Institución Universitaria

INTEGRACIÓN DE UN SISTEMA DE MONITOREO Y GESTIÓN DE INCIDENTES DE INFRAESTRUCTURA TECNOLÓGICA CON UNA COMUNIDAD DE PRÁCTICA. CASO DE ESTUDIO: SOREIN S.A.S Y QUÍMICA PRODES S.A.S.

Gustavo Adolfo Duque Osorio

Instituto Tecnológico Metropolitano
Facultad de Ciencias Económicas y Administrativas
Medellín, Colombia
2016

INTEGRACIÓN DE UN SISTEMA DE MONITOREO Y GESTIÓN DE INCIDENTES DE INFRAESTRUCTURA TECNOLÓGICA CON UNA COMUNIDAD DE PRÁCTICA. CASO DE ESTUDIO: SOREIN – QUÍMICA PRODES.

Gustavo Adolfo Duque Osorio

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:
Magister en Gestión de Innovación Tecnológica, Cooperación y Desarrollo Regional

Director (a):
MSc. Mauricio Vélez Salazar

Instituto Tecnológico Metropolitano
Facultad de Ciencias Económicas y Administrativas
Medellín, Colombia
2016

A mi padre, porque sé que estaría orgulloso.
A mi madre, porque este es fruto de su abnegación.
A mi hermana, por enseñarme el carácter que lleva a triunfar.
A mi esposa, por su paciencia y su entrega incondicional.
A mis hijas, esperando que encuentren en mí un ejemplo a seguir…

Agradecimientos

Agradezco especialmente a Sorein y Química Prodes por su colaboración en el trabajo de campo realizado para obtener los resultados. También al ITM y toda su planta docente y administrativa, que hoy hace posible este producto final.

Resumen

Un marco de trabajo colaborativo, compromete al usuario a realizar aportes a la comunidad y le permite aprovechar la información generada por otros usuarios. Sin importar su tamaño, diariamente las compañías generan gran cantidad de datos de toda índole, pero se desaprovecha su enorme potencial. Este proyecto presenta la integración de un sistema de monitoreo con una comunidad de práctica (CoP) relacionada con Infraestructura Tecnológica (IT), que recibe como insumo la información generada a partir del monitoreo y la gestión de incidentes de IT en dos PYMEs dedicadas a la importación y comercialización de productos químicos en la zona sur del Valle de Aburrá. Con esta propuesta se pretende compensar la falta de información real y contextualizada sobre las características de las tecnologías usadas actualmente en el entorno y los incidentes más comunes, entregando a los administradores de IT los argumentos necesarios para la toma de decisiones, diagnósticos de fallas y planes de mantenimiento preventivo y correctivo, entre otras aplicaciones, basándose en reportes e incidentes reales gestionados por las compañías que hacen parte de la CoP. Esta solución garantiza que el administrador de IT conoce el estado de su entorno, a la vez que amplía la muestra de los datos usados para análisis, estudios de futuro y toma de decisiones.

Palabras clave: Comunidades de Práctica, Sistemas de Monitoreo, Infraestructura Tecnológica, Inteligencia de Negocios, Gestión de la Información, Gestión del Conocimiento.

Abstract

A collaborative framework, the user agrees to make contributions to the community and lets you take advantage of the information generated by users. Regardless of size, every day companies generate large amounts of data of all kinds, but wasted its enormous potential. This project is building a community of practice (CoP) Technology Infrastructure (TI), which receives as input the information generated from a system monitoring and incident management TI installed two SMEs engaged in importing and marketing of chemicals in the south of the Valle de Aburrá. This proposal is intended to offset the lack of real and contextualized information, delivering TI managers the arguments needed for decision-making, fault diagnostics and plans of preventive and corrective maintenance, among other applications, based on reports and actual incidents managed by companies that are part of the CoP.

Keywords: Community of Practice, Monitoring Systems, Technology Infrastructure, Business Intelligence, Information Management, Knowledge Management**.**

Contenido

Pág.

Lista de figuras

Lista de tablas

Introducción

De acuerdo con la definición que presenta Vásquez en 2011, y apoyándose en el concepto que presenta Wenger en 1998, una Comunidad de Práctica (CoP) "*es un grupo de personas ligadas por una práctica común, recurrente y estable en el tiempo"*. Gracias a este interés común, los miembros aprenden permanentemente del entorno práctico y de la experiencia que los demás comparten en la comunidad. En la actualidad, existen herramientas que facilitan la interacción entre los miembros de una CoP, como internet y las aplicaciones web. Gracias a estos elementos, se superan barreras como la ubicación geográfica y el idioma, entre otras.

El hecho de pertenecer a una CoP representa una responsabilidad implícita de participar activamente, con elementos que enriquecen el conocimiento generado dentro del grupo. De ahí la estrecha relación entre las CoP y la gestión del conocimiento.
Para que una CoP tenga éxito, es necesario que el flujo de interacción entre los miembros sea alto. Este trabajo presenta una "automatización" de esta interacción, aumetando sustancialmente la cantidad de intervenciones de los miembros en la CoP. La información generada por un administrador de infraestructura tecnológica para su propio uso y beneficio, es compartida con los demás miembros de la CoP, sin que esto represente inversión de tiempo adicional.

A mediados de 1980, se ve la aparición de las primeras comunidades de aprendizaje (Preze et al 2003) que canalizaban los intereses comunes de la comunidad académica en un mismo lugar. La aparición de tecnologías de comunicación como la internet y la mensajería instantánea, facilitaron el crecimiento de este concepto (Droschl 2004).

Más tarde se fue dando reconocimiento al potencial del trabajo colaborativo y las comunidades de práctica. Anderson y Ellis (2005) presentan la aplicación de las CoP en la producción musical, aprovechando la World Wide Web. Herramientas como el blog, wiki, las redes sociales y la internet, permiten la conformación de redes colaborativas de una manera natural. El Ghali et al (2007) presentan la propuesta de un motor de wiki con algunas características asociadas a gestión de conocimiento, dando un empujón a lo que podría llamarse la era de la web semántica.

El gigante de las comunicaciones, Cisco Systems Inc, revolucionó las plataformas de enseñanza y aprendizaje en línea, con sus herramientas basadas en tecnologías web 2.0 (Frezzo et al 2008). Sin embargo, todas estas herramientas requieren de una interacción muy alta de los participantes, lo que se traduce en una demanda de tiempo significativa para mantener actualizada la comunidad.

En 2008, Olszak y Ziemba presentan un completo análisis sobre los beneficios que se obtienen a partir de las comunidades de práctica, dentro del modelo de la gestión del conocimiento, enmarcado en el contexto organizacional y empresarial de la region más poblada e industrializada de Polonia.

Las CoP han sido usadas en diferentes disciplinas a lo largo del tiempo. En la medicina, han sido de gran ayuda para el intercambio y la conformación de bases de datos de conocimiento. Ghosh et al (2009) muestran la aplicación de una comunidad de práctica con el fin de mejorar la calidad de los datos hospedados en un sistema integrado para el cuidado de la salud.

En la actualidad, la incorporación de técnicas de inteligencia artificial y sistemas expertos, direccionan el camino de las CoP y las demás herramientas de gestión del conocimiento, tal y como lo presentan Berkani et al (2013). Ahora es común encontrar soluciones basadas en redes neuronales o modelos de lógica difusa.

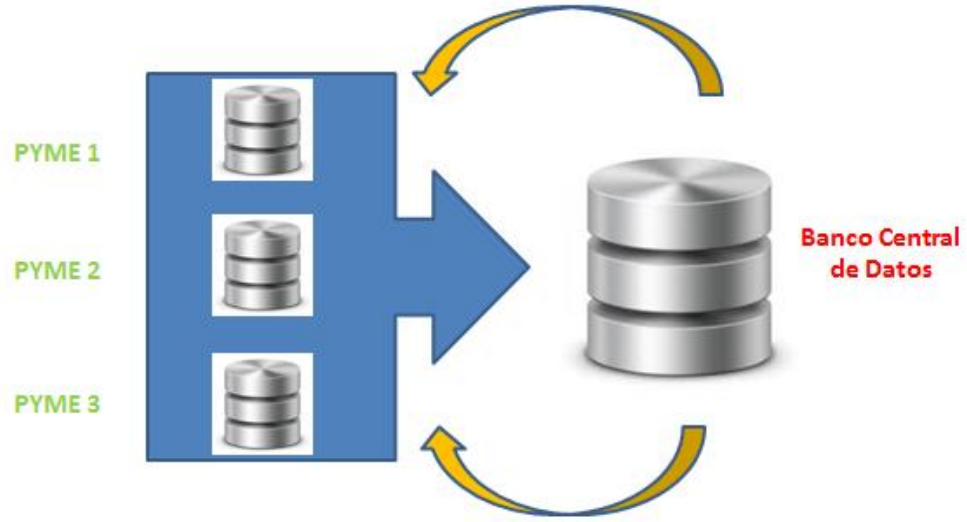
Por otro lado, en el marco económico actual, las Pequeñas y Medianas Empresas (PYMEs) juegan un papel determinante en el desarrollo en todas sus dimensiones. Un sector de PYMEs próspero es un claro indicador de crecimiento económico en su región (Nie, 2007). De acuerdo con la Organización para la Cooperación y el Desarrollo Económico (OCDE), en América Latina, el 95% de las compañías son PYMEs y emplean entre el 60% y 70% de los trabajadores. Es por esta razón que este tipo de organizaciones han captado la atención de la comunidad en general.

Las Tecnologías de la Información y la Comunicación (TICs) han penetrado profundamente la sociedad en pleno, desde el individuo hasta el contexto empresarial, al punto de que el Gobierno de Colombia creó, por ley, el Ministerio de TIC (Ley 1341 de 2009). Cada vez que las empresas, sin importar su tamaño, implementan prácticas relacionadas con TICs, obtienen un acceso más eficiente a la información disponible en el medio, hacen una mejor gestión del conocimiento interno y externo y pueden lograr la reducción de costos en sus procesos, por mencionar solo algunos de los beneficios (De León Sigg, M., Villa Cisneros, J. L., Vázquez Reyes, S., & Salcedo, J. A. R, 2014). Estas tecnologías permiten a los gerentes monitorear y controlar sus negocios con mejores resultados, además de mantenerse informados sobre el estado actual de su compañía y su entorno. Sin embargo, no siempre la implementación de herramientas asociadas a las TICs cumple con su objetivo principal. El desconocimiento de las bondades de la gestión de la información no permite que dichas herramientas sean aprovechadas al máximo.

La Infraestructura Tecnológica (IT) es uno de los pilares fundamentales en las TICs. Este pilar hace referencia al hardware y software utilizado para realizar las tareas propias del negocio. Como cualquiera de los elementos que conforman una organización, la infraestructura tecnológica debe ser monitoreada con el fin de medir su rendimiento, diagnosticar posibles fallas y dar al administrador los elementos necesarios para elaborar planes de mantenimiento preventivo y correctivo. Desde los grandes fabricantes de hardware y software como IBM y Hewlett Packard, hasta comunidades de software de código abierto (GNU) como Cacti y Nagios, han entrado a la competencia por posicionarse en el mercado del monitoreo de red. No obstante, esta información se usa a nivel intra-empresarial, dejando de lado su potencial valor en un entorno cooperativo.

Un marco de trabajo colaborativo, compromete al usuario a realizar aportes a la comunidad y le permite aprovechar la información generada por otros usuarios. La construcción de una base de datos compartida, amplía el campo muestral objeto de cualquier análisis, beneficiando a todos los miembros de dicha comunidad y generando una sinergia con resultados superiores a los que pueden lograrse con información individual (Ver figura 0 - 1). En otras palabras, la información generada por varias empresas y centralizada en una base de datos, brinda un enfoque más amplio que la misma información fraccionada para cada compañía en particular.

Figura 0-1: Modelo de un Banco Central de Datos en un Marco Colaborativo.



Fuente: elaboración propia.

