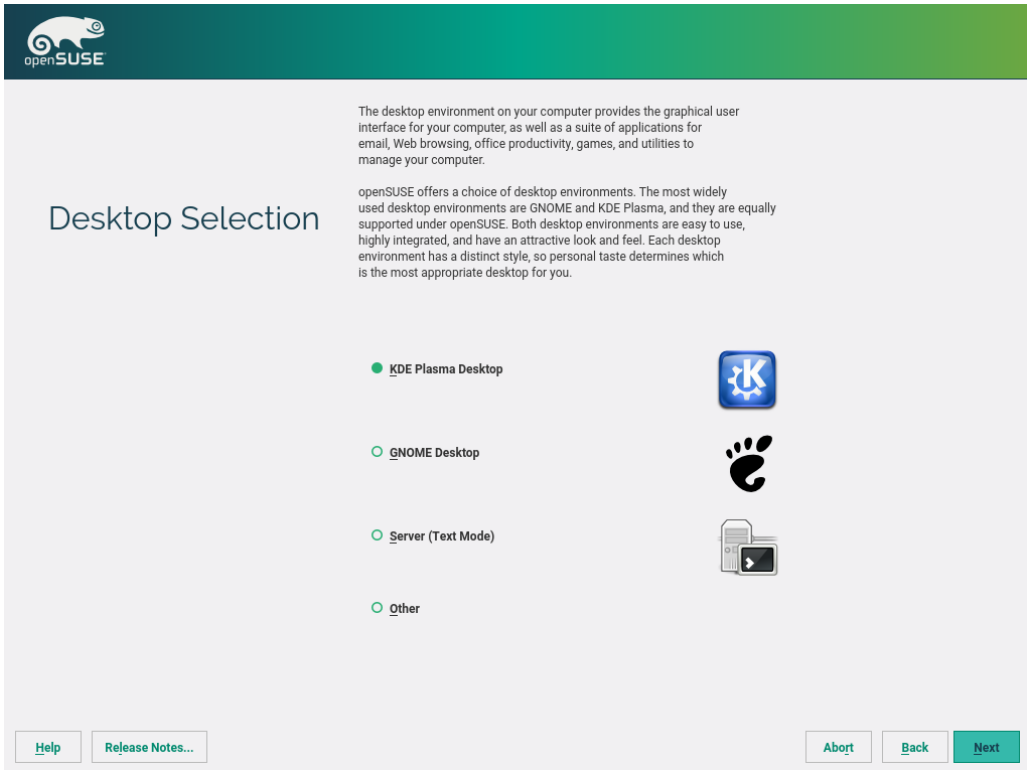

Figura 5: Captura de pantalla de instalación de sistema operativo Linux OpenSuse 42.2

3.4 Arquitectura de Nagios

3.4.1 Requisitos para la instalación de Nagios

Los requerimientos de Nagios Core para su instalación son:

- Servidor Linux
- Compilador C instalado
- Un web server, de preferencia Apache
- Librerías GD versión 1.6.3 o superior.

Nagios no especifica las características físicas que debe tener el servidor sobre el cual se montará la herramienta, pero de acuerdo con lo comentado por usuarios en distintos portales web o blog de ayuda, Nagios Core se instalará a modo de prueba en un servidor virtual que tiene las siguientes características:

- Procesador Xeon T-3 3.3Mhz
- Memoria RAM: 8GB
- Disco Duro: 500GB

De todas formas, el requerimiento de hardware es directamente proporcional a la cantidad de hosts y servicios a monitorear.

3.4.2 Componentes de la instalación de Nagios

Los requisitos hardware son muy variables. Dependen en gran medida del número de servicios y dispositivos a monitorear. Según la documentación existente en la página de Nagios., para una infraestructura de unos 200 equipos, se necesitaría un computador con procesador Intel un Dual-Core con 250GB de disco duro y, de 4 a 8GB de memoria RAM.

3.4.2.1 Nagios Core

Nagios Core es la herramienta open source más conocida y que ha servido además como base para otros softwares de monitoreo. Los requerimientos de software de Nagios son mínimos y ya fueron mencionados anteriormente, además que siguen la misma línea opensource que Nagios, logrando con esto no aumentar los costos monetarios para la implementación de esta herramienta.

3.4.2.2 Plugins

Un plugin es un script o aplicación que devuelve un resultado en un formato determinado.

Nagios no tiene plugins incorporados por defecto en su aplicación, sin embargo, existe un paquete que es considerado como estándar el cual contiene alrededor de 50 plugins que deben ser instalados manualmente. Estos plugins están desarrollados en C, sin embargo, dada la flexibilidad de Nagios, se pueden crear componentes propios utilizando distintos lenguajes como bash, php, python, entre otros.

Las características del valor devuelto por estos plugins son los siguientes:

- Debe retornar un valor numérico como resultado de su evaluación: 0 (OK), 1 (Warning), 2 (Critical), 3 (Unknow).

- El resultado del plugin debe ser una cadena de texto que será mostrada en la interface Web de Nagios.

- Opcionalmente, se puede añadir otra cadena de texto para proporcionar datos de rendimiento. Generalmente se usa para realizar gráficas con programas de terceros.

Entre los plugins estándar se encuentran algunos para monitorear si el host se encuentra en línea, si algún puerto tcp o udp está abierto, si el servicio http está levantado, etc.

3.4.2.3 NRDP (Nagios Remote Data Processor)

NRDP es un método flexible de transporte de datos y de procesamiento para Nagios, especial para uso en los tipos de chequeos pasivos de Nagios.

De forma predeterminada, NRDP tiene la capacidad de permitir que los agentes remotos y aplicaciones envíen comandos o resultados de chequeos a un servidor Nagios.

Para su funcionamiento, NRDP tiene 2 componentes:

- Servidor NRDP
  Que recibe las notificaciones desde los clientes remotos y las envía al servidor de Nagios.

- Cliente NRDP
  Que se instala en el cliente remoto y envía el resultado de los chequeos realizados por los aplicativos o servicios al servidor NRDP.

  Si bien este cliente viene en el mismo paquete que el servidor NRDP, puede ser reemplazo por otro servicio que realice la misma tarea.

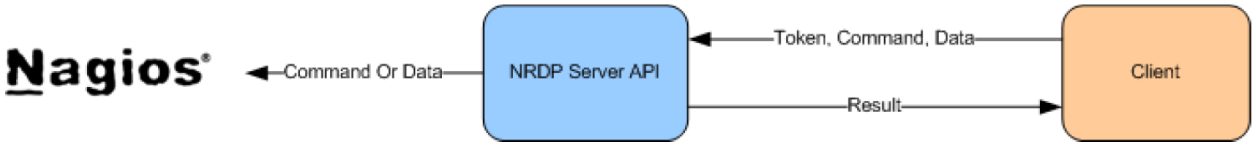

Figura 6: Diagrama del funcionamiento del componente NRDP

3.4.2.4 Chequeos Activos

Como se indicó anteriormente, los chequeos activos son aquellos chequeos que son generados por el demonio de Nagios que se encuentra en el servidor de monitoreo. Con este tipo de chequeo se evita el tener que instalar algún agente en el host que se va a monitorear. Por otro lado, esto produce que la carga de trabajo para el servidor de Nagios vaya en aumento a medida que se agreguen más hosts y servicios a monitorear.

En el caso de SMU, se utilizará el chequeo activo PING con la finalidad de monitorear si los dispositivos se encuentran en línea.

Figura 7: Proceso de chequeo activo

3.4.2.5 Chequeos Pasivos

Los chequeos pasivos son aquellos chequeos que son realizados por aplicaciones o servicios externos al servidor de monitoreo y cuyo resultado es enviado a éste para que sea interpretado por Nagios.

Ya que el proceso de chequeo es realizado por el cliente, liberando de carga de trabajo al servidor de Nagios y hace que esta característica se transforme en una de las principales ventajas de este tipo de chequeo.

Se espera que la mayoría de los plugins que se desarrollen o instalen serán para utilizar con este tipo de chequeo. Con esto se busca no sobrecargar el servidor de Nagios por la cantidad de dispositivos y servicios que deben ser monitoreados.

Figura 8: Ejecución del proceso de chequeo pasivo

Si bien el chequeo es realizado por un servicio externo a Nagios a través de un programa, un servicio, un script, etc., el resultado deberá ser enviado, de alguna forma, al servidor de monitoreo para su procesamiento e interpretación.

Una de estas formas es utilizar el componente NRDP que fue revisado anteriormente, lo que implica que se debe instalar en el host a monitorear el componente y el cliente PHP necesario para su funcionamiento. Sin mencionar el costeo en recursos y tiempo que implicará el despliegue de ambos componentes en los servidores de SMU, y posteriormente en las 2.000 cajas del Holding, se determinó la no instalación del cliente PHP ya que no es parte de los requerimientos para el funcionamiento de los aplicativos del local.

Tomando en consideración lo anterior y aprovechando la flexibilidad de Nagios, se determina el uso de un script desarrollado en BASH llamado **send_nrpd.sh** que permitirá el envío del resultado del chequeo al servidor de Nagios.

De esta forma, el diagrama del monitoreo será de la siguiente forma:

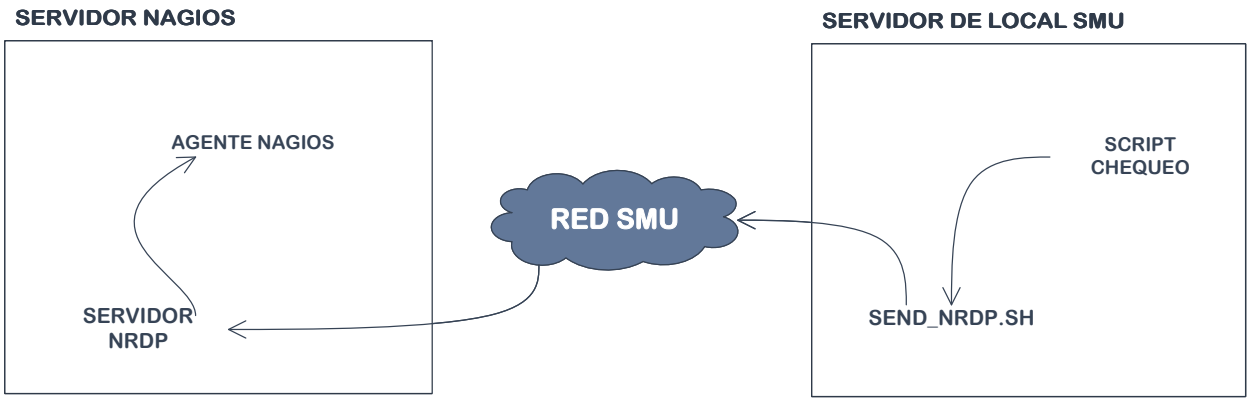

Figura 9: Diagrama de la solución propuesta para el monitoreo con Nagios

Para facilitar la instalación, mantenimiento y explotación del monitoreo con Nagios, y evitar interferir con los procesos propios del servidor del local, en cada uno de ellos se creará un grupo y usuario con la finalidad de asociarle un cron que permita la programación de ejecución de los scripts de monitoreo. Además, los scripts serán copiados en una carpeta asociada a este usuario con el fin de aislarlos del resto de usuarios del equipo.

Con esto, se puede centralizar sin problemas el mantenimiento del monitoreo ya que todos los locales usarán los mismos scripts y se encapsularán los medios que se usen para este fin.

3.4.2.6 Objetos de chequeo

Cada host y servicio a monitorear tiene su propia particularidad. La configuración de ellos dependerá del servicio o host monitoreado y variará entre otros aspectos en, a quién se notificará en caso de error, a quién se escalará la notificación en caso de que el error persista, cuál será el período para el chequeo, cada cuánto tiempo se ejecutará el chequeo, cuánto tiempo pasará antes de enviar la notificación, entre otros.

Para lograr esta configuración, Nagios trabaja con objetos que permiten que esta herramienta sea flexible y potente.

Los objetos son los elementos involucrados en la lógica de monitorización y notificación. Estos pueden ser definidos en uno o más archivos de texto con extensión CFG en un directorio específico.

Algunos de estos objetos son:

- Host

  Define el dispositivo a monitorizar. Los hosts son dispositivos en la red como servidores, impresoras, routers, etc. Los hosts tienen servicios asociados y dirección IP o MAC.

- Servicios

  Son los objetos centrales en la lógica del monitoreo.

  Los servicios están asociados a los hosts y pueden ser atributos de los hosts (uso del disco, carga de CPU, etc.), servicios provistos por los hosts (HTTP, POP3, FTP, etc.), entre otros.

  Algunas de las características asociadas a estos objetos son:

  - Período de tiempo por el cual se regirá el monitoreo.
  - Comando usado para comprobar el servicio.
  - El contacto para realizar las notificaciones.

- Comandos

  Se usan para indicar a Nagios qué programas o script se ejecutan para llevar a cabo los chequeos de servicios, las notificaciones, etc.

- Contactos

  Un contacto es la definición de una persona que debe ser contactado cuando ocurra algún suceso en la red.

  Algunas de las características asociadas a este objeto son:

  - Los períodos de notificación de los errores de hosts y servicios.
  - El comando por utilizar para enviar la notificación de los errores de hosts y servicios.

- Períodos de tiempo

  Son rangos de horarios que se asignan para cada día de la semana con el objeto de realizar alguna de las siguientes acciones:

  - Cuando los Hosts y servicios han de ser monitorizados.
  - Cuando los contactos deben recibir las notificaciones.

- Dependencias de host y servicios

  Una dependencia de host o servicio permite que cuando uno de ellos falla, no se notifique de éste a los hosts o servicios dependientes de él y no se intente comprobar su estado, porque éstos no han fallado realmente, sino que ha fallado el equipo del cual dependen.

- Escalado de notificaciones

  Se usan para intensificar las notificaciones respecto al cambio de estado de un host o servicio. Su funcionamiento es simple, una vez que se ha generado una alerta se envía una notificación, y si esta alerta permanece vigente en el período que se haya configurado, se enviará una nueva notificación a otro destinatario. La idea básica es que, si no se ha corregido la alerta después de la primera notificación, se envíe una nueva a un empleado de un nivel superior en el organigrama de la empresa.

3.5 Arquitectura actual de SMU

Los locales de SMU se encuentran ubicados a lo largo de Chile y están comunicados mediante una red ethernet WAN que, a pesar de que los locales no se envían información entre sí, permite que sean visibles entre ellos.

La labor de monitoreo está siendo diseñada para vigilar los procesos que existen en los locales, algunos servicios provistos por los dispositivos y el estado físico de algunos de ellos. Entre los dispositivos a monitorear encontramos los POS, balanzas, reloj control, servidores, etc.