Las decisiones que toman los administradores de Infraestructura Tecnológica (IT) de las PYMEs, normalmente no están soportadas por herramientas precisas que garanticen la información necesaria y suficiente, ya que este tipo de compañías no cuenta con la capacidad para invertir en este tipo de soluciones. El Project Management Body of Knowledge, mejor conocido como PMBOK (PMI, 2008), contiene las mejores prácticas relacionadas con la administración de proyectos, y cuenta con un proceso exclusivo para

la gestión de las adquisiciones, dando especial importancia a la correcta planificación de las mismas. Una correcta gestión de este aspecto garantiza que las inversiones hechas en IT están alineadas con el mapa estratégico de la compañía, y generan valor en el futuro. Por otro lado, solo 23 empresas colombianas se encuentran en el último reporte oficial del CMMI Institute (CMMI, 2014), encargado de medir y certificar la madurez de las compañías en la realización de sus procesos. Los jefes de IT de las PYMEs confían la responsabilidad de una decisión a la consulta con colegas o una breve investigación de documentación técnica o "blogs", lo que no representa una fuente fidedigna y objetiva de información. De acuerdo con un estudio realizado por la Business Software Alliance (BSA, 2014), el 43 % de las compañías en el mundo tienen irregularidades de licenciamiento en el software instalado. Esta situación se hace muy difícil de detectar cuando no se cuenta con un sistema de monitoreo que alerte sobre la presencia de software no autorizado en los activos de IT de la compañía.

Las compañías generan diariamente gran cantidad de información de IT relacionada con el inventario de hardware y software instalado, uso, rendimiento e incidentes presentados, con su correspondiente solución, entre muchos otros aspectos. Si bien, un mismo problema de IT pudo haberse presentado en varias compañías, no existe la disposición ni el tiempo para que se comparta esta información y se construya una base de conocimiento que les permita mejorar los tiempos de respuesta y la presentación de soluciones oportunas. Las CoP permiten centralizar y compartir las mejores prácticas, diagnósticos, datos estadísticos y cualquier otra información de interés común entre sus miembros. De ahí su importancia y valor en la actualidad.

Este trabajo busca articular la Ingeniería Informática con la Gestión Tecnológica, presentando una solución concebida desde la parte técnica, que al final se convierte en una herramienta útil en la toma de decisiones, estudios de futuro y análisis en general.

1. Capítulo 1: Descripción del Proyecto

1.1 Planteamiento del Problema

La Infraestructura Tecnológica de una compañía está comprendida por un amplio conjunto de herramientas que buscan facilitar la ejecución de las tareas propias del negocio. Hardware, Software, Redes de Datos y Comunicaciones, Telefonía, Servicios de Computación en la Nube, Sistemas de Almacenamiento, Bases de Datos y Repositorios, son algunos de los elementos que usan las organizaciones, de forma directa o indirecta, en el cumplimiento de sus labores diarias.

Los sistemas de monitoreo son comúnmente utilizados por las áreas de Informática y Telecomunicaciones de las compañías con el fin de supervisar el estado actual de su Infraestructura Tecnológica. Estos sistemas utilizan protocolos de escaneo que se encargan de detectar todos los elementos conectados a la red de la compañía y reúnen gran variedad de datos en forma estructurada. Una vez extraídos, estos datos pueden ser objeto de análisis para la elaboración de planes de mantenimiento preventivos y correctivos, propuestas de mejora, compra de Hardware y Software, entre muchos otros.

En la actualidad, es difícil encontrar una base de datos homogénea que contenga información relacionada con el comportamiento de la Infraestructura Tecnológica en las PYMES por varias razones:

- La compañía no cuenta con un área de Informática y Telecomunicaciones que realice tareas de gestión de la Infraestructura Tecnológica.
- El personal no posee el conocimiento necesario para recopilar esta información.
- No se encuentra utilidad en la gestión de este tipo de información.
- La información que existe es de acceso restringido o de uso comercial.

Con este proyecto se pretende adaptar y probar un sistema de monitoreo con el fin de recopilar datos relacionados con la Infraestructura Tecnológica de cada compañía, instalando y configurando una aplicación para capturar información en tiempo real, generando un banco de datos que sirva como insumo para cualquier tipo de análisis relacionado con estados actuales y tendencias, en temas relacionados con Tecnologías de la Información y la Comunicación. Posteriormente, la información generada en cada

participante de la CoP será cargada en una base de datos central, de manera anónima. Así, quedaría consolidada en un origen de datos homogéneo y estructurado, ofreciendo un insumo para los administradores de IT. Para superar la dificultad de la confidencialidad de la información, se propone un sistema de centralización anónima de la información, lo que significa que la muestra de datos no tendrá información sobre el origen. Adicionalmente, se incluye un contrato formal de confidencialidad entre los miembros de la comunidad y el ente administrador. Como apoyo, se debe realizar una campaña de sensibilización sobre CoP y trabajo cooperativo, sus beneficios y tendencias.

1.2 Hipótesis

La comunidad de práctica de IT se alimentará de los datos suministrados por el sistema de monitoreo de cada uno de los miembros, conformando una base de datos de conocimiento que será útil para el análisis y la toma de decisiones por parte de los administradores de IT, generando acciones oportunas y acertadas en la organización.

1.3 Objetivos

1.3.1 Objetivo General

Construir una comunidad de práctica de infraestructura tecnológica, adaptando un sistema de monitoreo en 2 PYMES de comercio exterior domiciliadas en la zona sur del Valle de Aburrá, con el fin de ofrecer una fuente de datos centralizada, homogénea y estructurada.

1.3.2 Objetivos Específicos

- Caracterizar los datos relacionados con infraestructura tecnológica que se generan en las PYMES y que formarán parte de la base de datos, usando metodología de levantamiento de requisitos.
- Determinar el sistema de monitoreo que cumpla con los requisitos que exige el proyecto, comparando varias opciones y evaluando sus principales prestaciones.
- Adaptar el sistema de monitoreo en 2 PYMES, instalando y configurando la aplicación de acuerdo con la caracterización realizada previamente.
- Integrar el sistema de monitoreo con una comunidad de práctica de infraestructura tecnológica, usando herramientas de software y bases de datos.

1.4 Metodología

Debido a que el proyecto se enfoca en el desarrollo de una solución basada en software, se propone el uso del estándar “RUP” (Rational Unified Process) para desarrollo de software, aceptado a nivel global como una metodología efectiva para el desarrollo estructurado de aplicaciones tecnológicas.

Ésta metodología se caracteriza principalmente por la implementación de las mejores prácticas de Ingeniería de Software, el desarrollo iterativo, la arquitectura basada en componentes y la inclusión de tareas que garantizan la calidad del software. Los flujos de trabajo del proceso son:

- Modelado del Negocio: Entendimiento de las reglas del negocio y el funcionamiento general del proceso de monitoreo de infraestructura tecnológica. Esta fase busca contextualizar a la persona que estará a cargo del proyecto de desarrollo o adaptación del software.
- Requerimientos: Se levantan los requerimientos de los usuarios de la comunidad de práctica. En esta fase, se caracteriza la información que se quiere obtener. Se detalla el tipo de dato, origen, periodicidad, temporalidad y cualquier otra información que el usuario final considere relevante. Adicionalmente, se documenta el comportamiento esperado del software.
- Análisis y Diseño: Se propone una arquitectura para el sistema, teniendo en cuenta el cumplimiento de los requisitos identificados en la actividad anterior y se describe la implementación de los mismos. Esta actividad implica la propuesta de la tecnología a usar, lenguaje y herramientas de hardware y software.
- Implementación: Se realiza la construcción de los elementos a instalar (ejecutables, bases de datos, binarios). Esta fase incluye la adaptación y parametrización del sistema de monitoreo y la integración con la comunidad de práctica.
- Pruebas: Garantizan la calidad de la solución desarrollada. Se realizan pruebas funcionales, de performance y de seguridad.
- Despliegue: En esta fase se realiza la instalación, adaptación y parametrización del sistema de monitoreo en ambiente productivo de 2 PYMES y su posterior integración con la comunidad de práctica, usando herramientas de software y bases de datos.

Se propone realizar una implementación en 2 empresas para observar la integración de la información recolectada en una plataforma única.

2. Capítulo 2: Caracterización de los datos de Infraestructura Tecnológica

En las áreas de IT se genera una gran cantidad de información, que podría clasificarse de acuerdo con el objetivo que se pretende alcanzar. En este caso, se debe apuntar a caracterizar los datos teniendo en cuenta la meta final: La conformación de una comunidad de práctica con información relevante para los administradores de IT. Partiendo del planteamiento anterior, y como producto de un proceso de levantamiento de requisitos, se propone una taxonomía conformada por 3 grandes grupos: Inventario, Monitoreo y Gestión de Incidentes.

2.1 Inventario

El inventario hace referencia a un listado de los activos de infraestructura tecnológica que posee la compañía. De este grupo se desprenden dos divisiones: hardware y software.

2.1.1 Hardware

El hardware es un artefacto físico, tangible, que realiza tareas computacionales complejas. Entre los tipos de hardware más comunes, se puede encontrar:

- Computadores de escritorio.
- Portátiles.
- Impresoras.
- Routers y Switches.
- Servidores (Físicos y Virtuales).
- Arreglos de Discos y Almacenamiento.
- Teléfonos IP.
- UPS.

Cada uno de estos dispositivos, posee una caracterización genérica, que permite distinguirlo y agruparlo al momento de realizar análisis estadísticos y otros informes. Del hardware se obtienen los siguientes datos de caracterización:

- Tipo (de acuerdo con el listado anterior)
- Fabricante.
- Modelo.
- Serie.
- Descripción.

De igual manera, al hardware se le puede asociar información relacionada con el área contable (depreciación – amortización) e información sobre la ubicación del activo y el responsable actual. Sin embargo, para este estudio, dicha información no será tomada en cuenta.

Estos datos pueden ser recopilados de forma automática, siempre y cuando el dispositivo se encuentre conectado a una red de área local o tenga un agente instalado, y soporte el protocolo de monitoreo establecido (SNMP – Simple network management protocol). Este protocolo le permite al dispositivo intercambiar información con el sistema de monitoreo, entregando datos sobre su identificación y su estado actual.

2.1.2 Software

El software hace referencia a un conjunto de instrucciones codificadas bajo un lenguaje que puede ser interpretado por el hardware, para realizar tareas específicas. Aunque el software no es tangible, sí hace parte de los activos de la compañía. A pesar de que existe una gran variedad de información acerca del software, para este estudio no es relevante profundizar en el tema, ya que lo que se busca es un modelo de integración, y para estudios posteriores se podría ampliar el alcance. Basta con tener en cuenta la información básica:

- Fabricante.
- Nombre.
- Versión.

En la mayoría de los casos se almacena información sobre la cantidad de licencias que la compañía posee, para poder cruzar esta información con la cantidad de licencias instaladas y así obtener la diferencia. Este dato es de suma utilidad, si se hace un control estricto del licenciamiento. Adicionalmente, con frecuencia los administradores de IT manejan un listado de software no autorizado. Este listado permite identificar las máquinas con dicho software instalado, y así realizar acciones preventivas y correctivas,

tales como desinstalación y restricción de privilegios administrativos para los usuarios finales.

2.2 Monitoreo

Los elementos que conforman la IT en una compañía, dependiendo de su rol, realizan su trabajo de manera permanente o periódica. El buen funcionamiento de la compañía, depende en gran parte de la IT. De ahí la importancia del monitoreo. Esta actividad permite recopilar información relacionada con el desempeño de la IT. Con estos datos, el administrador de IT puede configurar umbrales de aceptación de rendimiento para los dispositivos, alertas, alarmas y otras notificaciones, tareas de mantenimiento preventivo y acciones correctivas. Esta información también suele usarse para diagnosticar problemas en otros sistemas que estén relacionados con el elemento monitoreado. Los datos de monitoreo deben ser recopilados con una frecuencia mucho mayor a la del inventario, dependiendo también de la criticidad de la operación que soporte el dispositivo. Por ejemplo, un servidor que contiene una aplicación corporativa de tipo ERP (Enterprise Resource Plannig), debe tener una alta disponibilidad, y por lo tanto debe contar con un monitoreo mucho más exhaustivo, por tratarse de un proceso crítico para la empresa.
De acuerdo con el levantamiento de requisitos realizado en el estudio, entre los elementos a monitorear más importantes, se puede encontrar:

- Uso de CPU.
- Uso de Memoria.
- Tráfico de Red (Recepción y envío).
- Espacio disponible (Para el caso de servidores y sistemas de almacenamiento).
- Eventos (Normalmente suministrados por sistema operativo).

También es posible monitorear la disponibilidad de algún servicio en particular, por ejemplo una instancia de base de datos o la respuesta de un sitio web, pero estos últimos casos no serán parte de este estudio.

2.3 Gestión de Incidentes

La gestión de incidentes es una actividad que se rige por un estándar internacional llamado ITIL (Information Technology Infrastructure Library). De acuerdo con este estándar, un incidente podría definirse como *"cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo"* (Oficina de Comercio del Gobierno Británico, 2011). Los incidentes tienen un ciclo de vida, que se inicia con la identificación del evento, bien sea por información de un usuario que lo detectó, o por una alerta generada por un sistema de monitoreo. Una vez se identifica que existe un evento anómalo, se procede a clasificar el incidente. Esta clasificación puede tener varios subniveles, y es determinada por el administrador de IT. La clasificación para el caso de estudio, puede observarse en la Tabla 1-1.

Tabla 2-1: Clasificación de Incidentes de TI

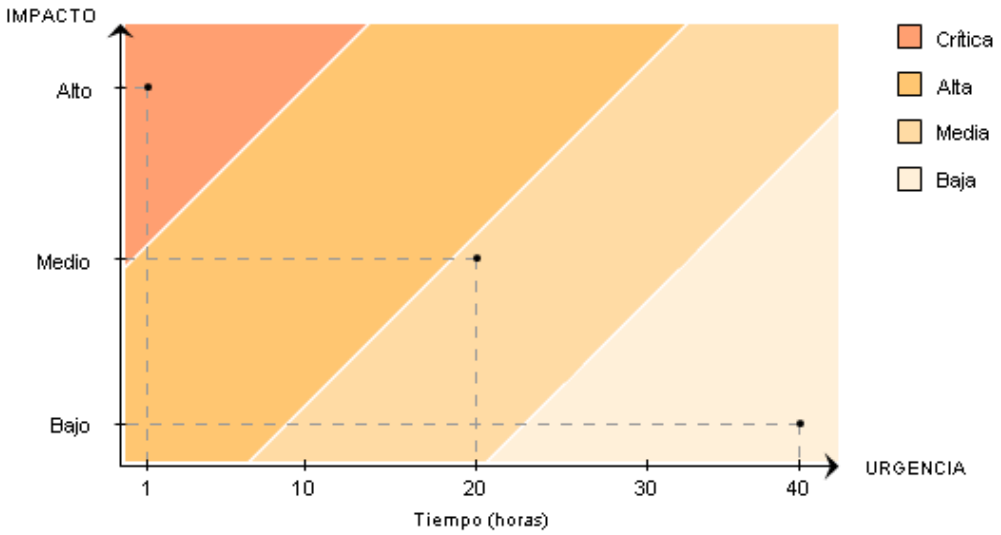
Tipo	Subtipo
Hardware	CPU
	Almacenamiento
	Memoria
	Red
	Otro
Sistema Operativo	Instalación
	Configuración
	Actualización
	Otro
Software	Instalación
	Configuración
	Actualización
	Otro
Bases de Datos	Instalación
	Configuración
	Actualización
	Otro

Fuente: elaboración propia.

Posteriormente, es necesario determinar la prioridad del incidente, dependiendo del impacto y la urgencia del evento presentado. El impacto puede determinarse dependiendo de la criticidad del servicio afectado y la cantidad de usuarios que están involucrados. La urgencia depende más del tiempo de resolución que el usuario o cliente esté dispuesto a aceptar, y normalmente está consignado en un documento denominado SLA (Service Level Agreement) o Acuerdo de Niveles de Servicio. Debido a que todas las compañías tienen diferentes servicios y su criticidad varía de acuerdo con

el negocio, no existe un estándar para este punto. Sin embargo, ITIL sugiere una matriz que se presenta en la figura 1 – 1.

Figura 2-1: Diagrama de Prioridades.



Fuente: ITIL (2011)

El incidente debe tener una descripción clara del evento, que le permita al administrador identificar el contexto de la situación que se está presentando. Una vez registrado el incidente, se procede con el escalamiento correspondiente. Debido a que este caso de estudio se desarrolla en PYMEs y estás no cuentan un área compleja de IT, el mismo administrador de IT es quien se encarga de darle gestión al incidente y escalarlo a un proveedor, si es el caso.

A partir de este momento, el incidente comienza a pasar por diversos estados, que pueden ser determinados a discreción del administrador de IT para dar un mejor seguimiento. Los estados tenidos en cuenta fueron:

- En Diagnóstico.
- Solución en Progreso.
- Escalado a Proveedor.
- En pruebas.
- Cerrado.

Para este caso de estudio, uno de los aspectos más importantes es la documentación generada en el proceso de diagnóstico y solución de los incidentes, ya que ésta será la materia prima para la CoP. Así, mientras el administrador de IT documenta sus incidentes y construye una base de conocimientos propia, también hace un aporte valioso a los demás miembros de la CoP, sin tener que invertir tiempo extra.

3. Capítulo 3: Análisis y Selección del Sistema de Monitoreo

El presente capítulo tiene como objetivo la presentación de diferentes sistemas de monitoreo y la selección de la opción mas apropiada y conveniente, aplicando los principios básicos de la decisión multicriterio. (Escobar y Gonzalez. 2004) (Romero. 1996).

Para comenzar, es necesario definir los atributos que el centro decisorio (en este caso las PYMEs) consideran relevantes a la hora de tomar la decisión. Estos atributos serán ponderados teniendo en cuenta la relevancia que el centro decisorio le otorga a cada uno, y las restricciones para tomar la decisión.

Los atributos definidos para este caso de decisión, con su correspondiente ponderación son:

- Funcionalidad: Mide la capacidad de cumplir con los requerimientos funcionales establecidos para este caso. (20 %)
- Costo: Corresponde al dinero que se debe invertir para la puesta en marcha de la solución, incluyendo licencias, parametrización, implantación e infraestructura, entre otros. (40 %)
- Usabilidad: La facilidad para ser usado por el usuario final. (20 %)
- Seguridad: Aspectos como autenticación, encriptación y cifrado. (20 %)

Para todos los atributos se define una escala entre 1 y 10, siendo 1 la calificación más baja y 10 la más alta.

En la actualidad, existe una vasta oferta de sistemas de monitoreo. De ahí la importancia de realizar un análisis detallado de sus características y prestaciones.

El funcionamiento básico de un sistema de monitoreo se argumenta en el intercambio de información entre un dispositivo conectado a la red y una consola central, usando un protocolo común y un agente, tal y como se observa en la figura 2 – 1.

Figura 3-1: Funcionamiento básico de un sistema de monitoreo.

Fuente: elaboración propia.

Los sistemas de monitoreo suministran información valiosa para los administradores de IT. Con este tipo de herramientas, es posible detectar eventos que afecten el servicio, y así poder tomar acciones al respecto. Para este análisis, se han seleccionado 4 sistemas de monitoreo con diferentes características: Monitor de Recursos de Microsoft Windows, TeMIP de Hewlett Packard, SCOM de Microsoft, OEM de Oracle, y Spiceworks.

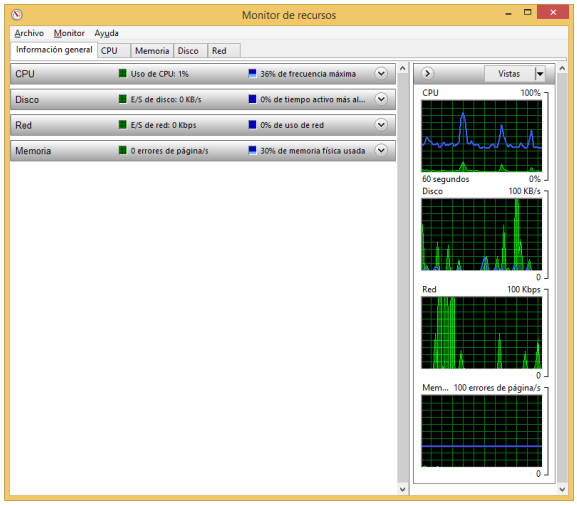
3.1 Monitor de Recursos de Windows (Microsoft)

Esta es una herramienta que permite recopilar datos de rendimiento de la máquina, y que viene integrado con el sistema operativo Microsoft Windows.

Entre sus ventajas, se puede mencionar que entrega datos sobre consumo de CPU, Memoria RAM, Red y Almacenamiento. Adicionalmente, no implica un costo adicional, puesto que viene incluído con el sistema operativo. También permite configurar métricas adicionales apuntando a otros servicios. Por último, cuenta con una interfaz gráfica que muestra una o varias métricas en determinados períodos de tiempo, tal y como se aprecia en la figura 2 - 2.

Las debilidades de esta opción radican en la imposibilidad para trabajar en red, ya que está desarrollado para trabajar con recursos locales. Tampoco cuenta con un sistema de alertas o notificaciones y su interfaz gráfica no es interactiva. La configuración de nuevas métricas y otras tareas administrativas es compleja y puede requerir de un experto.

Figura 3-2: Monitor de Recursos.



Fuente: Monitor de recursos Microsoft Windows 7.

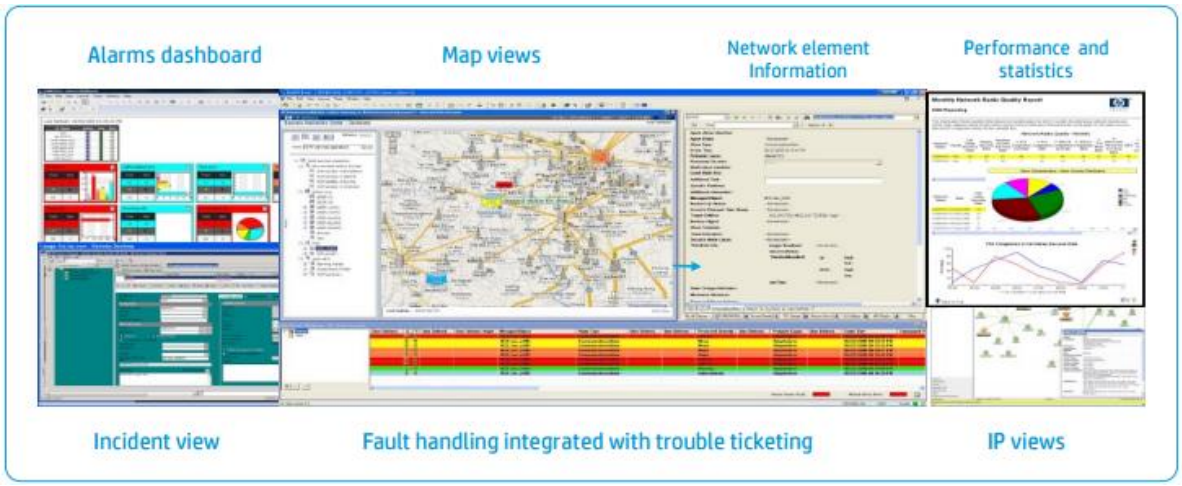
3.2 TeMIP (Hewlett Packard)

Se trata de una robusta herramienta desarrollada por Hewlett Packard para administración y monitoreo de IT (Figura 2 – 3).

Entre sus principales beneficios, se pueden mencionar su interfaz gráfica intuitiva e interactiva, compatibilidad con numerosos sistemas, soporte de integración mediante web services y un kit para desarrolladores que permite crear nuevas funcionalidades a partir de su propio framework.

Por tratarse de una herramienta tan poderosa, implica una labor de administración alta, lo que se traduce en la necesidad de contar con expertos para operar correctamente la herramienta. Su tiempo de implantación es alto, y puede tomar varios meses antes de que entre en operación. Finalmente, es un producto con unos costos de licenciamiento altos, lo que concentra su nicho en grandes compañías.

Figura 3-3: Consola de TeMIP.