El funcionamiento de los dispositivos de redes de los locales, como switch y AP, son responsabilidad del Area de Redes de la Gerencia de Comunicaciones por lo cual quedan fuera del alcance de este proyecto.

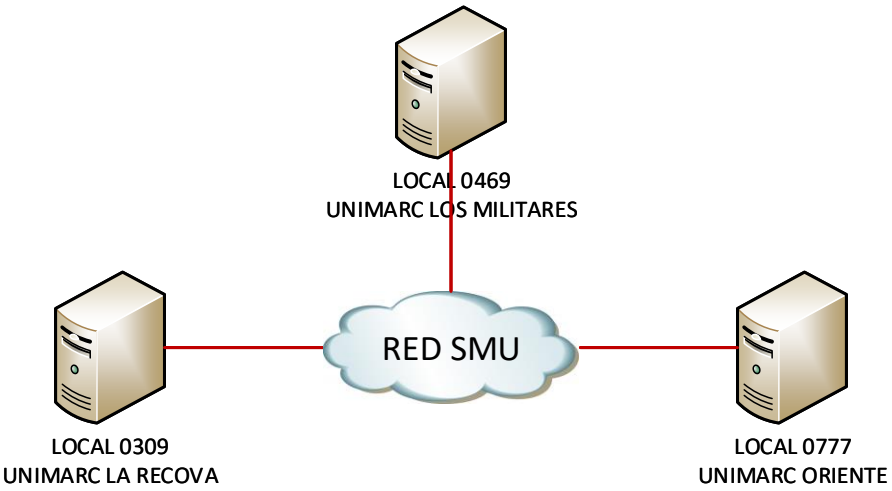

Figura 10: Esquema de red ethernet entre servidores de SMU

3.5.1 Arquitectura de un local de SMU

La infraestructura tecnológica de los locales de SMU es similar entre sí, con variantes en el hardware relacionado con la antigüedad y marca de ellos. Sin embargo, se ha iniciado un proceso de modernización de esta infraestructura con el fin de actualizar este hardware y homogenizar los distintos modelos existentes en los locales.

Respecto al software que se utiliza, aparte de los sistemas operativos y ofimáticos (Microsoft Office, Acrobat Reader PDF, etc.), existen otros específicos que tienen relación con el funcionamiento del local. El principal proveedor de estas herramientas es la empresa de origen uruguayo llamada Geocom.

3.5.1.1 Hardware

Los dispositivos más representativos en la operación de un local son:

- Servidor IBM o HP Proliant.
  Tiene sistema operativo SUSE Linux Enterprise, versiones 10 y 11, y en cada local este servidor recibe la información desde el ERP SAP que debe ser enviada a las cajas del local. Desde las cajas se envía información de ventas al servidor del local el cual por otros procesos las envía a concentradores de datos que son utilizados por ERP SAP o herramientas BI.

- POS o cajas marcas IBM, NCR o Toshiba
  Los POS se comunican vía ethernet y la variedad de marcas se genera por las distintas adquisiciones de cadenas de supermercados que realizó Unimarc en los años anteriores.
  Dada la variedad de cadenas del holding SMU, podemos encontrar locales OKMarket que tienen 1 caja hasta locales Unimarc que tienen 30 cajas.

El sistema operativo que utilizan los POS es la versión llamada SUSE Linux Enterprise Point of Service que tiene características específicas para ser utilizadas en retail.

- Balanza Mettler Toledo 8400 e Impact S.
  La diferencia entre ambas balanzas es que la Impact S tiene una pantalla táctil y más memoria RAM mientras que el otro modelo tiene un teclado.
  La cantidad de balanzas por local varía de acuerdo con el tamaño del mismo y su interface de comunicación, es por medio de red Wifi o ethernet.

- Computadores.
  Está compuesta por una gran variedad de modelos y con sistemas operativos que van desde Windows XP hasta Windows 7. Estos son utilizados en distintas áreas del local, por ejemplo, en la recepción, en tesorería, administración, etc. Desde estos equipos también se utilizan los aplicativos que tienen relación directa con la operación del local tales como SAP, Tesorería Online, entre otros.

- Impresora de flejes Datamax 4206.
  Esta impresora se conecta vía USB o paralela a un computador del local para imprimir los flejes de precios.

- Reloj control modelo Kronos 4500.
  Es utilizado para controlar la asistencia del personal del local. Dependiendo del tamaño de este, pueden existir hasta 2 relojes control.

- Impresora térmica Bixolon SP-350.
  Impresora con interface de comunicación ethernet que permite la impresión de un voucher por la marcación realizada por el trabajador en el reloj control. Cada reloj control del local tiene asociada una de estas impresoras.

- Impresora láser multifuncional Ricoh.
  Por lo general cada local cuenta con una unidad y tiene una interfaz ethernet, sin embargo, su supervisión y soporte está dado por contrato con 2 empresas externas a SMU por lo que tampoco están bajo el alcance de este proyecto.

Cada dirección IP asignada a los dispositivos que cuentan con conexión ethernet o wifi, es única para toda la cadena.

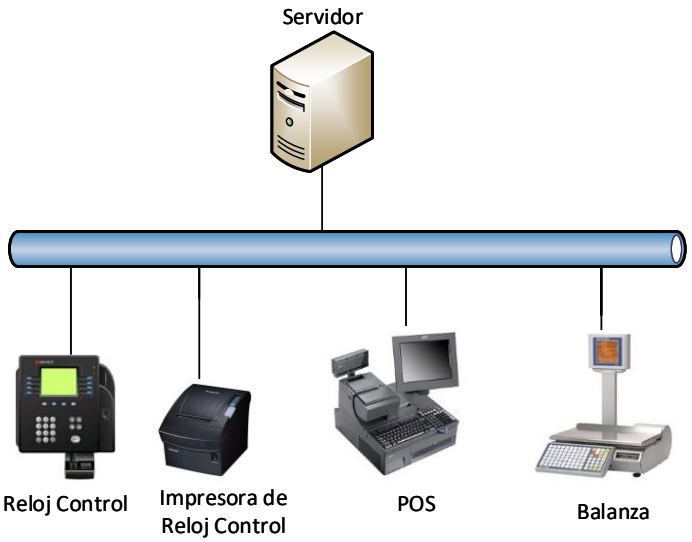

Figura 11: Esquema de comunicación dentro de los supermercados de SMU

3.5.1.2 Software

El software que existe en los locales se puede agrupar de la siguiente forma:

- Sistemas operativos
  Como ya fue mencionado anteriormente, los sistemas operativos existentes son:

  - SUSE Linux Enterprise versión 10 y 11 con SP3
    Utilizado en los servidores de los locales.

  - SUSE Linux Enterprise Point of Service.
    Utilizado en todos los POS de la compañía.

  - Windows
    Desde la versión XP hasta la 7 y se utiliza en los computadores de uso general que existen en los locales.

- Ofimática
  Que abarca programas de uso general como Microsoft Office, Acrobat Reader PDF, Snag IT!, etc.

- Motor de Base de datos
  En los locales se utilizan 2 tipos de motores de datos:

  - Informix
    Este motor de datos se encuentra instalado en su versión 11 y es utilizado en el servidor de cada local de todas las cadenas de SMU. En este motor de datos se concentra la información de ventas generadas por las cajas del local de los últimos 3 meses.

- MySql
  La versión que se encuentra instalada es la 5.1 y existe en cada POS del local y almacena su propia información, la que luego es enviada al servidor para su concentración y posterior envío a otros sistemas externos al local. Entre estos sistemas externos encontramos SAP y aplicaciones BI.

- Soluciones Geocom
  Las soluciones del proveedor Geocom que existen en locales y que permiten su operación son:

  - GEOPos
    Es una solución que permite la gestión del punto de venta.

  - GEOPricer
    Administra la presentación de la cartelería y precios en las góndolas frente a cambios, promociones o daños en las etiquetas.

  - GEOPromotions
    Administra beneficios o promociones por cualquier entidad de la venta, cliente, zona demográfica o segmento social.

  - Tesorería Online
    Administra y gestiona los valores recibidos por las ventas realizadas en los POS.

  - GEOConsole
    Administra la información que se envía a las cajas del local, además de las que éstas envían el servidor del local.

De las soluciones que se indicaron, la única que reside en el POS es GEOPos, el resto, está instalado en el servidor del local y son utilizados a través de una interfaz web.

3.5.2 Consideraciones generales para la implementación y explotación de la herramienta de monitoreo

Debido a que no solo se van a monitorear dispositivos, sino que también el comportamiento de distintos servicios y procesos que permiten la continuidad operacional de los locales es que se tomaron las siguientes decisiones para no interrumpir sus operaciones:

- Consultas a Geocom.
  Dado que algunos plugins o script necesitarán conectarse a las bases de datos de servidores y/o POS para leer información, se validarán con el proveedor Geocom estas consultas con el fin de asegurar la correcta ejecución de ellas y que no afecten o degraden el servicio monitoreado u otro servicio residente en el dispositivo.

- Pruebas en laboratorio QA.
  Se utilizará un servidor y POS del laboratorio de QA de SMU para probar los distintos plugins a desarrollar, esto con la finalidad de minimizar los riesgos de afectar la continuidad operacional de los locales.

- Locales piloto.
  Una vez que hayan finalizado con éxito las pruebas en el laboratorio de QA, se elegirá un número acotado de locales donde serán instalados los plugins de los monitoreos seleccionados.

- Selección de dispositivos y servicios a monitorear.
  Durante las reuniones iniciales con el equipo de Soporte para determinar qué se va a monitorear, fue normal escuchar la palabra “todo”.

  Para seleccionar los monitoreos que se van a realizar en esta primera etapa del proyecto, se eligieron indicadores básicos (dispositivos online, espacio en disco duro, tamaño de memoria RAM libre disponible) y otros relacionados directamente con las operaciones del local, tales como el procesamiento y actualización de precios, existencia de ticket de venta encolados en el POS, entre otros. Más adelante se explicará de qué se tratan los monitoreos a los procesos de los sistemas del local.

- Roles de usuarios para la administración y explotación de la herramienta de monitoreo.
  Para que la explotación de la herramienta de monitoreo sea eficiente, es necesario definir dentro de los equipos de Soporte algunos roles respecto a quién se le enviará la notificación cuando se genere una alerta y cómo se operará respecto a ella.

  Por otro lado, también se debe definir quien oficiará como administrador de la herramienta de monitoreo.

3.6 Implementación de la herramienta de monitoreo

Si bien se realizó la implementación de la herramienta en el Laboratorio de QA utilizando un servidor y un par de cajas de prueba, la instalación de los plugins y otras configuraciones se realizaron de forma manual, esto porque no existía el conocimiento

técnico para su automatización. De la misma forma se realizó la instalación de los tres locales pilotos elegidos. Sin embargo, durante este proceso se contrataron los servicios de asesoría de un experto en Linux con la finalidad de apoyar en la automatización de este proceso y en otros casos donde se requiera el desarrollo de script parar monitorear algún dispositivo o servicio.

El plan piloto de esta herramienta durará un mes y luego se planificará el rollout para su implementación en el resto de las cadenas de SMU. El plazo de este proceso se determinará una vez que se hayan automatizado los instaladores de los aplicativos.

3.6.1 Definiciones para la explotación

Una vez que se tomaron en consideración distintos aspectos para definir los puntos anteriormente señalados, se realizaron las definiciones que a continuación se detallan para la implementación de la herramienta de monitoreo.

3.6.1.1 Locales SMU para pilotos

Se decidió realizar la implementación del plan piloto en 3 locales de la cadena Unimarc de SMU.

Para la elección de estos locales se tomaron en consideración los siguientes aspectos:

- Número de cajas del local.
- Ubicación geográfica y nivel de servicio de los enlaces de comunicaciones.
- Cantidad de transacciones en los puntos de venta.
- Versión de sistema operativo Linux en los servidores de estos locales.

Los locales elegidos son:

- Supermercado Unimarc Los Militares

  Ubicación
  - Av. Manquehue Norte #457.
  - Las Condes.

  Configuración de servidor
  - Sistema operativo SUSE Linux Enterprise 11 SP3
  - Disco duro 70GB
  - Memoria RAM 4GB

  Número de cajas
  - 29 cajas

  Número de balanzas
  - 21 cajas

  Número de reloj control
  - 01 Reloj Control
  - 01 Impresora térmica

- Supermercado Unimarc Recova

  Ubicación
  - Brasil #715, La Serena

  Configuración de servidor
  - Sistema operativo SUSE Linux Enterprise 11 SP3
  - Disco duro 70GB
  - Memoria RAM 6GB

  Número de cajas
  - 32 cajas

  Número de balanzas
  - 18 cajas

Número de reloj control

- 01 Reloj Control
- 01 Impresora térmica

- Supermercado Unimarc Oriente

  Ubicación
  - Julio Buschmann #2223
  - Osorno

  Configuración de servidor
  - Sistema operativo SUSE Linux Enterprise 10 SP3
  - Disco duro 60GB
  - Memoria RAM 4GB

  Número de cajas
  - 29 cajas

  Número de balanzas
  - 11 balanzas

  Número de reloj control
  - 02 Reloj Control
  - 02 Impresora térmica

3.6.1.2 Chequeos por implementar

Si bien la lista de los chequeos abarca un sinfín de aspectos de los dispositivos y servicios que operan en los locales, solo para fines ilustrativos de esta Memoria, se ha decidido mostrar la implementación, ejecución y resultados de los siguientes chequeos:

- Ping
- Espacio libre en disco duro

- Espacio libre en motor de base de datos Informix
- Existencia de transacciones de venta encoladas en las cajas

A continuación, se muestra el detalle de los chequeos mencionados anteriormente.

3.6.1.2.1 Chequeo: Ping

- Objetivo
  Con este chequeo se busca detectar cuando el dispositivo a monitorear se encuentre fuera de línea.

- Dispositivo o servicio por monitorear
  Los dispositivos que se monitorearán en el local son:

  - Servidor de cajas
  - Balanzas
  - Reloj control
  - Impresora del Reloj Control

- Tipo de chequeo
  Este chequeo será configurado como activo, es decir, desde el servidor de Nagios se gatillará su ejecución.

- Período de tiempo
  Se configura para que realice el chequeo y notificación en el siguiente intervalo de tiempo:

  - De lunes a domingo entre las 06:00 AM y las 23:00 PM

- Umbrales para los cambios de estado del chequeo
  Se han definido los siguientes umbrales:

  - Warning: se activará cuando se hayan ejecutado una ronda de ping al dispositivo.

  - Critical: se activará cuando se hayan ejecutado tres rondas de ping al dispositivo.

  La ronda de ping significa que cada 30 segundos se ejecutarán 3 test de ping al dispositivo.