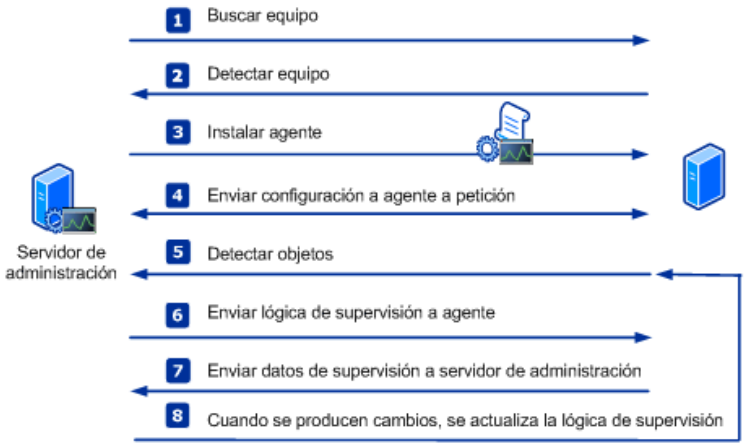


Fuente: Consola TeMIP (Hewlett Packard).

3.3 SCOM: System Center Operations Manager (Microsoft)

El grande de la informática, Microsoft, también cuenta con un producto para administración de IT: SCOM – System Center Operations Manager. Esta herramienta maneja una lógica muy similar a las demás opciones presentadas en este estudio, partiendo de una consola centrar e intercambiando información con los dispositivos que se quieren monitorear, usando un agente y un protocolo común, que se presenta en la figura 2 – 4.

Figura 3-4: Ilustración simplificada del proceso de detección y supervisión de objetos.



Fuente: Microsoft

SCOM cuenta con una compatibilidad nativa con plataformas Microsoft (Windows, SQL Server, entre otros), pero también puede interactuar con sistemas basados en Unix / Linux / AIX, usando comunicación por SSH (Secure Shell).

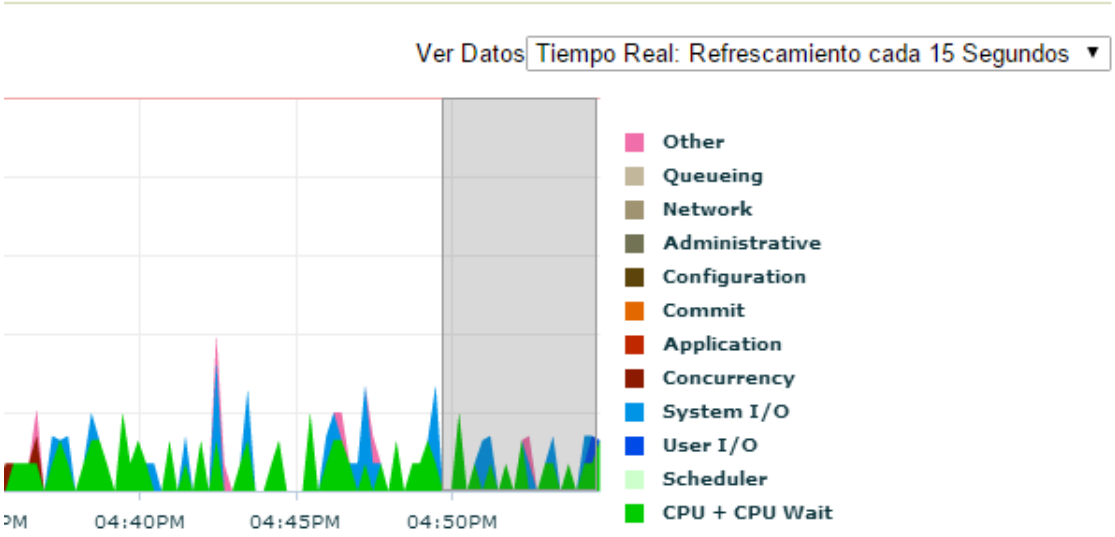
SCOM depende de una arquitectura de IT conformada por un servidor de administración, una base de datos operativa, una base de datos para almacenamiento y un servidor de informes, lo que supone una inversión importante a la hora de su implantación. Adicionalmente, su carga administrativa es alta, lo que supone personal dedicado a realizar esta tarea. Adicionalmente, se trata de un producto con altos costos de licenciamiento, no solo del producto, sino de la IT alterna asociada a su funcionamiento.

3.4 OEM (Oracle Enterprise Manager)

Oracle es una compañía que sobresale entre las más importantes del sector de la informática y la computación. Su apuesta para sistemas de administración de IT se concentra en la consola OEM.

Se trata de una solución robusta, con una gran variedad de funcionalidades como envío de notificaciones y alertas, configuración de métricas y umbrales, interfaz gráfica interactiva, entre otras. Adicionalmente, cuenta con una integración nativa con motores de bases de datos Oracle, lo que ofrece un monitoreo mucho más detallado del que podría ofrecer cualquier otra plataforma (Figura 2 – 5), entregando información sobre eventos de espera (CPU, Concurrencia, Commit, I/O), estado de los tablespaces y eficiencia de las sentencias SQL ejecutadas, por mencionar solo algunas.

Figura 3-5: Vista de Actividad de Sesión Superior en OEM.



Fuente: Consola Oracle Enterprise Manager Versión 11.2.

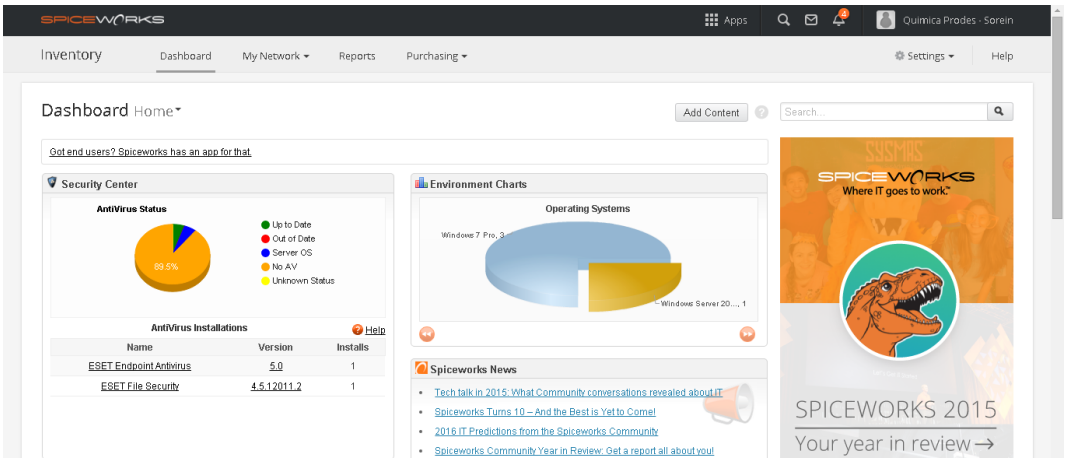
El funcionamiento de esta consola requiere de un procesamiento alto, lo que sugiere que debe instalarse en un servidor con capacidades suficientes para soportar esta carga. Como todos los productos Oracle, la consola OEM requiere de un entrenamiento especial, ya que su administración tiene un alto grado de complejidad. Adicionalmente, es importante mencionar que esta plataforma acarrea altos costos de mantenimiento y licenciamiento.

3.5 Spiceworks

Spiceworks es una herramienta que ofrece funcionalidades para administrar IT. Esta plataforma puede soportar desde una pequeña infraestructura hasta una compañía con varios cientos de equipos.

En su oferta, Spiceworks presenta tres grandes características: Inventario, Monitoreo de Red y "Help Desk" o Mesa de Ayuda. Esta aplicación es de descarga y uso gratuito, aunque no es una aplicación de código abierto. Cuenta con una interfaz gráfica bastante amigable (Figura 2 – 6) y su instalación puede tardar entre 3 días y 4 semanas, dependiendo del tamaño de la infraestructura que será monitoreada. Contiene un Metabuscador, que facilita la interacción entre el usuario administrador y la consola, y provee un sistema de reportes predeterminados, aunque pueden construirse nuevos reportes con su generador de expresiones. Su administración es bastante sencilla, y provee información valiosa a los administradores de TI.

Figura 3-6: Pantalla principal de Spiceworks.



Fuente: Dasboard Spiceworks

Por otro lado, por tratarse de una aplicación gratuita, presenta un banner permanente de publicidad, que para algunas compañías podría ser molesto. Adicionalmente, a pesar de que Spiceworks es una compañía con cerca de 10 años en el mercado, y que nació como un proyecto gratuito, nada garantiza que continúe siendo así, además de

que no cuenta con una red de soporte para solución de incidentes propios de la aplicación.

Una vez realizado el análisis de los sistemas propuestos, la tabla de decisión multicriterio con los totales ponderados queda así:

Sistema	Funcionalidad (20 %)	Costo (40 %)	Usabilidad (20 %)	Seguridad (20 %)	TOTAL
Monitor de Recursos (Windows)	4	10	3	4	6,2
TeMIP	6	1	4	8	4
SCOM	7	1	5	8	4,4
OEM	8	1	7	7	4,8
Spiceworks	7	10	8	7	8,4

Con el resultado anterior, se determina que Spiceworks es la solución más apropiada para realizar la implementación.

4. Capítulo 4: Instalación y Configuración del Sistema de Monitoreo y Gestión de Incidentes de IT

Después de determinar el sistema de monitoreo que se va a usar, se procede con la instalación y posterior configuración.

4.1 Instalación

Spiceworks es una aplicación que se ejecuta sobre entornos Windows y su instalación se realiza a través de un ejecutable que se descarga del sitio web oficial de Spiceworks (**www.spiceworks.com/downloads**). Como primer paso, es importante revisar los requerimientos técnicos mínimos que el fabricante sugiere para soportar la operación de la herramienta:

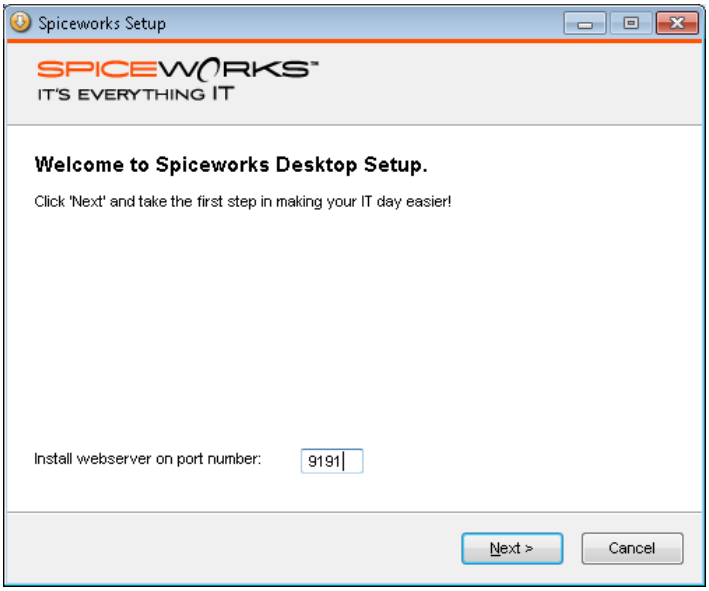
- Procesador Intel Pentium 4 a 1.5 GHz.
- 4 GB de memoria RAM.
- 1 GB de espacio disponible en disco.
- Sistema Operativo Microsoft Windows XP / Windows Server 2008 o superior.

Se procede con el aprovisionamiento del servidor sobre el que se instalará la aplicación, tarea realizada por el administrador de IT de cada compañía. Con el servidor disponible, se procede con la instalación de la aplicación siguiendo los siguientes pasos:

- Se ejecuta el instalador con permisos de administrador. Esta instalación requiere de permisos para navegar en internet.

- Se selecciona el puerto http sobre el cuál será publicada la aplicación web (Figura 3 – 1).

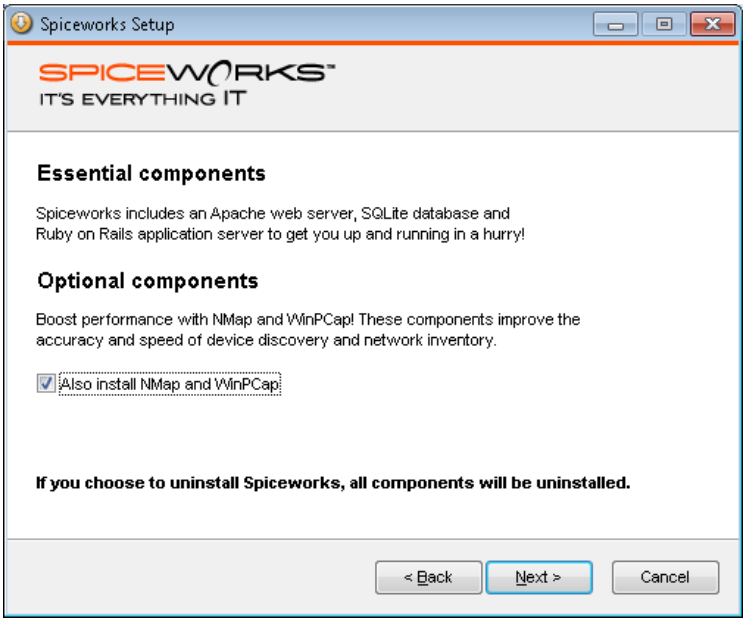
Figura 4-1: Pantalla inicial de instalación.



Fuente: Spiceworks

- Se selecciona la opción para instalar los componentes NMap y WinPCap para mejorar el rendimiento del proceso de identificación de elementos de red (Figura 3 – 2).

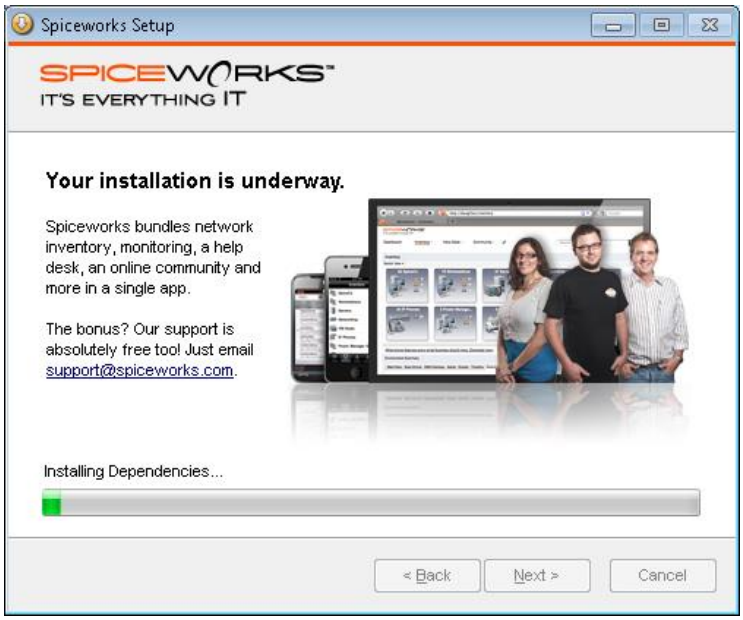
Figura 4-2: Selección de componentes NMap y WinPCap.



Fuente: Spiceworks

- Se selecciona el directorio de instalación de la aplicación y se inicia la instalación. Este proceso incluye la instalación del servidor web Apache y el motor de base de datos SQLite (Figura 3 – 3).

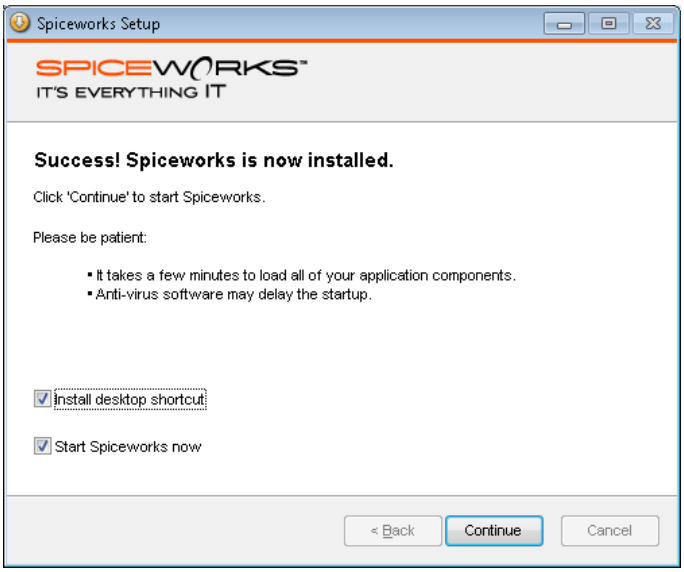
Figura 4-3: Progreso de instalación.



Fuente: Spiceworks

- Se selecciona la opción de crear un acceso directo desde el escritorio para facilitar su acceso (Figura 3 – 4).

Figura 4-4: Creación de acceso directo y finalización de la instalación.



Fuente: Spiceworks

4.2 Configuración

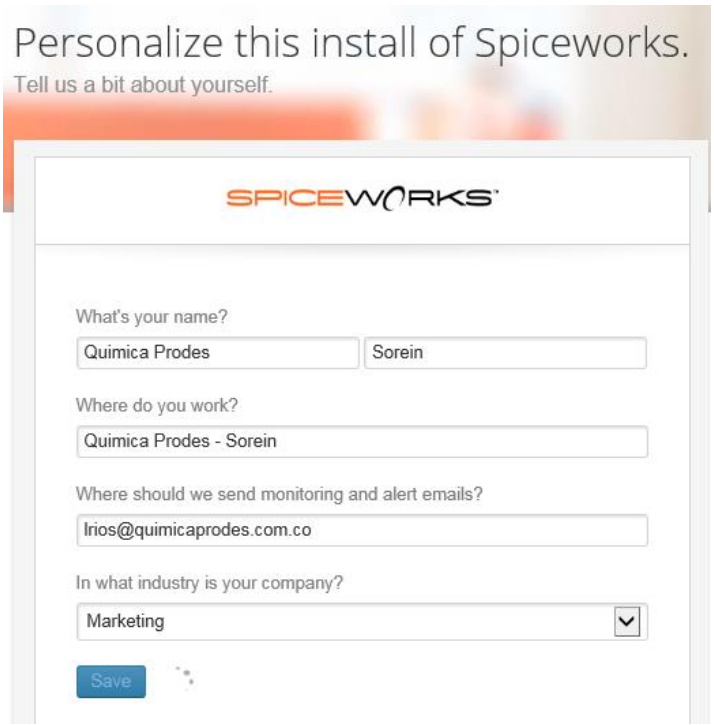
Una vez instalada, la aplicación se encuentra lista para iniciar. Sin embargo, es necesario adelantar la configuración que permite recolectar y almacenar la información de acuerdo con las necesidades del negocio. En el capítulo 1 se realizó una caracterización de la información que se desea obtener, y este paso está encaminado a lograr dicho objetivo.

La configuración está dividida en dos módulos: Inventario y "Help Desk" o Mesa de Ayuda, y se realiza inicialmente con la colaboración de un asistente suministrado por la misma aplicación. Posteriormente, será necesaria la configuración de algunos elementos desde el módulo de administración de Spiceworks.

4.2.1 Inventario

El proceso de inicio de la aplicación puede tardar algunos minutos cuando se hace por primera vez. Posteriormente, se solicita el usuario y contraseña necesarios para autenticarse. Una vez autenticados, la aplicación solicitará algunos datos generales de la compañía (Figura 3 – 5).

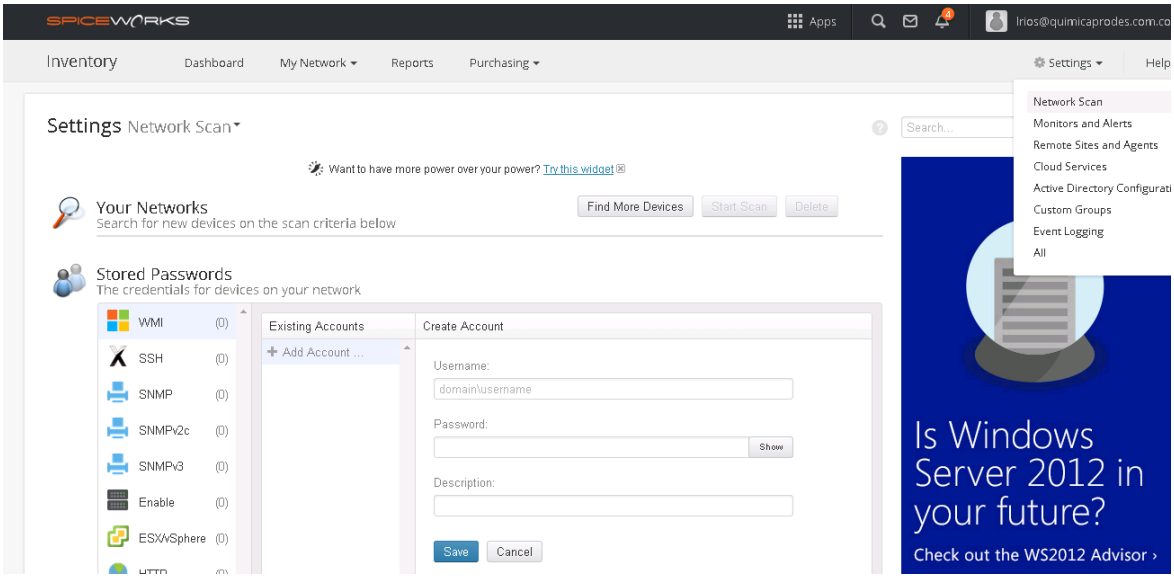
Figura 4-5: Información básica de la compañía y el administrador.



Fuente: Spiceworks

Se debe definir la red o segmento de red objeto del escaneo. Puede ser una dirección IP o un rango. Se configura una red privada completa tipo “C”. Para hacerlo, se selecciona el menú “Settings – Network Scan”, en la sección “Your Networks” (Figura 3 – 6).

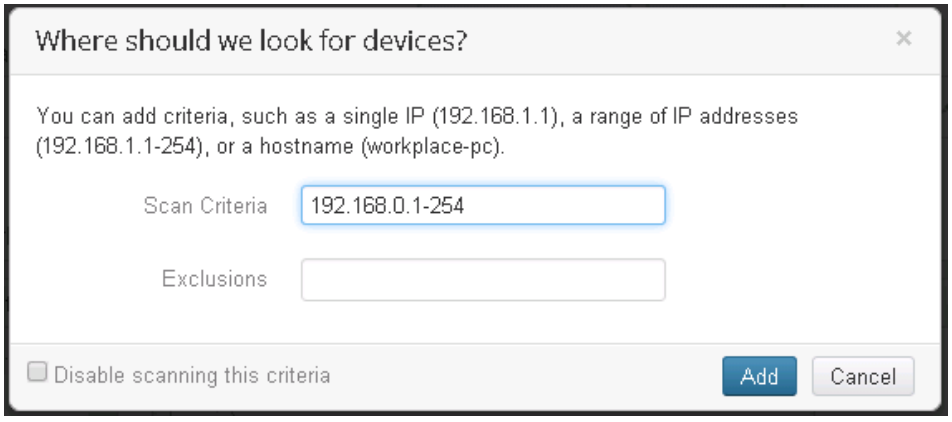
Figura 4-6: Pantalla principal de escaneo de red.



Fuente: Spiceworks

Se pulsa el botón “Find More Devices” y se diligencia el formato con la información solicitada. Existe la opción de configurar una dirección IP o segmento de red para que sea excluida del proceso de escaneo de red, como puede observarse en la figura 3 - 7.

Figura 4-7: Configuración de red o segmento de red objeto de escaneo.