- Notificación y escalamiento

  - Notificación
    Se ha definido que se enviará un correo electrónico al área Soporte Nivel 1 y Soporte Nivel 2 cuando el umbral tenga el valor de **Critical.**

  - Escalamiento
    En caso de persistir la falla, se volverá a enviar un correo a las áreas señaladas anteriormente y se enviará un correo electrónico a la Subgerencia de Operaciones y Formatos TI de la cual dependen las áreas de Soporte mencionadas anteriormente.

3.6.1.2.2 Chequeo: Espacio libre en disco duro

- Objetivo
  Con este chequeo se busca evitar que el disco duro quede sin espacio libre. Además, se ha programado el script para que cuando se llegue al umbral de WARNING por el espacio libre, se ejecute automáticamente el borrado de archivos en algunos directorios predefinidos.

- Dispositivo o servicio por monitorear
  El dispositivo que se monitoreará en el local es:

  - Disco duro del Servidor de cajas

- Tipo de chequeo
  Este chequeo será configurado como pasivo, es decir, el script se ejecuta en el host (servidor del local) y se envía el resultado al servidor de Nagios para su procesamiento.

- Período de tiempo
  Se configura para que realice el chequeo y notificación en el siguiente intervalo de tiempo:

  - De lunes a domingo entre las 06:00 AM y las 23:00 PM

- Umbrales para los cambios de estado del chequeo
  Se han definido los siguientes umbrales:

  - Warning: se activará cuando el espacio libre en el disco duro del servidor sea menor al 20%.

- Critical: se activará cuando el espacio libre en el disco duro del servidor sea menor al 10%.

- Notificación y escalamiento

  - Notificación
    Se ha definido que se enviará un correo electrónico al área Soporte Nivel 1 cuando el umbral tenga el valor de **Critical.**

  - Escalamiento
    En caso de persistir la falla, se volverá a enviar un correo al área de Soporte Nivel 1, además del Soporte Nivel 2 y a la Subgerencia de Operaciones y Formatos TI.

3.6.1.2.3 Chequeo: Espacio libre en motor de base de datos Informix

- Objetivo
  Con este chequeo se busca evitar que el motor de base de datos Informix se quede sin espacio libre, lo que lleva primero a una degradación en la performance del motor de datos Informix y luego, a que ciertos procesos no puedan ser ejecutados tales como la actualización de precios, captura de las ventas realizadas por las cajas, entre otros.

- Dispositivo o servicio por monitorear
  El servicio que se monitoreará en el local es:

  - El motor de base de datos Informix que se encuentra instalado en el Servidor de cajas.

- Tipo de chequeo

  Este chequeo será configurado como pasivo, es decir, el script se ejecuta en servidor del local y se envía el resultado al servidor de Nagios para su procesamiento.

- Período de tiempo

  Se configura para que realice el chequeo y notificación en el siguiente intervalo de tiempo:

  - De lunes a domingo entre las 06:00 AM y las 23:00 PM

- Umbrales para los cambios de estado del chequeo

  Se han definido los siguientes umbrales:

  - Warning: se activará cuando el espacio en el área datadbs del motor de datos Informix sea menor al 20%.

  - Critical: se activará cuando el espacio en el área datadbs del motor de datos Informix sea menor al 10%.

- Notificación y escalamiento

  - Notificación

    En esta etapa de piloto, se ha definido que se enviará un correo electrónico al área Soporte Nivel 1 y Soporte Nivel 2. En el caso de este chequeo, la notificación a Soporte Nivel 1 será meramente informativa ya que se tiene contratado servicios de asesorías externos para resolver los incidentes con el motor Informix, y es deber de Soporte Nivel 2 dar aviso al proveedor.

El correo será enviado cuando el umbral tenga el valor de **Critical.**

- Escalamiento

  En caso de persistir la falla, se enviará un correo electrónico a la Subgerencia de Operaciones y Formatos TI.

3.6.1.2.4 Chequeo: Existencia de transacciones de venta encoladas en las cajas

- Objetivo

  Con este chequeo se busca evitar que las transacciones de venta generadas en las cajas se encolen y no suban al servidor. Este encolamiento provoca que no se puedan realizar las cuadraturas de las ventas de los cajeros de turno, además del envío de la información a los servidores centrales que procesan, entre otros servicios, el stock online de mercaderías y la venta online de los locales.

  Las transacciones de venta se refieren a la venta con boletas electrónicas, facturas electrónicas, entre otros documentos.

- Dispositivo o servicio por monitorear

  El servicio que se monitoreará en el local es:

  - Tabla ticket de la base de datos de las cajas.

- Tipo de chequeo

  Este chequeo será configurado como pasivo, es decir, el script se ejecuta en el host (caja del local) y se envía el resultado al servidor de Nagios para su procesamiento.

- Período de tiempo
  Se configura para que realice el chequeo y notificación en el siguiente intervalo de tiempo:

  - De lunes a domingo entre las 08:00 AM y las 23:00 PM

- Umbrales para los cambios de estado del chequeo
  Se han definido los siguientes umbrales:

  - Warning: se activará cuando se encuentren transacciones de venta con una antigüedad de 15 minutos.

  - Critical: se activará cuando se encuentren transacciones de venta con una antigüedad mayor a 30 minutos.

- Notificación y escalamiento

  - Notificación
    Se ha definido que se enviará un correo electrónico al área Soporte Nivel 1 cuando el umbral tenga el valor de **Critical.**

  - Escalamiento
    En caso de persistir la falla, se volverá a enviar un correo al área de Soporte Nivel 1, además del Soporte Nivel 2 y a la Subgerencia de Operaciones y Formatos TI.

3.6.1.3 Asignación de roles

La Subgerencia TI Operaciones y Formatos, que pertenece a la Gerencia Corporativa Tecnología y Procesos, está compuesta por las siguientes áreas:

- Subgerencia de DesarrolloTI
  Se encarga de los desarrollos de los sistemas del ambiente SAP y de los aplicativos propios del funcionamiento de la tienda, tales como el software de punto de venta, tesorería online, pistolas de radio frecuencia, entre otros.

- Subgerencia FrontOffice y de Operaciones
  Su principal función es garantizar la continuidad operacional de las tiendas y centros de distribución, fijando como objetivo: “Prevenir y atender las necesidades de las tiendas y centros de distribución con sentido de urgencia”.

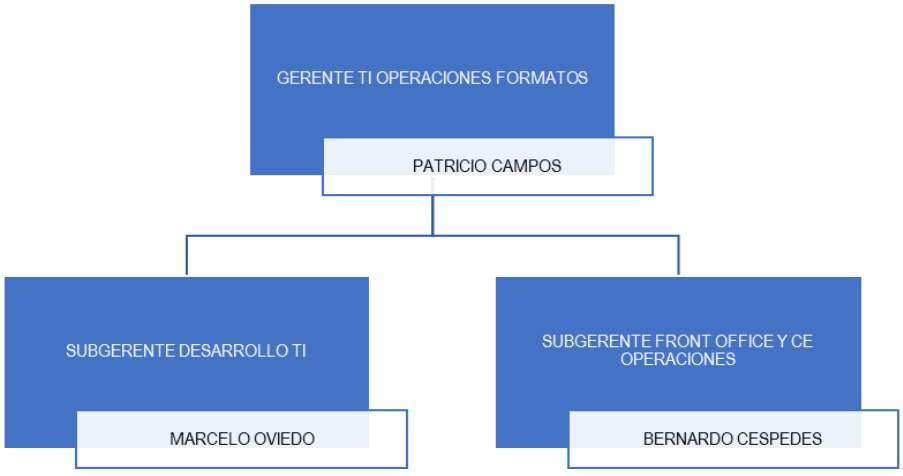

Figura 12: Organigrama de la Gerencia TI Operaciones y Formatos

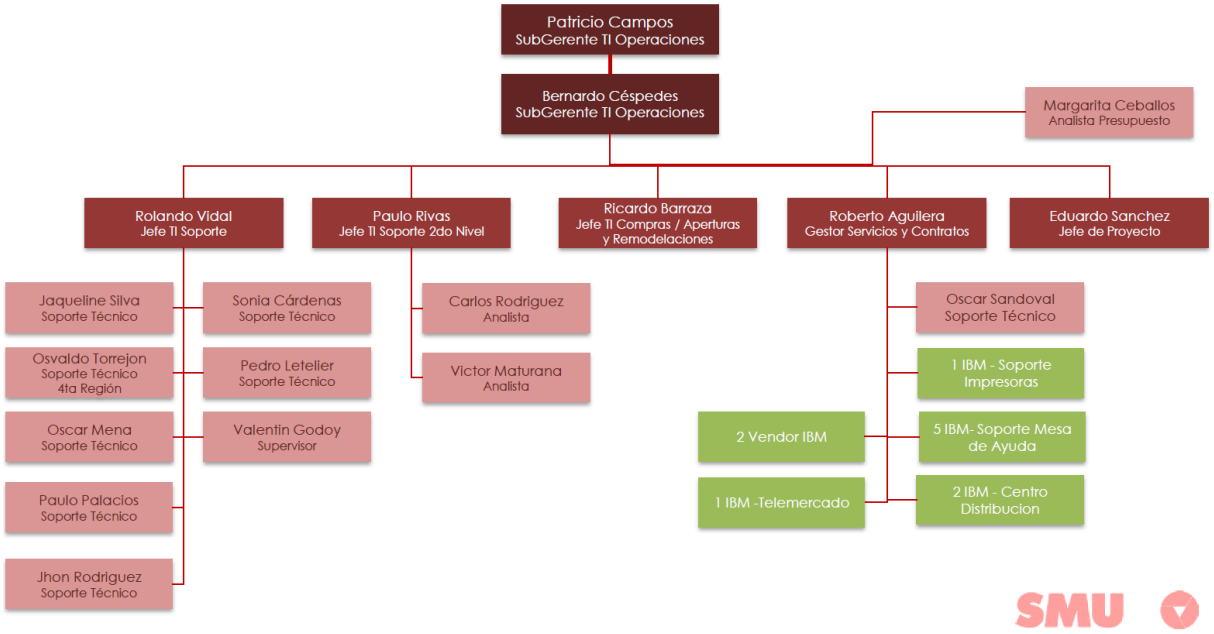

Figura 13: Organigrama de la Subgerencia de Operaciones TI

Es dentro de la Subgerencia FrontOffice y Operaciones que se encuentran las áreas que entregan el soporte de los distintos sistemas de las tiendas y centros de distribución. Estas áreas son:

- Soporte Nivel 1

  Esta área es quien recibe en primera instancia los problemas y/o incidentes que no pueden ser resueltos por la Mesa de Ayuda.

  Está conformada por personal interno y externo que trabajan por medio de turnos que abarcan los 7 días de la semana, desde las 7am hasta las 12am.

  Si esta área no puede resolver el problema o incidente, lo escala al área de Soporte Nivel 2.

- Soporte Nivel 2

  Esta área recibe los problemas y/o incidentes que no pueden ser resueltos por Soporte Nivel 1. Y en caso de que tampoco pueda resolver la incidencia, lo derivada directamente a los proveedores correspondientes, según sea el aplicativo o proceso involucrado.

  Está conformado solamente por personal interno de SMU.

El flujo normal de los reportes de problemas o incidencias de los usuarios está dada por la siguiente figura:

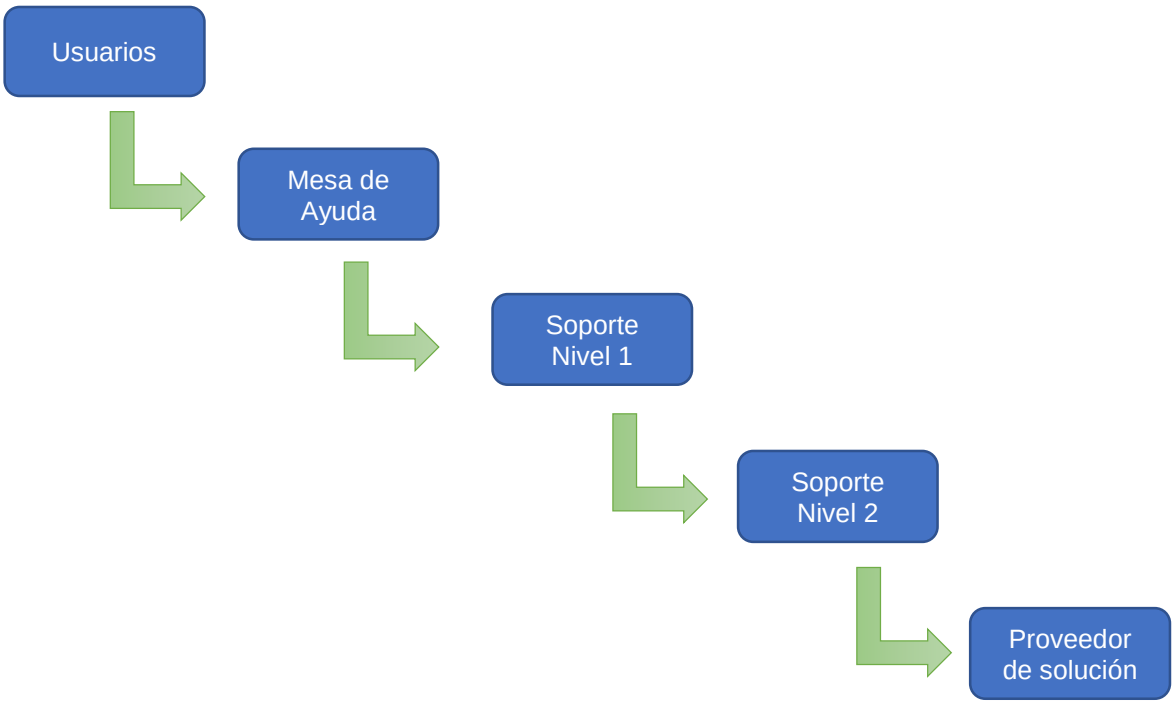

Figura 14: Flujo de reportes de incidencias desde los locales de SMU

Como se puede apreciar en la Figura anterior, la Mesa de Ayuda recibe el llamado del usuario solicitando asistencia siendo registrado en la herramienta Máximo, y lo soluciona si tiene la documentación para realizarlo, de lo contrario, lo deriva o escala al área de Soporte Nivel 1 para su análisis.

Si bien la estructura mostrada en la Figura 14 muestra claramente el flujo que deben seguir los escalamientos de problemas o incidentes ocurridos en los locales, se ha tomado la decisión que las notificaciones de alertas que se generen por los chequeos implementados sean atendidas directamente por las áreas de Soporte que posean las capacidades técnicas para su resolución.