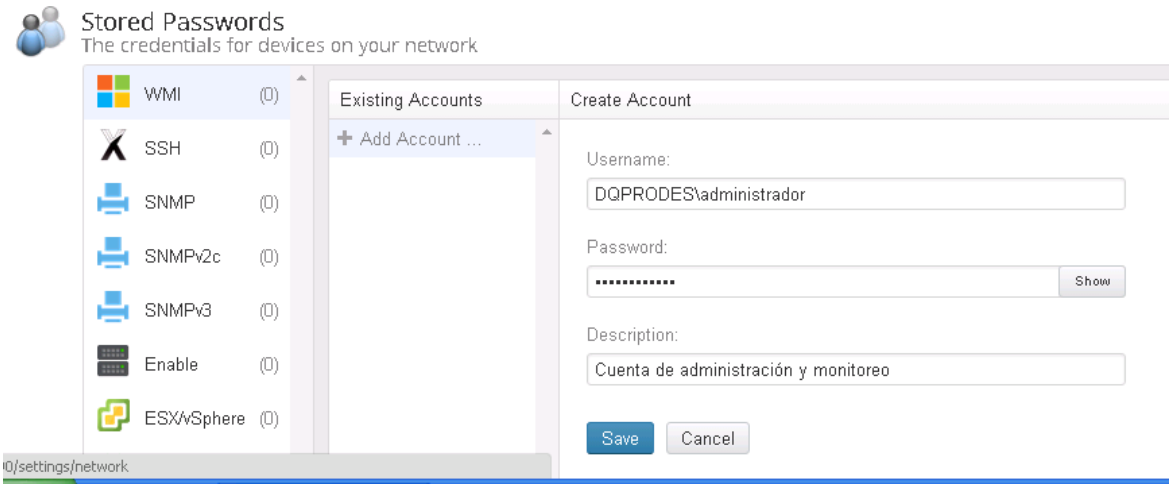


Fuente: Spiceworks

Para obtener información de los dispositivos de red, es necesario contar con credenciales de autenticación que tengan los permisos necesarios. En este caso, debido a que la red está administrada por un controlador de dominio, se usará una

cuenta del dominio para dicha autenticación. Esta configuración se realiza en la opción "Settings – Network Scan", en la sección "Stored Passwords" (Figura 3 – 8). Es posible almacenar cuentas para diferentes protocolos o sistemas operativos. Este caso de estudio solo requiere de cuentas de Microsoft y su protocolo WMI (Windows Management Instrumentation).

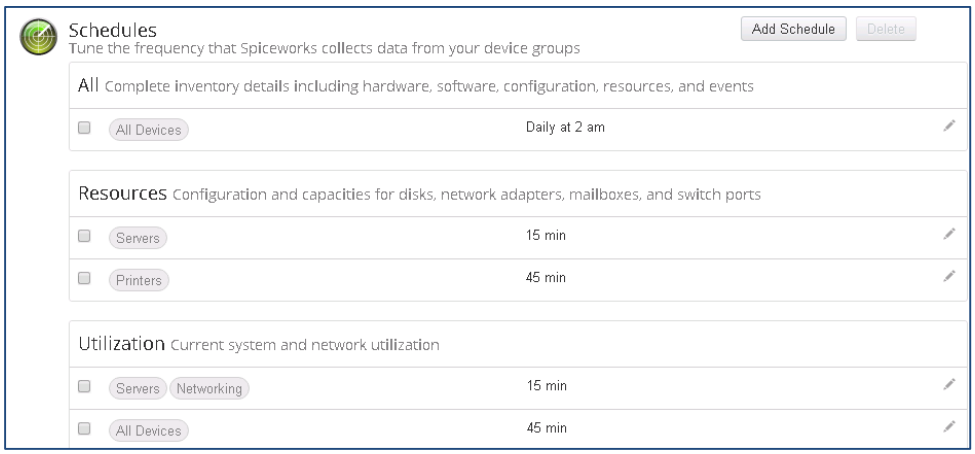
Figura 4-8: Configuración de credenciales de autenticación en dispositivos de la red.



Fuente: Spiceworks

Como se observa en la figura 3 – 8, en la sección "Schedules" se configura el horario y la periodicidad de los escaneos, dependiendo del tipo de dispositivos, recursos y servicios que serán objeto de monitoreo (servidores, equipos de escritorio, capacidad de procesamiento, servicios en la nube).

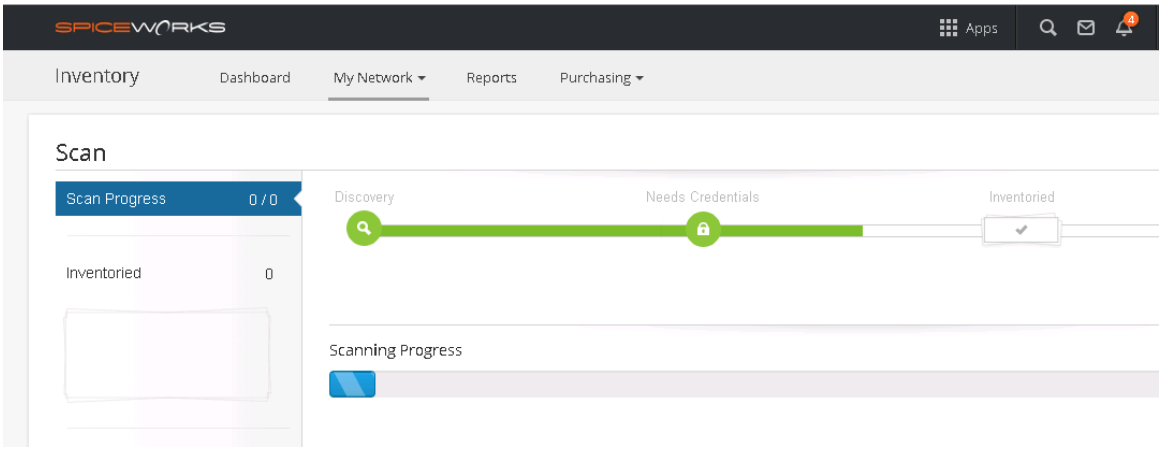
Figura 4-9: Programación de tipos y orígenes de escaneo.



Fuente: Spiceworks

Finalmente, se puede iniciar de forma manual el escaneo inicial de la red, con el fin de encontrar los dispositivos que se encuentran conectados a la red. Para hacerlo, se selecciona el botón “Start Scan” que se encuentra en la sección inicial de esta pantalla (Figura 3 – 9).

Figura 4-10: Escaneo inicial para descubrir los dispositivos conectados a la red.



Fuente: Spiceworks

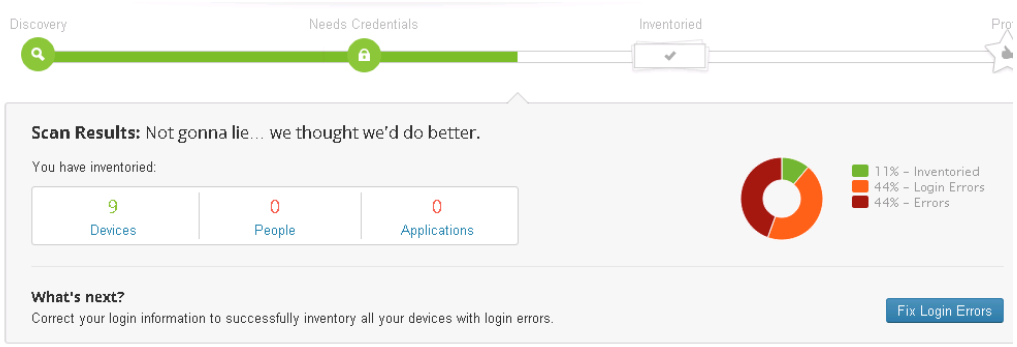
Es importante considerar que solo se detectan los dispositivos que se encuentren encendidos Sin embargo, si se cuenta con un controlador de dominio, Spiceworks se encargará de extraer la información de los equipos que estén registrados en el dominio y agregarlos al inventario de hardware (Figura 3 – 10). Este paso no se recomienda si no se hace un correcto manejo de la información que se consigna en el directorio activo, ya que podría suministrar información desactualizada o incompleta, que se convierte en “basura” para la aplicación.

Figura 4-11: Alerta de equipos hallados desde Directorio Activo.

Fuente: Spiceworks

Al finalizar el proceso de escaneo, se observa un resumen, que incluye el porcentaje de los dispositivos encontrados satisfactoriamente, y un informe de los errores, como se aprecia en la figura 3 - 11. Estos errores pueden hacer referencia a problemas de autenticación, credenciales, protocolos o permisos.

Figura 4-12: Resumen del proceso de escaneo de red.

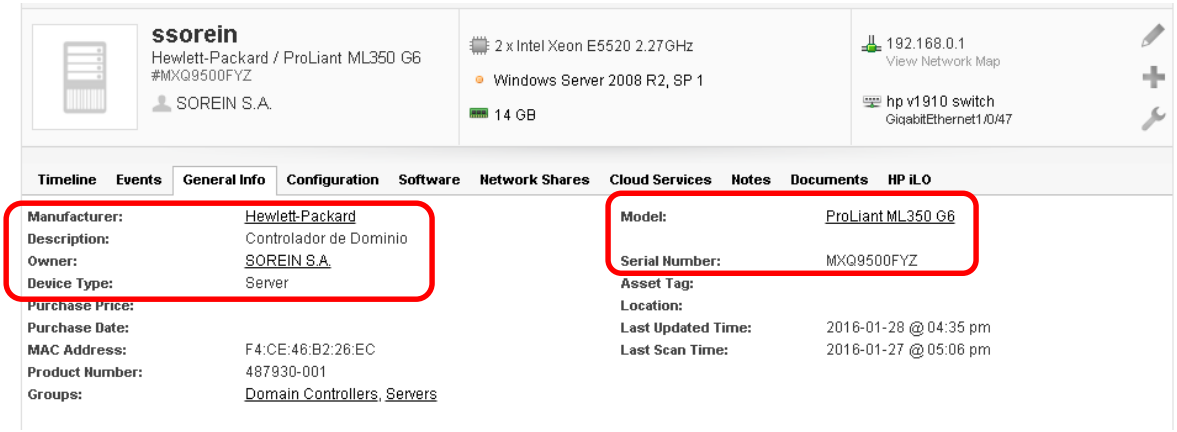


Fuente: Spiceworks

Con este procedimiento, se concluye la configuración básica inicial del módulo de inventario.

Se toma como ejemplo un dispositivo de red para confirmar que suministra la información que se requiere, de acuerdo con el capítulo 1. Estos datos son: Tipo, Fabricante, Modelo, Serie y Descripción. Como puede observarse en la figura 3 - 12, los datos requeridos se encuentran almacenados en la información general del dispositivo. En caso de que alguno de los campos no contenga información o esta tenga algún error, puede ser editada a discreción del administrador.

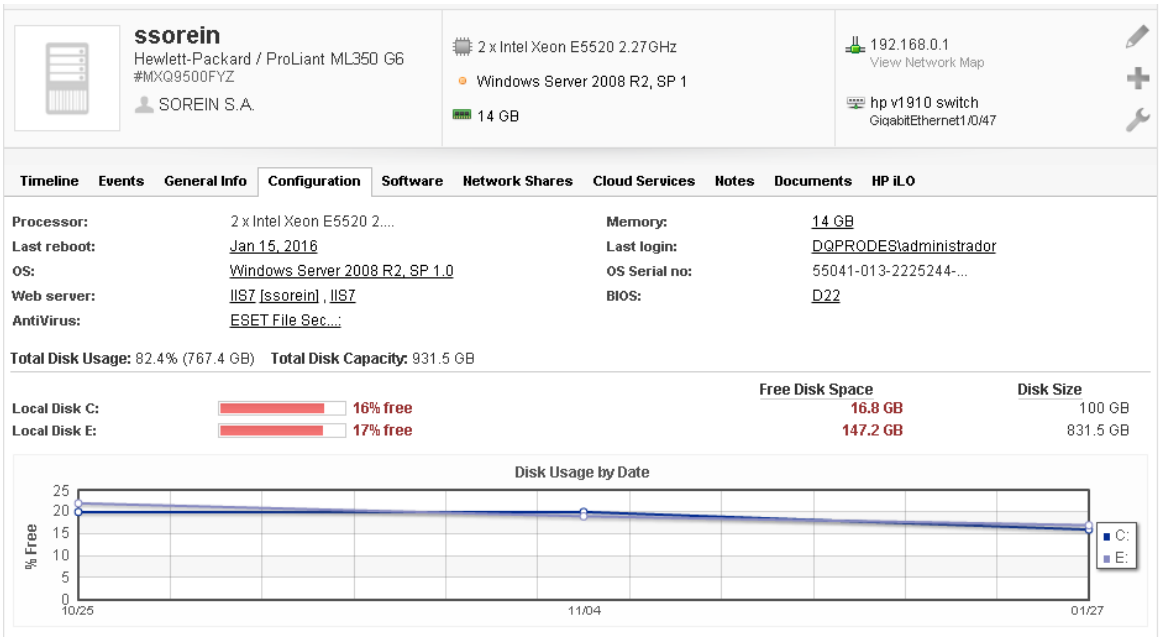
Figura 4-13: Información general del dispositivo.