De esta forma, las alertas que necesitan un mayor conocimiento técnico o que luego de un rápido análisis se haga necesario derivarlas a un proveedor externo, serán vistas por el área de Soporte Nivel 2.

Lo expuesto anteriormente es aplicable ya que para los monitoreos pilotos que se van a desarrollar, se les conocen los orígenes que provocan estas alertas.

Para ejemplificar, los chequeos descritos en la presente memoria serán atendidos por:

- Soporte Nivel 1
    - Chequeo Ping
    - Chequeo Espacio libre en disco duro
    - Existencia de transacciones de venta encoladas en las cajas

- Soporte Nivel 2
    - Chequeo Espacio libre en motor de base de datos Informix

3.6.1.4 Administración de Nagios

La administración de la herramienta Nagios será responsabilidad del área de Soporte Nivel 2.

Las tareas que tendrá esta área se pueden dividir en dos y dependen de la finalidad de ellas.

- Por un lado, se encuentran las tareas propias de la administración de la herramienta y entre ellas podemos mencionar las siguientes:
    - Alta y baja de los dispositivos o servicios a monitorear.
    - Mantención de los usuarios con acceso a Nagios.
    - Mantención de las distintas configuraciones del Nagios, tales como:
        - Listas de correos para las notificaciones.
        - Horarios habilitados para realizar los chequeos y para enviar las notificaciones.
    - Mantención de los scripts de chequeos.
- Pero la tarea principal, aquella que permitirá cumplir con los objetivos de la implementación de esta herramienta, es la gestión de las distintas alertas que se generen con la finalidad de realizar un uso eficiente de los recursos de TI y lograr minimizar los riesgos de interrupción de la operación de los locales.

  Entre las tareas que se deben llevar a cabo están las siguientes:
    - Generar informes de los distintos chequeos para detectar la recurrencia en la generación de incidentes con la finalidad de

determinar si existe algún problema en los dispositivos o servicios monitoreados.

- Analizar los tiempos de respuesta y resolución de las alertas generadas por Nagios.

- Evaluar si las configuraciones de chequeo de los dispositivos y servicios son las correctas y/o mejorables. Entre los cambios que se podrían realizar está el ajustar el cuándo se genera la alerta o modificar el período en el cual se realiza el chequeo.

Si bien es importante analizar qué se debe monitorear, cuándo se generará la alerta y el envío de la notificación, es primordial analizar los datos que entreguen los monitoreos, y no solo de las alertas por los incidentes que se generen, sino que además verificar que cuando no se genere una alerta, esta se debe a que el dispositivo o servicio está operando normalmente y no estamos frente a un mal análisis de los parámetros que se configuraron inicialmente para dicho monitoreo.

3.6.1.5 Envío de Notificaciones y Escalamiento

La generación de la alerta de un incidente está dada por cada tipo de chequeo realizado y varía según el tiempo en el cual se cumple el umbral Crítico y la cantidad de veces que se realiza la revisión.

Dado que las áreas de Soporte Nivel 1 y 2 se encuentran en el mismo lugar físico y con la finalidad de mantener una comunicación fluida, las notificaciones serán enviadas a ambos grupos de Soporte. De todas formas y dependiendo de las capacidades técnicas de las áreas, cada chequeo que se realiza tiene definido cual es el área que debe resolver

el incidente y en caso de no lograrlo, seguir el flujo normal de escalamiento de incidentes, tal como se aprecia en la Figura 14.

En general y como parte de este período de implementación de piloto, se estableció que, si el incidente no ha sido resuelto en 24 horas, se enviará una notificación a la Subgerencia TI de Operación y Formato.

Se ha modificado el mensaje que se envía por defecto en el correo de alerta que envía Nagios por otro formateado y más legible.

La siguiente es una muestra del correo de alerta por el servicio PING que ha llegado al umbral de Crítico. En el fondo, esta alerta está indicando que el servidor del local UNI-0469 Los Militares se encuentra fuera de línea:

Notificacion:	**PROBLEM [CRITICAL]**
Servicio:	**PING**
Servidor:	UNI-0469
Direccion IP:	192.168.1.187
Estado:	CRITICAL
Hora/Fecha:	11-05-2017 15:08:11
Mas Info ..	http://192.168.1.181/nagios/cgi-bin/extinfo.cgi?type=2&host=UNI-0469&service=BACKUP
Info Adicional:	PING CRITICAL - Packet loss = 100%
Duracion Estado:	0d 1h 15m 31s

Figura 15: Imagen de correo personalizado de notificación de Nagios

3.6.2 Implementación

Como el objetivo de esta Memoria no es ilustrar ni detallar el paso a paso de la instalación del servidor de Nagios ni de los plugins de los objetos o servicios a monitorear, solo se mencionarán algunos aspectos de dicha instalación. Entre ellos podemos indicar que:

- La instalación de los plugins se realizó en forma manual.
  En el futuro se espera automatizar este proceso ya que la cadena cuenta con alrededor de 2.000 cajas repartidas entre sus distintos formatos.

- La instalación del servidor Nagios se realizó en forma manual al igual que las definiciones de los distintos objetos utilizados en Nagios.
  Entre estos objetos tenemos la configuración de los dispositivos a monitorear, la configuración de usuarios, de los correos para el envío de las notificaciones, entre otros.

- En los servidores de los locales se creó un usuario y un directorio para los scripts de monitoreo.
  Con la intención de encapsular las tareas de monitoreo, se decidió la creación de un usuario para programar en su crontab específico del servidor la ejecución de estos scripts. Se busca con esto no interferir con el crontab asociado al usuario root del servidor que contiene otros scripts relacionados con la operación propia del servidor y de algunos servicios instalados en él.
  Se evaluará el éxito de este punto con miras a ser replicado en los scripts que serán instalados en las cajas de la cadena.

Los chequeos que se realizarán en estos locales son:

- Ping
- Espacio libre en disco duro

- Espacio libre en motor de datos Informix
- Existencia de transacciones de venta encoladas en las cajas

A modo de ejemplo, las siguientes figuras muestran cómo se visualizan algunos de los monitoreos implementados en este piloto.

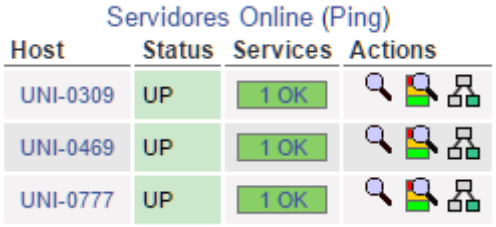

Figura 16: Visualización del estado del chequeo Ping.

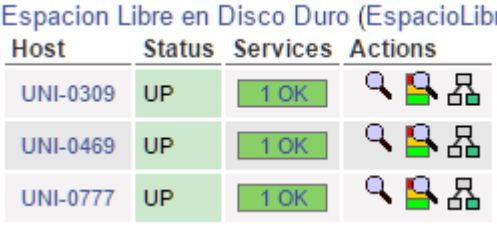

Figura 17: Visualización del estado del chequeo Espacio libre en el disco duro

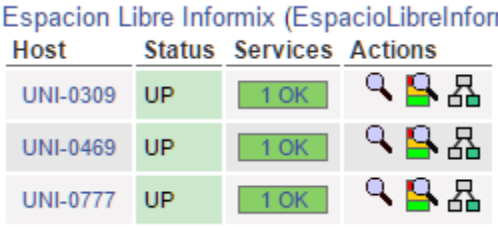

Figura 18: Visualización del estado del chequeo Espacio libre en Informix

Esta imagen muestra todos los servicios configurados, y en la columna *Status Information,* el porcentaje de espacio libre del disco duro y del motor de base de datos:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
UNI-0309	EspacioLibreInformix	OK	12-11-2016 08:56:07	0d 0h 41m 55s	1/3	OK - Espacio Libre 21%
	EspacioLibreSDA1	OK	12-11-2016 09:30:58	0d 0h 7m 4s	1/3	OK - Espacio Libre 20%
	Ping	OK	12-11-2016 09:37:39	0d 0h 52m 23s	1/3	PING OK - Packet loss = 0%, RTA = 0.30 ms
UNI-0469	EspacioLibreInformix	OK	12-11-2016 08:55:50	0d 0h 42m 12s	1/3	OK - Espacio Libre 32%
	EspacioLibreSDA1	OK	12-11-2016 08:55:22	0d 0h 42m 40s	1/3	OK - Espacio Libre 22%
	Ping	OK	12-11-2016 09:37:37	0d 0h 52m 25s	1/3	PING OK - Packet loss = 0%, RTA = 0.31 ms
UNI-0777	EspacioLibreInformix	OK	12-11-2016 08:56:22	0d 0h 41m 40s	1/3	OK - Espacio Libre 23%
	EspacioLibreSDA1	OK	12-11-2016 08:55:10	0d 0h 42m 52s	1/3	OK - Espacio Libre 28%
	Ping	OK	12-11-2016 09:36:49	0d 0h 53m 13s	1/3	PING OK - Packet loss = 0%, RTA = 0.32 ms

Figura 19: Visualización global de algunos de los chequeos habilitados en este piloto

3.7 Ejecución

Si bien el objetivo de esta Memoria no es entregar detalles de la implementación, de los scripts utilizados, etc., no se puede dejar de mencionar que se realizaron pruebas forzadas de las alertas programadas, siendo estas de relativa facilidad debido al modelo pasivo de monitoreo implementado.

Las ejecuciones de estos chequeos se llevaron a cabo sin mayores problemas y dentro de los parámetros configurados inicialmente.

A continuación, se especificará el desarrollo de estos chequeos y se detallarán las alertas que fueron generadas por ellas, el motivo y la consecuencia del análisis de estos.

Es importante destacar que solo se mostrarán los dispositivos o servicios que generaron alguna alerta y, además son casos representativos ya que algunas de ellas se produjeron más de una vez.

3.7.1 Chequeo: Ping

Como se indicó anteriormente, este chequeo busca detectar cuando un dispositivo se encuentre fuera línea. Son variadas las razones por las cuales puede ocurrir esta situación, entre ellas podemos nombrar caída del enlace de comunicaciones del local, problemas con el punto de red al cual está conectado el dispositivo, falla del dispositivo, entre otras.

Durante el período de prueba nos encontramos con la ocurrencia de algunas de estas razones, pero, además de detectó un suceso especial durante el monitoreo de la impresora del reloj control.

El resumen de las alertas generadas por el chequeo y agrupadas por local es el siguiente:

- **Local**
  Unimarc La Recova UNI-0309
    - **Objeto monitoreado**
      Servidor de Cajas.
        - **Motivo de la alerta**
          Pérdida de enlace con el local debido a problemas de comunicaciones en la red de fibra óptica del proveedor Telefónica Chile.
        - **Búsqueda del origen del incidente**
          El proveedor Telefónica Chile indica que se produjo un corte en la fibra óptica que entrega servicio a este local. Agrega además que este corte afectó a otros clientes del área.

- **Solución del incidente**
  La solución fue entregada por el proveedor Telefónica Chile mediante la reparación del corte.

- **Objeto monitoreado**
  Balanza 03, ubicada en la sección de carnicería.

  - **Motivo de la alerta**
    Pérdida de comunicación en distintas oportunidades durante el día.

  - **Búsqueda del origen del incidente**
    Se llama al local y el usuario indica que hay ocasiones en las cuales el trabajador para a tocar el cable de red de la balanza.

  - **Solución del incidente**
    Se envía un técnico del área de redes al local y este informa que el punto de red se encuentra defectuoso procediendo a cambiarlo, también indica que amarra el cable de red al mueble de carnicería para impedir que los trabajadores lo pasen a tocar.

- **Objeto monitoreado**
  Balanza 02, ubicada en la sección de envasado.

  - **Motivo de la alerta**
    Pérdida de comunicación en distintas oportunidades durante el día.

- **Búsqueda del origen del incidente**

  Se llama al local y el usuario indica que, como esta balanza se encuentra en la sección donde se envasan los cortes carnes y pollo para la venta en las islas de autoservicio, el trabajador apaga la balanza una vez que ha dejado de usarla.

- **Solución del incidente**

  Se instruye a usuario para que comunique a los trabajadores que utilizan esta balanza que no deben apagarla, debe estar siempre encendida para que reciba las actualizaciones de precios que pueden llegar en cualquier momento del día.

- **Objeto monitoreado**

  Reloj Control.

  - **Motivo de la alerta**

    Pérdida de comunicación en distintas oportunidades durante el día.

  - **Búsqueda del origen del incidente**

    Se llama al local y el usuario indica que, el conector del cable de red se encuentra con sus filamentos al descubierto, no tiene la capa protectora de plástico.

  - **Solución del incidente**

    Se envía un técnico del área de redes al local para que cambie el cable de red del reloj control y adicionalmente, revise el estado

del cable de red de la impresora del reloj control y de los puntos de red al que están conectados ambos dispositivos.

- **Local**

  Unimarc Los Militares UNI-0469

  - **Objeto monitoreado**

    Balanza 01, ubicada en la sección de rotisería.

    - **Motivo de la alerta**

      Pérdida de comunicación.

    - **Búsqueda del origen del incidente**

      Se llama al local y el usuario indica que la balanza no enciende.

    - **Solución del incidente**

      Se envía un técnico al local para que realice una revisión de la balanza.

      El análisis del técnico indica que falló la placa madre de la balanza y que su origen puede estar en que el interior de la balanza estaba con suciedad por falta de una mantención preventiva.

      Se solicitará el cambio de la pieza para reponer en servicio la balanza.

      Además, se está gestionando con los proveedores un acuerdo que permita realizar mantenciones preventivas y no solo correctivas a las balanzas, además de otros dispositivos que no cuentan con este servicio.

- **Objeto monitoreado**
  Balanza 02, ubicada en la sección de envasado.

  - **Motivo de la alerta**
    Pérdida de comunicación en distintas oportunidades durante el día.

  - **Búsqueda del origen del incidente**
    Se llama al local y el usuario indica que, como esta balanza se encuentra en la sección donde se envasan los cortes carnes y pollo para la venta en las islas de autoservicio, el trabajador apaga la balanza una vez que ha dejado de usarla.

  - **Solución del incidente**
    Se instruye a usuario para que comunique a los trabajadores que utilizan esta balanza que no deben apagarla, debe estar siempre encendida para que reciba las actualizaciones de precios que pueden llegar en cualquier momento del día.

- **Objeto monitoreado**
  Impresora del Reloj Control.

  - **Motivo de la alerta**
    Pérdida de comunicación con el dispositivo.

  - **Búsqueda del origen del incidente**
    Se llama al local y el usuario indica que apagó la impresora porque se le acabó el rollo de papel para la impresión de los

voucher de marcaciones, y ésta comenzó a alertar de esta situación con un “molesto” bip de alerta constante.