Fuente: Spiceworks

En la sección “Configuration” (Figura 3 – 13), se puede observar la información relacionada con el almacenamiento y el espacio disponible en discos y su comportamiento en la línea de tiempo.

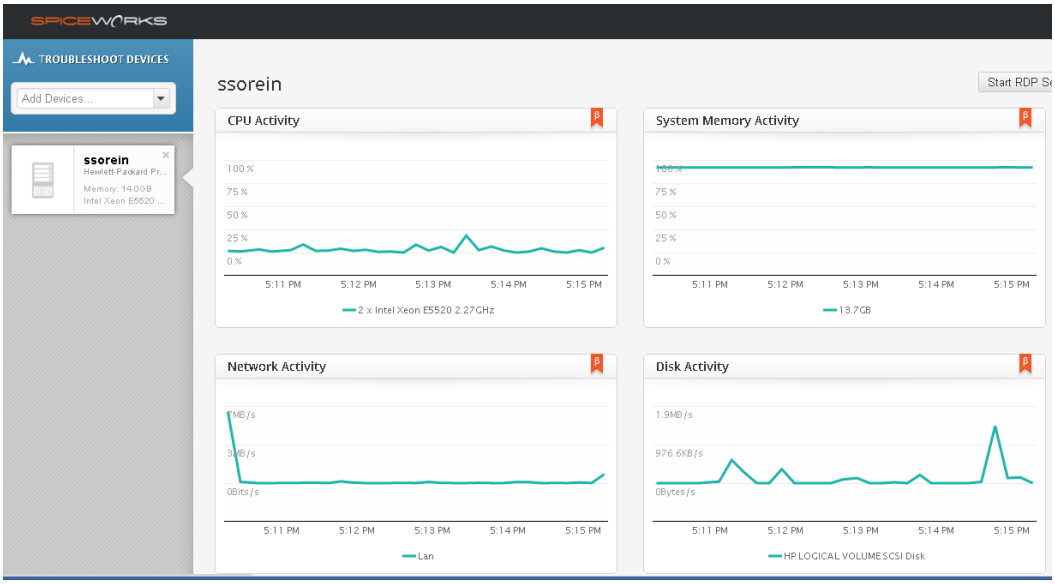
Figura 4-14: Información de espacio disponible en discos.



Fuente: Spiceworks

Adicionalmente, la información de monitoreo puede ser visualizada desde la opción “Troubleshoot Devices” (Figura 3 – 14). En esta vista, se observa información de consumo de CPU, Memoria y Actividad de Red.

Figura 4-15: Monitoreo de recursos del dispositivo.



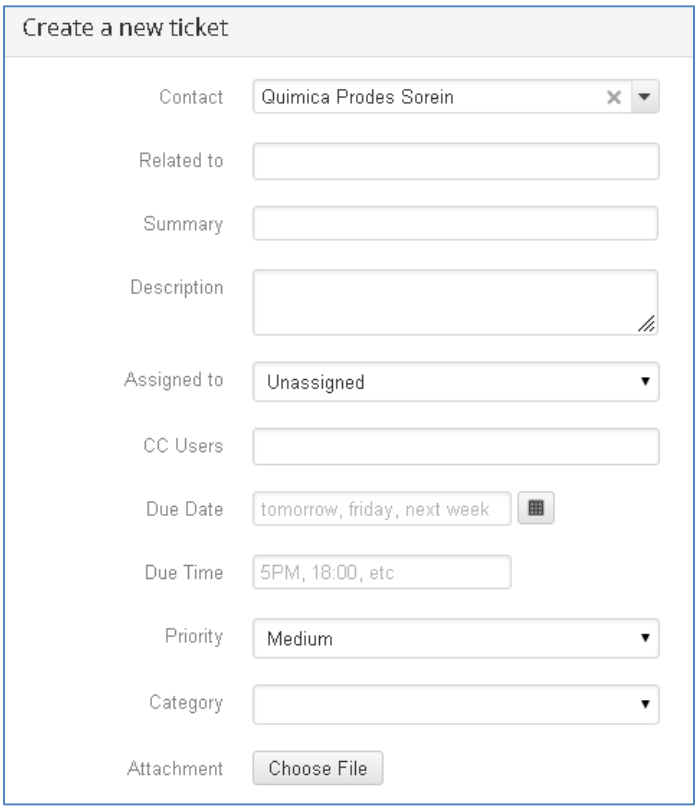
Fuente: Spiceworks

4.2.2 “Help Desk” o Mesa de Ayuda

Este módulo ofrece la funcionalidad necesaria para gestionar los incidentes de IT que se presentan en la compañía. Su configuración debe estar orientada a obtener la información que se caracterizó en el capítulo 1: Categoría, Subcategoría, Prioridad, Estado, Responsable, Descripción y Documentación.

Se procede a realizar una verificación del módulo para confirmar si la información requerida se encuentra disponible. Para tal efecto, se observa un formulario de un incidente nuevo (Figura 3 – 16) y se revisa cada uno de los campos que contiene.

Figura 4-16: Formulario para ingresar incidentes de IT.

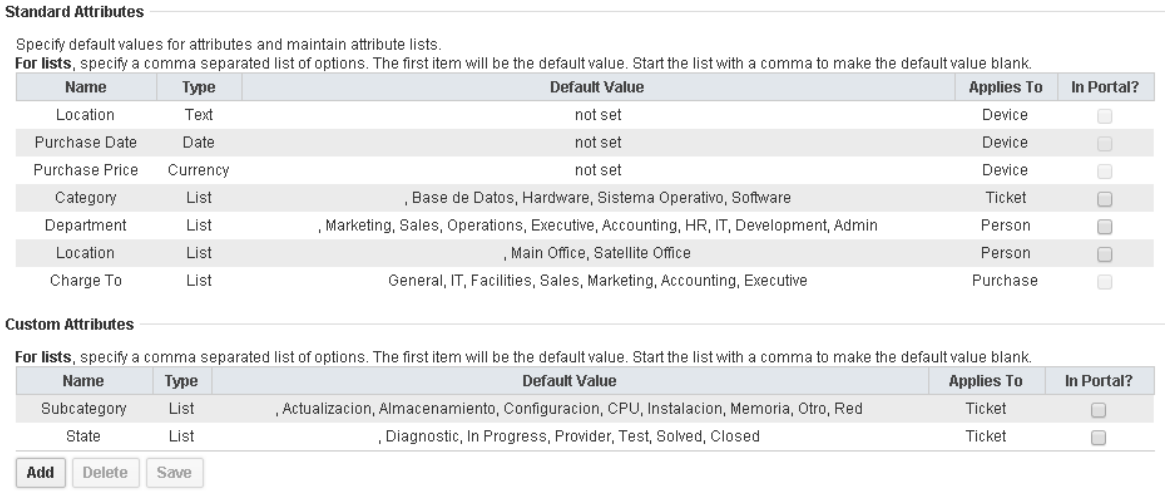


Fuente: Spiceworks

De acuerdo con el contenido del formulario, se concluye que los campos "Subcategoría" y "Estado" no están incluidos, lo que implica una configuración adicional para este módulo. Adicionalmente, El campo "Category" ofrece una lista de valores que no concuerda con la caracterización que se presenta en la tabla 1 – 1: Clasificación de Incidentes de IT.

La configuración que hace falta, debe realizarse por la opción “Advanced & International Options”, en las secciones “Standard Attributes” y “Custom Attributes”, tal y como se observa en la figura 3 - 17. Esta opción permite crear campos personalizados y asociarlos a cualquier módulo de la plataforma. Para este caso, los nuevos campos hacen parte del módulo de “Help Desk” o Mesa de Ayuda.

Figura 4-17: Configuración de campos personalizados para la gestión de incidentes de IT.

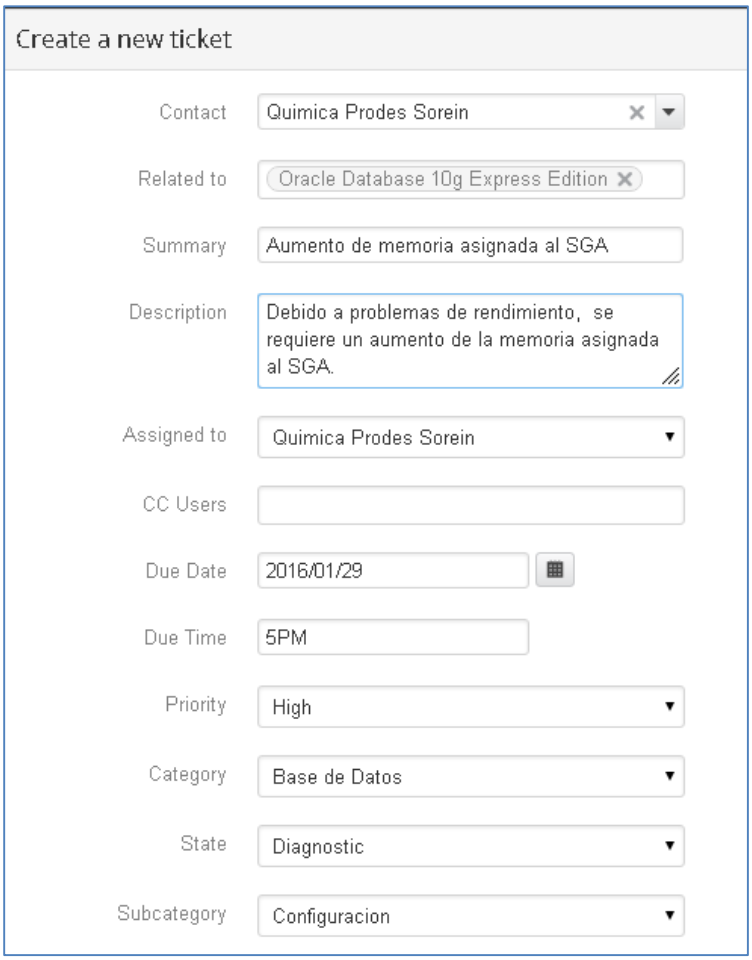


Fuente: Spiceworks

Los campos se configuran para que se comporten como listas desplegables, y se ingresan los valores que dicho campo puede aceptar.

Una vez realizados estos cambios, el formulario para la creación de incidentes de IT (figura 3 – 18) presenta todos los campos definidos en la caracterización inicial.

Figura 4-18: Formulario para la creación de incidentes de IT personalizado.