- **Solución del incidente**
  Se instruye al usuario para que maneje un stock apropiado de rollos de papel para evitar esta situación, además, desconocía que el rollo de papel utilizado en las impresoras térmicas de caja para la emisión de las boletas, también le sirve esta impresora dado que utilizan la misma tecnología de impresión.
  Adicionalmente, se le comunicó al área de Servicio a Personas de este caso para que reforzara lo indicado al usuario del local y que lo difundiera también al resto de los locales de la cadena.

3.7.2 Chequeo: Espacio libre en disco duro

Este chequeo se concibió para prevenir que el servidor se quedara sin espacio libre en el disco y en caso de generarse esta incidencia, notificar al área de Soporte Nivel 1. Si bien en un principio esta alarma funcionó para el caso que se expondrá, ocurrieron eventos de este tipo en locales que no estaban dentro de los pilotos de este proyecto, lo que llevó a que se modificara la concepción inicial de este monitoreo. Más adelante, en las conclusiones se profundizará sobre este tema.

El resumen de las alertas generadas por el chequeo y agrupadas por local es el siguiente:

- **Local**
  Unimarc Oriente UNI-0777

  - **Objeto monitoreado**
    Disco duro del Servidor de Cajas

- **Motivo de la alerta**
  Espacio libre en el disco duro de un 92%

- **Búsqueda del origen del incidente**
  Se realizó una actualización de versión al aplicativo GEOPricer y se realizaron respaldos de este y de la base de datos para que, en caso de ser necesario, se realice un rollback del procedimiento de actualización de versión.

- **Solución del incidente**
  Se eliminaron archivos temporales, archivos LOG y algunos respaldos antiguos de aplicativos y base de datos.
  El espacio disponible luego del borrado de archivos fue de un 72%.

3.7.3 Chequeo: Espacio libre en motor de datos Informix

Durante el período que se llevó a cabo el monitoreo en los locales piloto, no se generaron incidentes relacionados con este chequeo.

3.7.4 Chequeo: Existencia de transacciones de venta encoladas en las cajas

Como se indicó anteriormente, las transacciones de venta generadas en las cajas de los locales deben ser enviadas, casi inmediatamente, al servidor del local y luego a otros servidores centrales donde estos datos son utilizados por distintos procesos, tales como

cuadratura de venta de los cajeros del local, información sobre stock y venta online, entre otros.
La necesidad de incluir este chequeo nació de los incidentes reportados por los locales cuando no se podían realizar las cuadraturas de venta.

- **Local**
  Unimarc Oriente UNI-0777

    - **Objeto monitoreado**
      Tabla ticket de la base de datos de las cajas.

        - **Motivo de la alerta**
          Se registraron tickets de venta pendientes de envío al servidor con una antigüedad mayor a los 30 minutos.

        - **Búsqueda del origen del incidente**
          Se detecta que se almacenó un caracter extraño en el nombre de un cliente cuando se le realizó una factura de venta. En este caso, el dato llegó de esta forma desde la plataforma de fidelización de clientes.

        - **Solución del incidente**
          Se corrigió el carácter extraño, que correspondía a una vocal con acento, por el correcto lo que permitió que el ticket fuera enviado al servidor y el resto de ellos que se encontraban encolados.
          Al mismo tiempo, se envió un correo electrónico al área de Fidelización para que modificara el carácter que ocasionó el problema.

3.8 Análisis de la ejecución y resultados de los chequeos

Es importante identificar que la ejecución de los chequeos debe analizarse desde dos puntos de vista. Por un lado, tenemos el funcionamiento propio del sistema de monitoreo Nagios y por el otro, los distintos chequeos que se crearon para este piloto.

Por este motivo, al revisar y analizar estos puntos separadamente, se buscará responder lo siguiente:

- Evaluar si la solución de sistema de monitoreo seleccionada, Nagios, cumple con las características necesarias para lograr los objetivos declarados en esta Memoria.

- Si la creación y definición de los chequeos es correcta y cumplen con la finalidad para la que fueron diseñados.

3.8.1 Análisis de la ejecución del sistema de monitoreo Nagios

Durante el tiempo de ejecución de este proyecto piloto, el sistema de Nagios como herramienta de monitoreo, se ha mantenido estable en su funcionamiento. No fue necesario realizar cambios en su configuración, más que algunos por errores menores en los parámetros configurados, tales como direcciones IP de los servidores, nombre de archivos, entre otros.

Sobre la ejecución de la herramienta de monitoreo Nagios, podemos destacar algunos puntos importantes, tales como:

- Disponibilidad

  No se han producido caídas inesperadas de los servicios propios de Nagios, lo que habla de su correcta instalación y configuración, así como del sistema operativo Suse Linux sobre la cual se encuentra instalada esta herramienta.

- Performance.

  No se ha observado una ralentización del servidor donde se encuentra alojado y tampoco, respecto al tiempo de respuesta de las alertas y visualizaciones e interacciones con la página web de Nagios.

  De todas formas, es importante señalar que el tiempo transcurrido de evaluación de este piloto y la cantidad de chequeos existentes no es significativa, es menor, aun así, la performance hasta ahora ha sido impecable.

- Escalabilidad.

  Si bien el número de chequeos existentes en este piloto no es muy grande, el comportamiento hasta ahora permite asumir que no existirán mayores problemas para ir aumentando la cantidad de locales monitoreados, así como también la cantidad de chequeos por incorporar.

- Configuración.

  Existen distintas formas de configurar Nagios, por un lado, está la creación y modificación de los distintos objetos utilizados en los chequeos mediante un editor de texto de Linux, como puede ser el aplicativo VI, hasta algunos plugins que permiten realizar esta labor gráficamente mediante una página web. Por el momento se ha decidido no utilizar ningún tipo de plugins en esta etapa de piloto, así que se ha utilizado el editor VI para crear y modificar los distintos archivos de configuración. Esta tarea puede ser desarrollada mientras el sistema de monitoreo está funcionando, solo se deben reiniciar los servicios de Nagios para que éste asuma la nueva configuración. Nagios también permite que se puede evaluar si las configuraciones están correctas mediante un

programa que se puede ejecutar desde la consola de Linux. Esto es muy útil ya que, de encontrarse un error de sintaxis en los archivos de configuración, el programa de validación envía el mensaje mediante la consola señalando además la ubicación del error. Todo esto permite que Nagios pueda seguir trabajando con la configuración anterior correcta, no logrando interrumpir en ningún momento el monitoreo. Es importante señalar que esta funcionalidad fue utilizada luego de detectar algunos errores realizados en la configuración de los chequeos y que debieron ser corregidos de esta forma.

- Backup de archivos de configuración.
  Dado que la configuración de los objetos utilizados en el monitoreo es a través de múltiples archivos de texto ubicados en directorios específicos, el backup o respaldo de estos archivos fue realizado manualmente mediante la copia de estos a otro servidor. Fue este un proceso simple y rápido ya que los archivos no son de gran tamaño.

3.8.2 Análisis de la ejecución de los chequeos

Como se señaló anteriormente, la ejecución de los monitoreos se llevó a cabo dentro de los parámetros esperados, salvo algunos inconvenientes menores, errores como la configuración del período de monitorización, la ubicación de los archivos de script, entre otros. Estos errores de configuración fueron corregidos tempranamente por lo que el desarrollo del monitoreo se desarrolló sin problemas.

En SMU no existe una herramienta de monitoreo que permita prevenir y/o alertas de incidencias que afecten la continuidad operacional de los locales. Sí existen algunas

herramientas pero que pertenecen a proveedores externos y que monitorean principalmente los sistemas y enlaces de comunicaciones, y otros proveedores externos que monitorean sus propios servicios, tales como base de datos, datacenter, entre otros.

Esta situación, que es la que se quiere corregir, nos lleva también a no tener historial de los chequeos que se han implementado en este piloto. A pesar de que estos chequeos representan incidentes que se han presentado en los locales y de los cuales existen registros a través de ticket en la herramienta Máximo de la Mesa de Ayuda, estos solo permiten cuantificar la cantidad de veces que se han producido estos incidentes. Esta herramienta Máximo aún no es asimilada correctamente por los distintos actores que interactúan con ella, por lo que no es posible determinar con exactitud el tiempo que lleva al técnico resolver la incidencia.

Sin embargo, durante el tiempo transcurrido en este piloto, ocurrieron las incidencias que se chequean en otros locales que no se encuentran bajo monitoreo lo que permitió realizar una comparación entre los tiempos de reporte del local a la Mesa de Ayuda hasta la solución de la incidencia, versus la respuesta del técnico que recibe la alerta a través de la herramienta Nagios.

Sobre los tiempos involucrados para la solución de los distintos incidentes, las estadísticas fueron obtenidas usando el tiempo en el cual se recibe la alerta desde Nagios hasta que se deriva a otra área para su solución, de lo contrario, el tiempo que le llevó a alguna de las áreas de Soporte su solución, si esta se encontraba dentro de su ámbito de conocimiento.

Dado que los chequeos creados en este piloto buscan objetivos propios, es que se analizará la ejecución de ellos en forma separada para una mayor claridad.

3.8.2.1 Análisis de la ejecución del chequeo Ping

Este tipo de chequeo es una parte básica y esencial para prevenir y anticiparse a los problemas que se originan cuando un dispositivo se encuentra fuera de línea. Por un lado, los servidores deben estar en línea para recibir los cambios de precios de los productos, así como también para capturar la información de ventas que se generan en las cajas del local. Las cajas, por otro lado, deben estar en línea para recibir las actualizaciones de precios, y si una de ellas no las recibe provocará que se vendan productos con diferencias de precios generando la emisión de notas de crédito para subsanar esta situación, y obviamente la molestia de los clientes quienes, generalmente, atribuyen a estas incidencias a una política de la compañía con el objetivo de engañarlos. También no es menor la situación de incomodad y estrés que provoca toda esta situación en el personal de cajas que son la cara, la primera línea de atención al cliente.

Si bien el área de telecomunicaciones monitorea los distintos enlaces de comunicaciones, también es cierto que todavía no existe una cultura de notificar a todas las áreas que se pueden ver afectadas cuando ocurre alguna circunstancia de pérdida de comunicaciones. Por ello cuando se recibió notificación desde Nagios porque el servidor del local Unimarc La Recova se encontraba fuera de línea, la respuesta del área de Comunicaciones TI fue que el problema se debía a la fibra óptica y que el proveedor Telefónica Chile ya se encontraba revisando esta situación.

De todas formas, la generación de esta alerta permite informar de esta situación al resto del equipo que entrega Soporte directo a las tiendas, por lo tanto, sigue siendo una herramienta útil de información para estas áreas.

Una vez que el proveedor Telefónica solucionó el problema de corte, esta situación fue informada por el área de Comunicaciones a las áreas de Soporte quienes tuvieron luego que revisar el estado del servidor y cajas, además de chequear el correcto funcionamiento de los servicios de actualización de precios y captura de ventas.

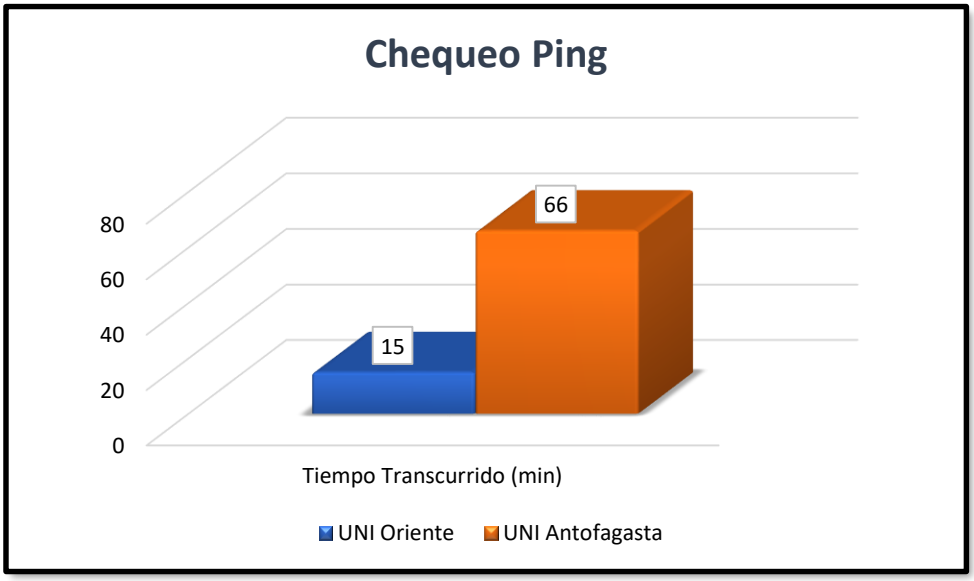

Figura 20: Gráfico comparativo de tiempo de resolución para el chequeo Ping

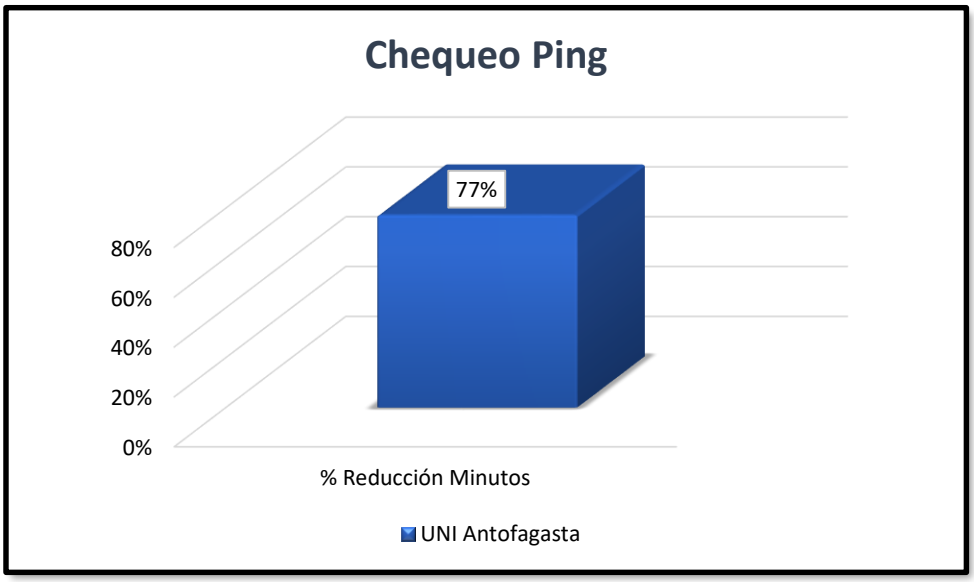

Figura 21: Gráfico de la reducción de tiempo en la resolución de la incidencia de un local monitoreado versus uno sin monitorear

El gráfico relacionado con el caso de la pérdida de enlace con el local La Recova, muestra el tiempo que demoraron las áreas de Soporte en informarse sobre la ocurrencia de este incidente.

Aun así, se puede apreciar que existe una disminución del 77% en el tiempo de respuesta respecto a un local que no se encuentra monitoreado, independiente que la función de estas áreas solo sea notificar o consultar a las áreas de Comunicaciones TI sobre cuál es el motivo de la pérdida de comunicaciones con este local.

Las alertas recibidas por balanzas fuera de línea generaron que se reaccionara de dos formas:

- El mal estado de los puntos de red de balanza ya sea por cables sueltos que son pasados a traer por parte de los colaboradores de las áreas donde estas se encuentran instaladas o las rosetas sueltas, llevaron a la necesidad de programar y ejecutar mantenciones preventivas de los distintos dispositivos del local que se comunican a través de una red ethernet. Esta necesidad llevó a que se revisaran los contratos existentes con algunos proveedores para entregar este tipo de soporte y se logró que, sin modificar el contrato actual y obviamente sin aumentar el costo de éste, el proveedor realizara una visita técnica a los locales con el fin de evaluar y corregir el estado de estas instalaciones.

- Respecto a algunos casos en que las balanzas fueron apagadas por los usuarios de éstas, se les indicó directamente que al apagarlas se impide que los precios sean actualizados en ellas y que provoque un encolamiento y sobrecarga de procesos en el servidor ya que este intentará enviar cada cierto tiempo los cambios de precios a esa balanza.

Esta solicitud también fue reforzada por el área de Operaciones a la cual se le solicitó apoyo para la comunicación de todos los locales sobre este tema en particular.

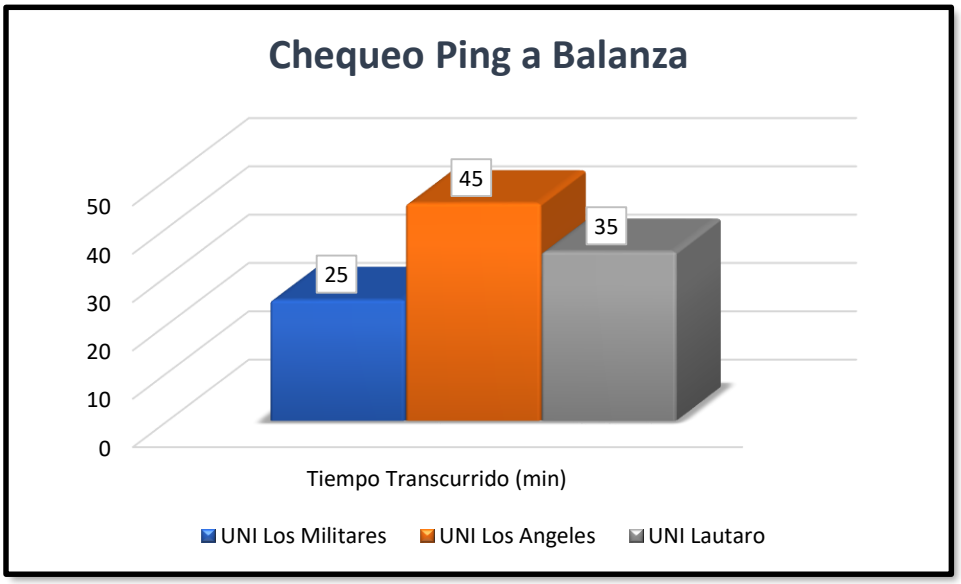

Figura 22: Gráfico comparativo de tiempo de resolución para el chequeo Ping a Balanza

En este gráfico, se comparó el tiempo que transcurrió desde que se recibió la alerta desde Nagios en el local Unimarc Los Militares hasta que se escaló al proveedor externo para que visitara el local, versus, el tiempo transcurrido desde que se reportan problemas de precios no actualizados en balanzas a través de la Mesa de Ayuda hasta que se escala al proveedor externo para realizar una visita al local y revisar el estado de las conexiones de red de las balanzas involucradas.

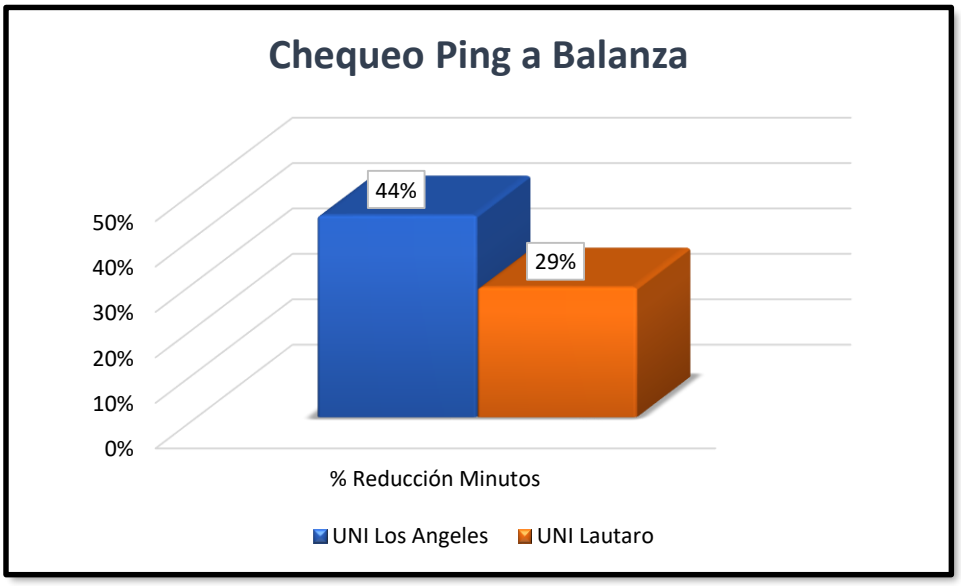

Figura 23: Gráfico de la reducción de tiempo en la resolución de la incidencia de locales monitoreados versus uno sin monitorear

Claramente podemos ver como se ha reducido el tiempo de respuesta desde un 29% hasta un 44% en el reporte realizado por el usuario del local Unimarc Los Angeles.

El caso de las alertas generadas por el monitoreo del reloj control y su impresora, es muy similar a lo expuesto en el chequeo de las balanzas.

- El reloj control también fue agregado a la revisión preventiva por parte del proveedor externo.

- Sobre la impresora que fue apagada por el usuario del local porque se quedó sin papel, se le instruyó que debe manejar un stock de papel suficiente y que las impresoras de cajas poseen el mismo tipo de papel, de esta forma puede pedir prestado hasta que recibe el pedido. También se le solicitó al área de Personal que reforzara mediante una comunicación directa a todos los usuarios de Servicios de Personas de la cadena lo expuesto anteriormente.

Para la compañía es importante que el reloj control e impresora se encuentren en línea para que cuando el colaborador marque su ingreso o salida al local, se imprima el voucher de respaldo de esta situación. Este punto ha sido “reclamado” en otras oportunidades por los Sindicatos de los locales que, por este u otro motivo, no reciben el voucher de la marcación realizada como respaldo.

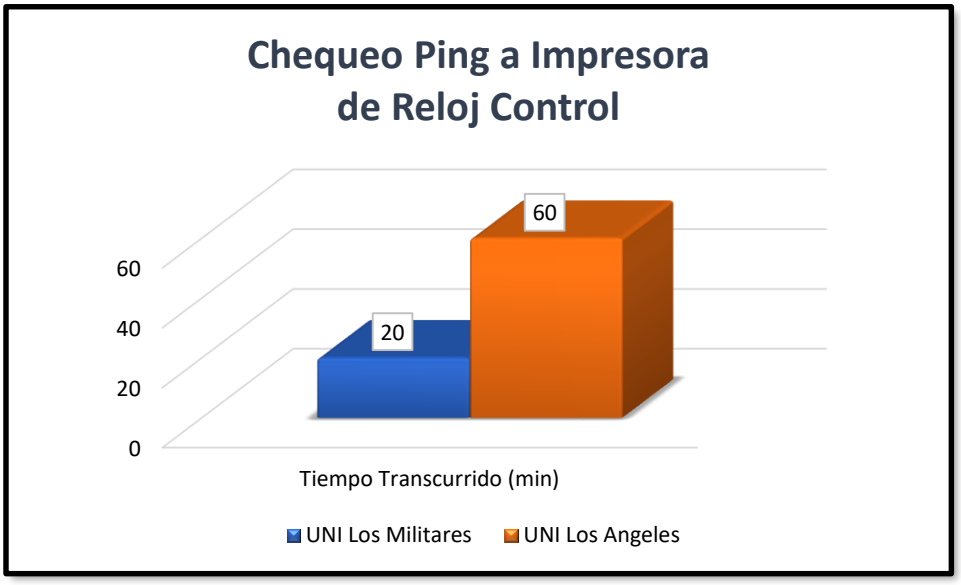

Figura 24: Gráfico comparativo de tiempo de resolución para el chequeo a Impresora de Reloj Control

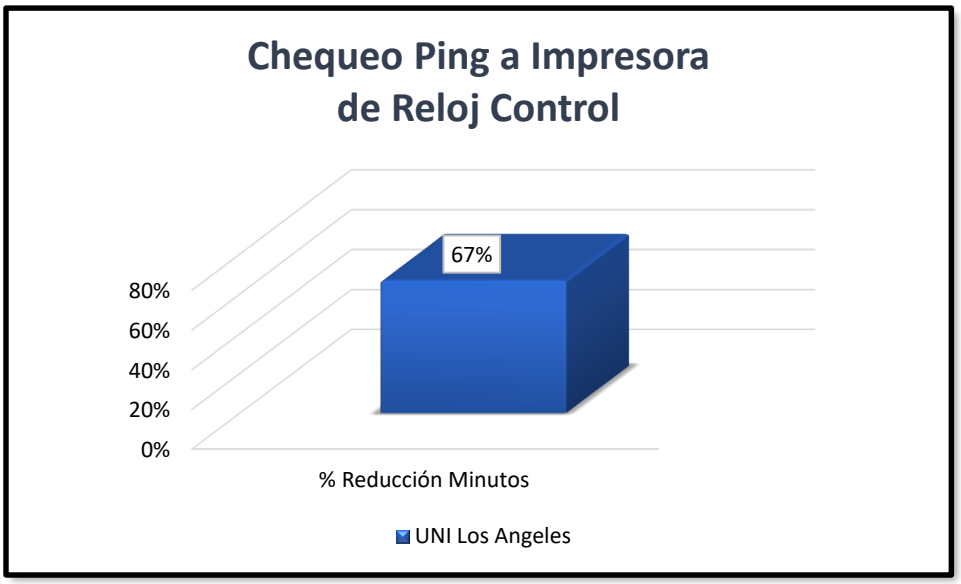

Figura 25: Gráfico de la reducción de tiempo en la resolución de la incidencia de un local monitoreado versus uno sin monitorear

En los gráficos anteriores, podemos ver cómo ha disminuido el tiempo de atención para estos requerimientos llegando a un 67% menos.

En este caso en particular, debemos señalar que el tiempo se evalúa desde que se recibe la alerta o el ticket que el usuario creó en la Mesa de Ayuda hasta que el técnico de Soporte se comunica con este usuario. Esta medición se realiza de esta forma porque existen oportunidades en las cuales cuesta comunicarse con el usuario o este se encuentra ocupado. Una vez que se establece la comunicación, se realizan pruebas remotas de revisión del cableado y de los puntos de red, y dependiendo del resultado de éstas, se define si se deriva al proveedor externo encargado de las comunicaciones o al proveedor que tiene el contrato de servicios con las impresoras, esto porque ha ocurrido en ocasiones que es la impresora la que no enciende o que tiene dañado el puerto de comunicaciones ethernet.

3.8.2.2 Análisis de la ejecución del chequeo Espacio libre en disco duro

Cuando un disco duro del servidor de un local se queda sin espacio libre, provoca que este no pueda recibir los cambios de precios que son enviados desde SAP y tampoco que capture la venta que se genera desde las cajas. Ambos casos afectan a diferentes procesos y áreas interesadas en la información que se produce en los casos señalados anteriormente.

Si bien en un principio de diseñó con la finalidad de prevenir que el disco duro no se llenara debido a los archivos que se generan normalmente con los distintos programas y servicios que se encuentran instalados en el servidor, tales como archivos LOG generados por el servidor HTTP Apache, el servicio GeoPricer que procesa los cambios de precios recibidos desde SAP, archivos propios del sistema operativo Linux Suse, este punto de vista cambió cuando se generó una incidencia en un local que no se encontraba monitoreado en este piloto.

El incidente que se señala ocurrió en el local Unimarc Temuco. El Administrador del local mencionado, reportó a la Mesa de Ayuda que no habían recibido los cambios de precios correspondientes al día. Luego de las revisiones básicas ejecutadas por el área de Soporte Nivel 1, tales como verificar que el servidor se encontrara en línea, que los servicios del proceso GeoPricer se encontraran operativos, se detectó que el disco duro del servidor se encontraba con solo 1% de espacio libre disponible. Luego de borrar manualmente algunos archivos LOG y otros archivos de respaldo, el espacio disponible aumentó, pero en solo unos minutos volvió a disminuir al 1%. Soporte Nivel 1 escaló este incidente a Soporte Nivel 2 quien detectó que el motor de base de datos Informix estaba generando archivos temporales de más de 5 Gigabytes. Finalmente se escaló con el DBA del proveedor Geocom para que revisara el estado de la base de datos, detectando que existían índices corruptos en la base de datos y que Informix intentaba autoreparar creando los archivos temporales, pero que al quedar sin espacio en el disco duro no finalizaba. Finalmente, el DBA realizó un proceso manual de reparación de la base de

datos quedando este operativo luego de 8 horas desde que el usuario creó el ticket en la Mesa de Ayuda, y 7 horas desde que el área de Soporte Nivel 1 comenzara con la revisión del incidente.

Esta situación ha llevado a que se esté planificando crear un nuevo tipo de monitoreo. Este tendrá la responsabilidad de supervisar el directorio específico que es utilizado por el motor de base de datos Informix para almacenar sus archivos temporales de intercambio, velando que el tamaño de estos no exceda un máximo que se debe definir. Esta medida es importante ya que es una forma de verificar el estado de funcionamiento del motor de base de datos, no solo basta con saber si el servicio Informix se encuentra "levantado", hay que supervisar otros aspectos.

Respecto al caso del local Unimarc Oriente cuyo espacio de disco duro disponible fue alertado por Nagios, se acordó con el proveedor Geocom que se mantendrá solamente el respaldo de la última versión de los aplicativos que vayan a ser actualizados, además de asignar una ruta específica para estos respaldos.

Si bien el borrado de los archivos se ejecutó manualmente siguiendo algunas rutas preestablecidas, se ha determinado realizar a futuro un cambio en el diseño de este monitoreo. Se ha decidido modificar el comportamiento de este cuando se cumplan los umbrales establecidos, y en vez de que cambie el estado a Warning cuando el espacio libre del disco duro sea menor al 20% y a Critical cuando sea menor al 10%, cuando el espacio libre sea menor al 25%, se ejecutará automáticamente un script que borrará algunos archivos predefinidos y solo se enviará una notificación desde Nagios cuando el espacio libre sea menor al 15%.

Este nuevo proceder permitirá que este monitoreo no solo sea informativo, sino que permitirá realizar una acción preventiva, permitiendo que una situación actual pase de reactiva a proactiva.

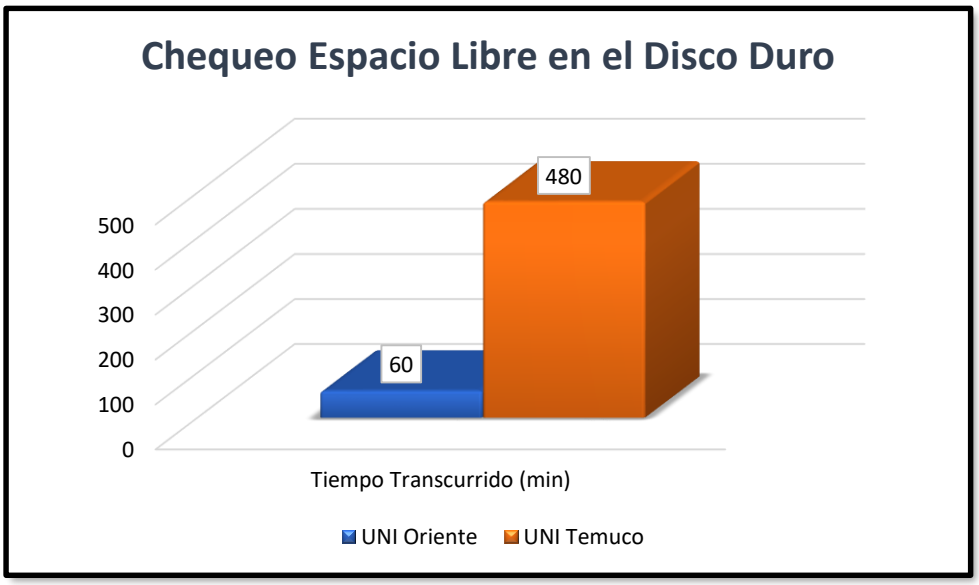

Figura 26: Gráfico comparativo de tiempo de resolución para el chequeo Espacio Libre en el Disco Duro

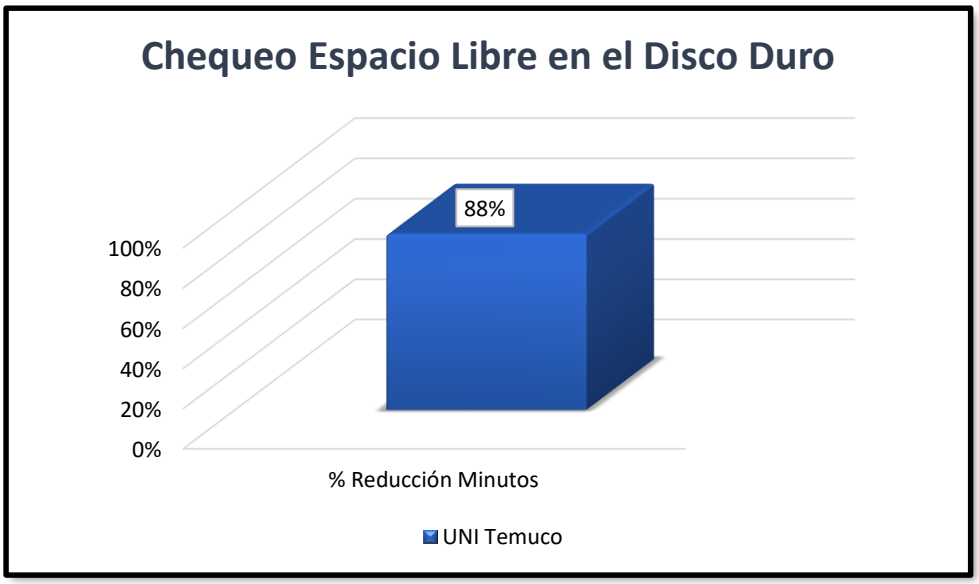

Figura 27: Gráfico de la reducción de tiempo en la resolución de la incidencia de un local monitoreado versus uno sin monitorear

Tal como se aprecia en los gráficos, la reducción del tiempo de respuesta en minutos para este caso es de un 88%, de pasar de 8 horas a 1 hora y sin que los usuarios del local se enteraran que el disco duro se estaba quedando sin espacio libre.

En ningún caso se vieron interrumpidas las labores operacionales del local, ratificando de esta forma que para una compañía como SMU, es necesario contar con una herramienta de monitoreo constante.

3.8.2.3 Análisis de la ejecución del chequeo Espacio libre en motor de datos Informix

Este monitoreo fue agregado en este piloto debido a que se tuvieron ocurrencias de esta incidencia en los servidores de otros locales. Esta problemática produce que cualquier interacción entre los servicios y el motor de base de datos Informix se interrumpa, tales como la actualización de precios o captura de ventas generadas en las cajas del local.

Este chequeo realiza una verificación directamente en el motor de datos utilizando un script. Dado que a estos servidores se le realizó una mantención a la base de datos mucho antes de la implementación del monitoreo con Nagios, no se ha producido alguna incidencia respecto a este monitoreo.

Sin embargo, se modificaron en una oportunidad los umbrales establecidos para que se activara el estado Critical cuando el espacio libre de Informix fuera menor a un 35%. Esto tuvo como finalidad medir los tiempos de respuesta de los escalamientos establecidos para este monitoreo y compararlo con una incidencia ocurrida en el local Unimarc Coquimbo de la cual se tiene registro del ticket levantado por el usuario del local en la Mesa de Ayuda.

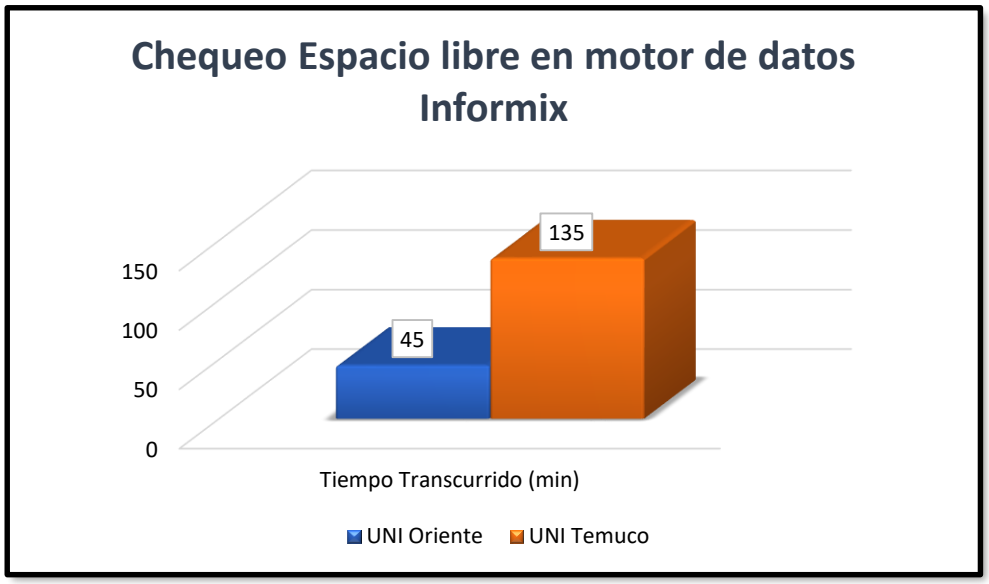

Figura 28: Gráfico comparativo de tiempo de resolución para el chequeo Espacio libre en motor de datos Informix

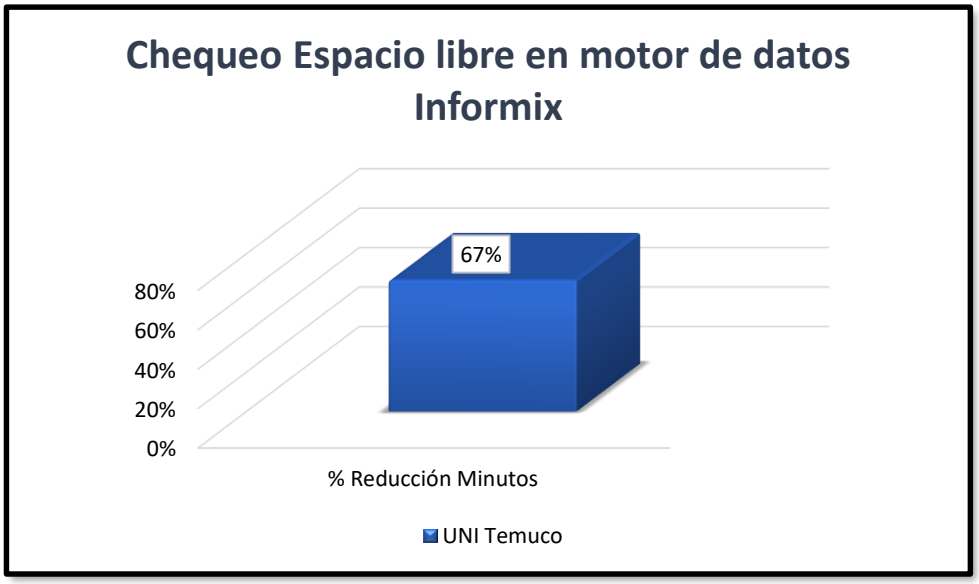

Figura 29: Gráfico de la reducción de tiempo en la resolución de la incidencia de un local monitoreado versus uno sin monitorear

Como ha ocurrido con el resto de los chequeos, podemos apreciar cómo se ha reducido el tiempo de respuesta para este requerimiento, recordando que este incidente fue gatillado a propósito para evaluar la configuración del monitoreo y los tiempos de respuesta de los técnicos de Soporte Nivel 1.

3.8.2.4 Análisis de la ejecución del chequeo Existencia de transacciones de ventas encoladas en las cajas

Este monitoreo fue creado para detectar, al menos según los casos anteriores, cuando las ventas de las cajas no son capturadas por el servidor del local. Hasta ahora, se han detectado dos situaciones que generan esta incidencia:

- La existencia de un carácter de control en alguno de los campos del cliente como pueden ser, el nombre, la dirección y/o el giro comercial.

- Existencia de algún incidente en el servidor del local. Algunos de ellos ya se encuentran monitoreados en este piloto, tales como el espacio libre en el disco duro del servidor del local y el espacio libre en el motor de base de datos Informix.

Si bien existen otros servicios que operan en el servidor del local y son los encargados de capturar la información generada desde las cajas, estos no se han incorporado en este monitoreo piloto, sin embargo, si se tiene proyectado incorporarlos más adelante.

La ocurrencia de este incidente en el local Unimarc Oriente se debió a que en el nombre del cliente existía un caracter de control ASCII que impedía que los registros fueran capturados por el servidor, provocando además que no solo quedaran encolada la

información en la caja donde se genera la alerta por Nagios, sino que afecta a otras cajas del local.

Cuando se ingresa el rut del cliente, ya sea para realizar la venta por medio de una factura o nota de crédito electrónica, o para acceder a las promociones existentes en el local asociados al rut, la caja solicita los datos de este cliente a la plataforma de fidelización mediante un servicio web, y es desde esta plataforma que vienen todos los datos básicos del cliente, incluidos estos caracteres de control. A pesar de que se ha solicitado a la plataforma de fidelización la corrección de estos datos mediante algún filtro u otra revisión, no ha existido respuesta positiva ya que esta modificación genera costos monetarios y el impacto es acotado.

Este monitoreo debe ser afinado ya que, si bien se levanta la alerta, se deben revisar diferentes procesos para encontrar el origen del encolamiento de la información en las cajas. Por ahora, no se revisan automáticamente los campos en las tablas donde se almacenan los datos de los clientes.

El procedimiento actual que se sigue cuando este encolamiento es producido por un caracter extraño es el siguiente:

- El técnico de Soporte Nivel 1 envía un correo al área de fidelización solicitando que se corrija el campo de los datos básicos del cliente que tiene el caracter de control ASCII.

- Elimina manualmente el carácter en el campo de afectado de los datos del cliente, en la base de datos de la caja.

- Reinicia manualmente, en el servidor del local, el servicio GeoposConsole que es el encargado de capturar las ventas desde las cajas.

- Chequea cada 5 minutos si la información pendiente de las cajas comienza a ser capturada por el servidor del local.

Si bien es claro visualizar que en este monitoreo, para el caso de los caracteres de control ASCII, puede ser mejorado a través de la automatización de la eliminación automática de los caracteres que no corresponden, esto debe ser revisado y probado con rigurosidad ya que se manipularía la base de datos de la caja, e independiente de lo anterior, se debe enviar el correo electrónico al área de Fidelización para que corrija el campo y de esta forma prevenir que vuelva a generarse esta incidencia en este, u otro local de la cadena SMU.

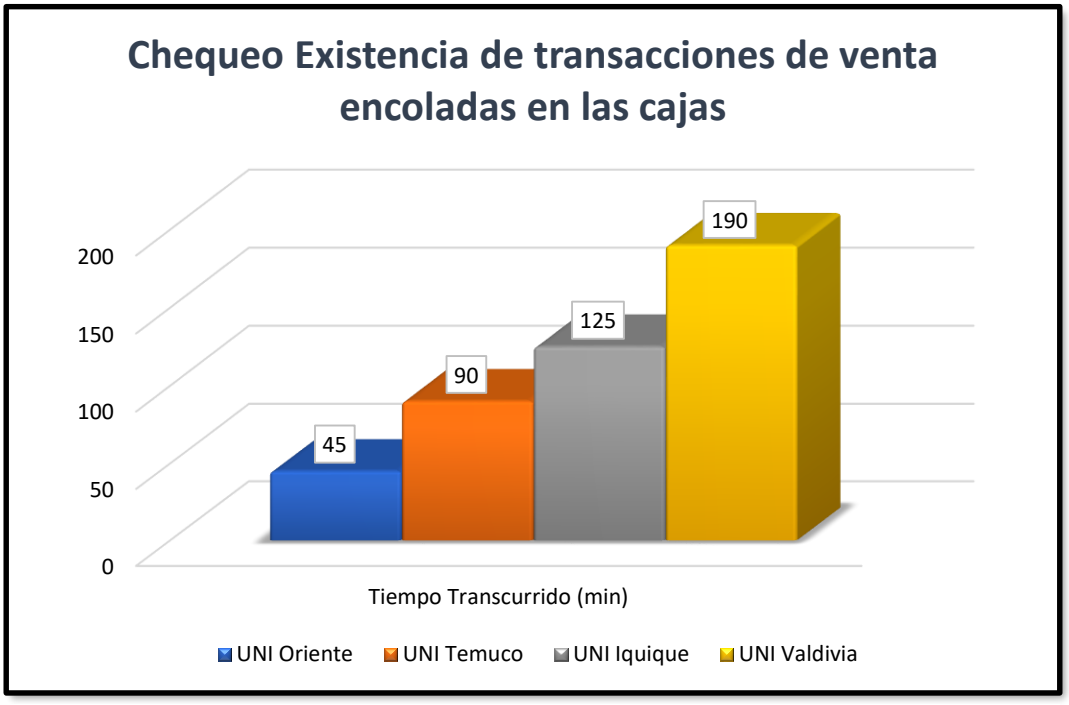

Figura 30: Gráfico comparativo de tiempo de resolución para el chequeo Existencia de transacciones de venta encoladas en las cajas

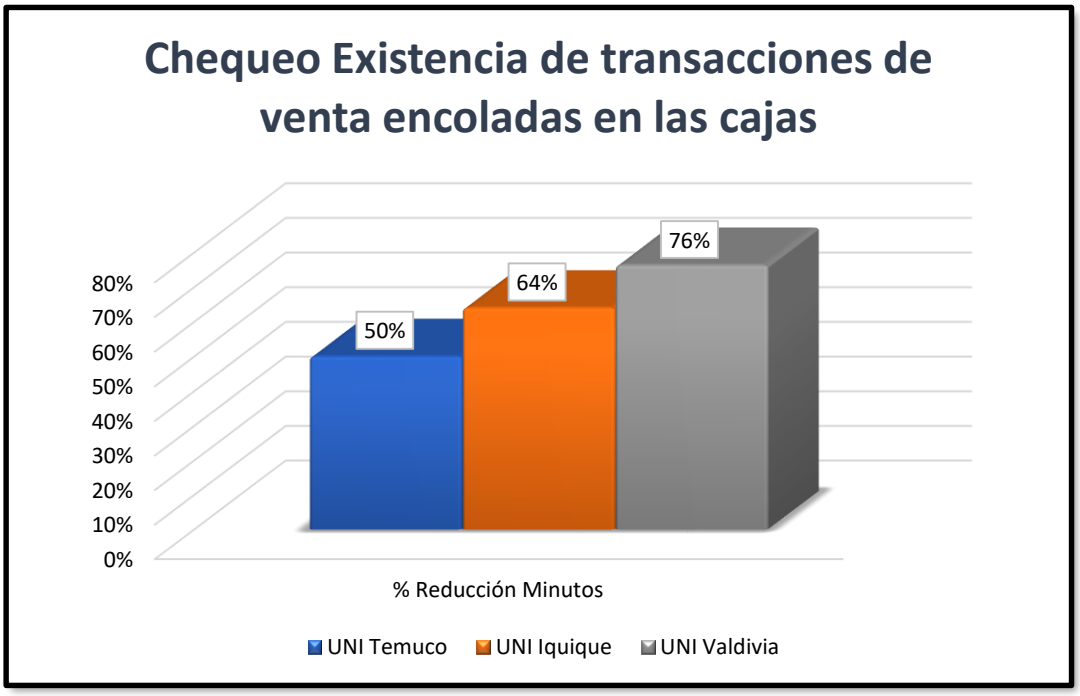

Figura 31: Gráfico de la reducción de tiempo en la resolución de la incidencia de un local monitoreado versus uno sin monitorear

Para este chequeo se contaban con estadísticas de otros locales obtenidos a través de la Mesa de Ayuda.

Nuevamente se mantiene la tendencia de disminución de los tiempos de respuesta frente a los incidentes, donde podemos apreciar que se reduce entre un 50 y 76% el tiempo completo para la solución de esta incidencia. Sin embargo, es importante señalar que el caso ocurrido en el local Unimarc Valdivia y que tuvo una duración de 190 minutos para su solución definitiva, fue atendida por un técnico externo nuevo del área de Soporte Nivel 1. Este motivo hace necesario evaluar la implementación de un método automático de corrección para el caso de los caracteres de control ASCII.

IV. CONCLUSIONES

La motivación para desarrollar e implementar una plataforma de monitoreo que permita a las áreas de Soporte anticiparse a los incidentes o agilizar el tiempo de respuesta en caso de ocurrencia de un incidente, nace en parte por la misión fijada por la Gerencia TI Operaciones el cual es: *"Garantizar la Continuidad Operacional de Nuestras Tiendas",* siendo como objetivo el *"Prevenir y atender las necesidades de las Tiendas con sentido de Urgencia"*.

La Continuidad Operacional de las Tiendas significa que el local debe estar en pleno funcionamiento en lo que respecta a TI, una interrupción del funcionamiento implica que el local deja de atender a los clientes, deja de vender. Esto no puede ocurrir y se deben realizar todos los esfuerzos por minimizar los riesgos de que estos eventos ocurran, o en su defecto, agilizar la solución para restablecer el proceso que haya sido interrumpido.

Luego de implementar y explotar la herramienta de monitoreo Nagios, en su versión Core, podemos decir que este sistema de monitorización es el adecuado para cumplir con el objetivo de prevenir, alertar y ejecutar acciones que permitan corregir las incidencias que ocurran en los locales. Es cierto que las configuraciones realizadas para este piloto son básicas, pero no es menos cierto que las características explotadas como las notificaciones, ejecución de script de chequeos por desarrollo propio, entre otras, nos permiten vislumbrar un gran futuro respecto al monitoreo y de cómo pasar, en la actualidad, desde una situación de reacción a una situación proactiva y correctiva como se pudo apreciar en el Chequeo de Espacio Libre en el Disco Duro.

El sistema Nagios es una herramienta poderosa, flexible y escalable, cumple con lo necesario y se transforma en una apoyo real y necesario para cumplir con la Misión que ha sido definida y establecida por la Gerencia TI Operaciones.

A través de la ejecución y análisis de los distintos chequeos implementados para este piloto, podemos apreciar que la herramienta Nagios por sí sola no permite lograr los objetivos definidos en esta Memoria, la correcta selección de los monitoreos a realizar y su correcta configuración son puntos importantes que complementan a esta herramienta.

Si nos detenemos en las estadísticas generadas por los distintos monitoreos realizados, podemos ver que en todos los casos de generaron reducciones en los tiempos de respuesta a las incidencias o problemas de los locales.

Tipo de chequeo realizado	Local	% Reducción Minutos
Ping a Balanza	UNI Lautaro	29%
Ping a Balanza	UNI Los Angeles	44%
Existencia de transacciones de venta encoladas en las cajas	UNI Temuco	50%
Existencia de transacciones de venta encoladas en las cajas	UNI Iquique	64%
Ping a Impresora reloj control	UNI Los Angeles	67%
Existencia de transacciones de venta encoladas en las cajas	UNI Valdivia	76%
Ping	UNI Antofagasta	77%
Espacio libre en el disco duro	UNI Temuco	88%

Figura 32: Tabla resumen de Porcentajes de reducción de tiempo de solución incidentes

.

Como se puede apreciar en el cuadro resumen de las reducciones de tiempo de las soluciones de los incidentes de algunos locales que no se encuentran monitoreados,

versus aquellos existentes en este piloto, el ahorro en tiempo va desde un 29% hasta un 88%.
Este ahorro significa que el local volvió antes a la normalidad de sus procesos o simplemente no alcanzó a enterarse que existía alguna incidencia. Este punto es importante ya que abre un abanico de posibilidades en lo que se refiere a la automatización de correcciones a problemas conocidos.

Luego de analizar los datos anteriores, podemos afirmar con seguridad que se han logrado cumplir con los objetivos específicos declarados en la presente Memoria:

- Se identificaron los servicios y hardware que serán monitoreados, esto en base a las experiencias de incidentes reportados con anterioridad a este piloto.

- Se crearon las alertas y los plugins (script) necesarios para la correcta ejecución de los monitoreos.

- Las notificaciones fueron recibidas en el tiempo estimado y dirigidas a las áreas idóneas para la resolución o escalamiento de los incidentes que se generaron.

- Se están almacenando los datos obtenidos de estos monitoreos con el fin de generar en un futuro, con las herramientas apropiadas, los KPI y estadísticas que permitan reducir las incidencias y mejorar los tiempos de respuesta, además, de aportar información a la Gerencia con la finalidad aportar para la gestión del área.

- Las áreas de Soporte se han movido de la reactividad hacia la proactividad, ya sea mediante la ejecución de labores automáticas de mantenimiento como es el borrado de archivos para prevenir que el disco duro del servidor se quede

sin espacio libre, como para evitar que sea el usuario del local sea quién reporte el incidente a través de la Mesa de Ayuda.

Esto quedó claramente demostrado en las comparaciones que se realizaron respecto a los tiempos involucrados desde el reporte de la incidencia, hasta su resolución o escalamiento.

También se observó que hace falta fortalecer una cultura de comunicación entre las distintas áreas de TI con la finalidad de estar al tanto de cualquier incidencia que afecte no solo a un área específica, al área a la cual pertenece el servicio o hardware que generó la incidencia, sino que a las restantes y que puedan ser afectadas en algún ámbito de su trabajo.

Si bien la implementación de Nagios y de los chequeos de este piloto fueron desarrollados por personal interno de SMU, la cual era una de las metas propuestas por la Gerencia TI, se vislumbra en el futuro que quizás sea necesario contar con el apoyo de profesionales externos para el desarrollo de algunos plugins, lo que no significa que el control y mantención de esta plataforma siga siendo responsabilidad de las áreas de Soporte TI de SMU.

Finalmente, podemos mencionar que el contenido desarrollado en esta Memoria permite a las áreas de Soporte TI de SMU el acercarse a los estándares existentes a nivel mundial en cuanto a lo que compete a la administración de servicios de TI. El adoptar las prácticas definidas en ITIL, permitirá a las áreas de Soporte mejorar la eficiencia de sus procesos ya que se centra en la satisfacción del cliente estructurando tareas y actividades, siguiendo pautas que están definidas y probadas, las expectativas de mejoras en el área son grandes.

El futuro para este proyecto se ve excepcional, los nuevos desafíos serán aumentar los locales, dispositivos y servicios a monitorear, agregar nuevos chequeos a los existentes en este piloto y buscar que los que se implementen, puedan realizar alguna acción

automática para reducir la necesidad de supervisión de un técnico de Soporte, disponibilizando a este para otras labores y garantizando la continuidad operacional de los locales.

V. GLOSARIO

AP

Acrónimo de Access Point y es un dispositivo de red que interconecta equipos de comunicación inalámbricos.

Archivo Log

Es un archivo de texto secuencial donde se registran todos los acontecimientos que afectan a un proceso particular, ya sea una aplicación del sistema, un motor de base de datos, entre otros.

ASCII

Sistema de codificación de caracteres alfanuméricos que asigna un número del 0 al 127 a cada letra, número o carácter especial recogidos; el ASCII extendido permite hasta 256 caracteres distintos.

Crontab

Es el nombre del programa que permite a usuarios Linux/Unix ejecutar automáticamente comandos o scripts (grupos de comandos) a una hora o fecha específica. Es usado normalmente para comandos de tareas administrativas, como respaldos, pero puede ser usado para ejecutar cualquier cosa.

Fleje

Lámina de papel o cartulina en las que se muestran los precios de los productos. Este término es usado ampliamente en las empresas del retail.

Host

Se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

ICMP

Internet Control Message Protocol (en español: Protocolo de Mensajes de Control de Internet) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un host no puede ser localizado.

Informix

Es un Sistema de gestión de bases de datos relacionales que fue creada en 1970 y posteriormente adquirida por IBM.

Máximo Help Desk

Solución de Mesa de Ayuda de IBM.

Ping

Es una utilidad que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

Plugin

Un complemento es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica.

POS

Acrónimo de Point Of Sales y en español también es conocido como Terminal Punto de Venta (TPV) o Caja, el cual es el dispositivo que permite gestionar las tareas relacionadas con la venta.

Root

Es el usuario principal en Linux y que tiene permisos de lectura, escritura y ejecución de cualquier aplicación del sistema.

SAP

es un sistema informático integrado de gestión empresarial diseñado para modelar y automatizar las diferentes áreas de la empresa y la administración de sus recursos.

Script

Es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano.

Software privativo o propietario

Se denomina software propietario,1 o privativo,2 al software del cual no existe una forma libre de acceso a su código fuente, el cual solo se encuentra a disposición de su desarrollador y no se permite su libre modificación, adaptación o incluso lectura por parte de terceros. El término ha sido creado para designar al antónimo del concepto de software libre, por lo cual en diversos sectores se le han asignado implicaciones políticas relativas al mismo. Para la Fundación para el Software Libre (FSF), este concepto se aplica a cualquier programa informático que no es libre o que solo lo es parcialmente (semilibre), sea porque su uso, redistribución o modificación está prohibida, o sea porque requiere permiso expreso del titular del software.

Software Open Source

El software de código abierto (en inglés open source software u OSS) es el software cuyo código fuente y otros derechos que normalmente son exclusivos para quienes poseen los derechos de autor, son publicados bajo una licencia de software compatible con la Open Source Definition o forman parte del dominio público. Esto permite a los usuarios utilizar, cambiar, mejorar el software y redistribuirlo, ya sea en su forma modificada o en su forma original.

VI. BIBLIOGRAFIA

www.smu.cl
http://www.spri.eus/euskadinnova/es/enpresa-digitala/agenda/nagios-herramienta-para-gestion-diagnostico-linux/3909.aspx
http://www.whatsupgold.com/es/
https://es.wikipedia.org/wiki/Zabbix
http://zabbixudenar.blogspot.cl/2013/11/ventajas-y-desventajas.html
http://www.zabbix.com/
http://www.spri.eus/euskadinnova/es/enpresa-digitala/agenda/nagios-herramienta-para-gestion-diagnostico-linux/3909.aspx
http://www.nagios.org
https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/activechecks.html
https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/passivechecks.html
https://es.wikipedia.org/wiki/Software_propietario
https://es.wikipedia.org/wiki/Software_de_código_abierto
www.geocom.com.uy