Fuente: Spiceworks

5. Capítulo 5: Integración de los Sistemas de Monitoreo con la Comunidad de Práctica.

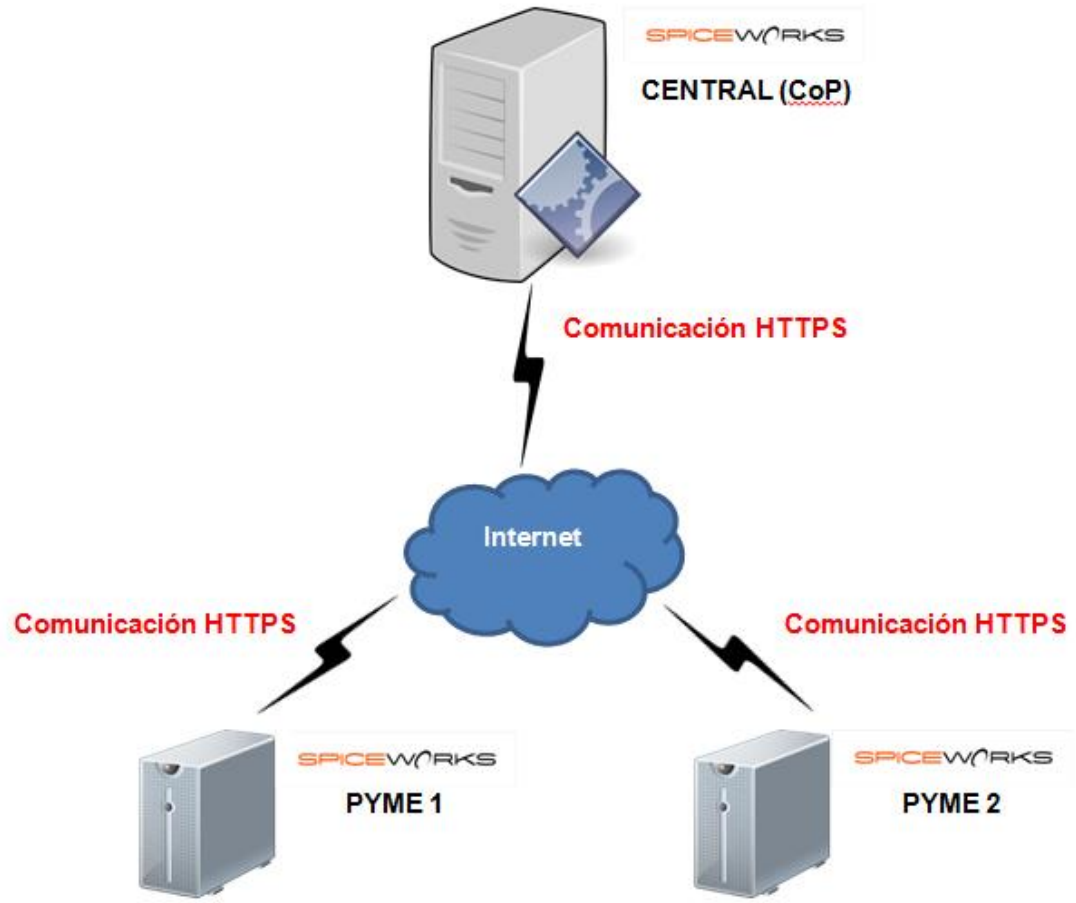
Una vez realizada la configuración del sistema de monitoreo en las dos compañías que son objeto del presente caso de estudio, se aborda el reto de la integración de ambos sistemas en una CoP. Con tal integración, se incrementa la cantidad de información disponible para cada actor de la comunidad, con la posibilidad de tener acceso a la información y base de conocimiento que aportan las demás compañías que forman parte de la CoP. Esta relación garantiza una sinergia, ya que el aumento de la masa crítica permite un tamaño muestral más amplio, y por lo tanto, ofrece la posibilidad de tomar decisiones con argumentos más sólidos. Una toma de decisiones apropiada, se basa en un análisis de las necesidades propias, pero también tiene en cuenta el entorno. Cada vez que se emprende un proyecto, los administradores de IT, sin saberlo, realizan permanentemente ejercicios de vigilancia tecnológica, que les permiten obtener información del entorno para tomar sus propias decisiones.

Para poder realizar una integración de sistemas exitosa, es necesario conocer con detalle la arquitectura y el modelo de datos de las aplicaciones involucradas. En este caso, tanto el origen como el destino tienen las mismas características. También debe tenerse en cuenta el modelo de sincronización de datos, si será unidireccional o bidireccional y si se trata de un proceso sincrónico o asincrónico, además de la periodicidad con la que se realizará la integración. Por último, se debe garantizar elementos de seguridad como comunicación cifrada y que la información suministrada será completamente anónima y no comprometa la confidencialidad para cada una de las compañías que conforman la CoP.

5.1 Arquitectura

La arquitectura propuesta se basa en una plataforma central, que será el nodo común entre todos los actores que pertenecen a la CoP, tal y como se observa en la figura 4 - 1. Cada instalación del software de monitoreo se conecta con la plataforma central con el fin de intercambiar la información que se quiere compartir, en este caso, información de inventario de hardware y software y la base de conocimiento construida a partir de la gestión de incidentes de IT.

Figura 5-1: Arquitectura general de la solución.

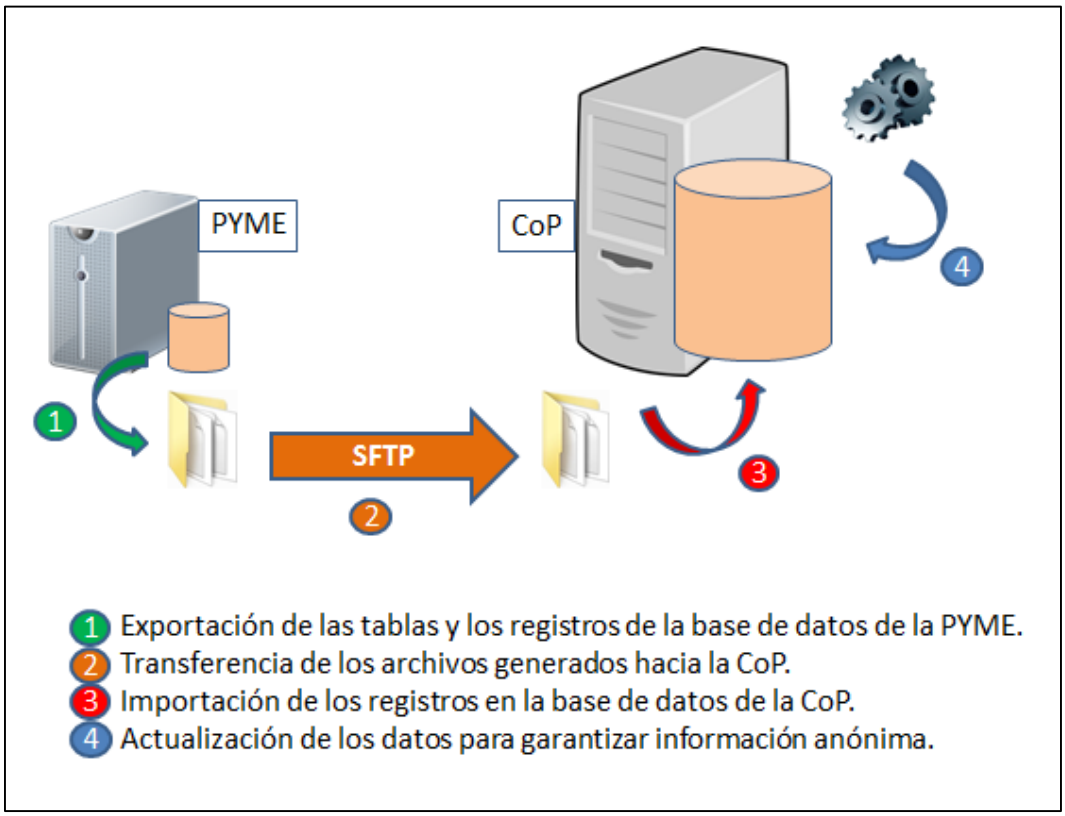


Fuente: elaboración propia.

Teniendo en cuenta los elementos generales mencionados a lo largo de este trabajo, se propone un sistema de integración que ejecuta las siguientes tareas (figura 4 – 2):

- Proceso de exportación de las tablas y registros necesarios para la integración.
- Transferencia de los archivos que contienen la información exportada, desde el cliente (PYME) hacia el servidor (CoP).
- Ejecución de proceso de importación de los registros de la PYME a la base de datos de la CoP.
- Modificación de los datos de la PYME en la base de datos de la CoP para garantizar que son anónimos.

Figura 5-2: Abstracción de alto nivel del modelo de integración.



Fuente: elaboración propia.

Este proceso supone una integración asincrónica, debido a las limitaciones del motor SQLite para conexiones remotas, unidireccional y con una periodicidad programable de acuerdo con las necesidades. Para garantizar que la información fluye con la inmediatez característica de las CoP, se propone ejecutar el proceso de integración con una periodicidad de un (1) minuto.

5.1.1 Exportación

El proceso de exportación presenta diversos retos. Inicialmente, debe tenerse en cuenta que el motor de base de datos es SQLite. La conexión a este motor debe realizarse usando el ejecutable “sqlite3.exe” y la librería “sqlite3.dll”. Estos archivos permiten la interacción con la base de datos a partir de la línea de comandos de Microsoft Windows o Powershell, y por ende, desde cualquier archivo de ejecución por lotes (.bat o .ps1). Posteriormente será tratado con detalle el modelo de datos, para identificar las tablas que serán objeto del proceso de exportación.

El proceso de integración se traduce en varios archivos de ejecución de sistema operativo basados en Powershell (Microsoft) y archivos de sentencias para SQLite y FTP.

El proceso de integración, inicia con la conexión a la base de datos, que para el caso de SQLite, no es más que un archivo con extensión “.db”. Por medio de un archivo, se envían a la conexión SQLite, las sentencias necesarias para la exportación, como puede observarse en la figura 4 – 3.

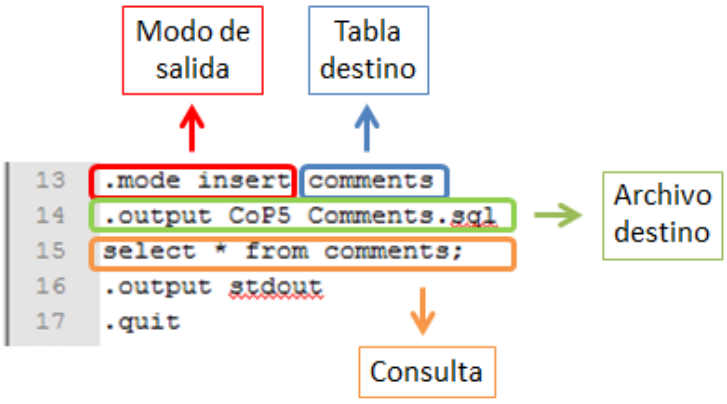
Figura 5-3: Lineas de archivo .bat para conexión a SQLite.

```
#Crea las credenciales para ejecución remota
$pass = ConvertTo-SecureString [redacted] -AsPlainText -Force
$cred=new-object -typename System.Management.Automation.PSCredential -argumentlist ".\administrator",$pass
#Elimina los archivos generados en la ejecución anterior
del c:\Spiceworks\db\IntegracionCoP\1\CoP*.sql
cd c:\Spiceworks\db\IntegracionCoP\1
#Establece conexión con la base de datos local y ejecuta los comandos correspondientes
#para exportar los registros
type .\ScriptExport_SQLite.txt | .\sqlite3 c:\Spiceworks\db\spiceworks_prod.db
#Se realiza la transferencia del archivo concatenado por FTP
ftp -n -s:ScriptFTP.dat [redacted]
#Ejecuta las tareas de importación en la CoP
Invoke-Command -ComputerName [redacted] -FilePath C:\Spiceworks\db\IntegracionCoP\1\IntegracionCoP.ps1 -Credential $cred
exit
```

Fuente: elaboración propia.

El archivo que contiene las sentencias para ejecución en SQLite (figura 4 – 4), se encarga de configurar el modo de salida para que sea en formato “INSERT”, redireccionando el resultado a un archivo “.sql”, además de definir el nombre de la tabla destino. Este modo genera un archivo de salido listo para ser importado en una base de datos con la misma estructura, en este caso, la base de datos de la CoP. Después de configurar el modo de salida, se realiza la consulta a la tabla que se desea exportar. Este proceso se repite cuantas veces sea necesario. Para finalizar, se cierra la conexión a la base de datos para evitar sesiones huérfanas o inactivas.

Figura 5-4: Líneas de ejecución sobre SQLite para exportación.



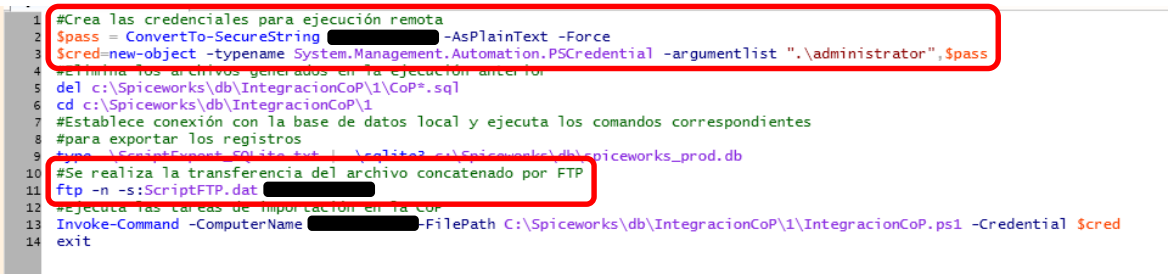
Fuente: elaboración propia.

5.1.2 Transferencia FTP

Para realizar la transferencia de los archivos generados en la exportación, se usa el protocolo FTP (File Transfer Protocol). Es importante que el tipo de conexión entre el cliente y el servidor se realice de forma segura. Para esto, se establece una relación de confianza entre ambos hosts, agregando origen o destino, según sea el caso, en el listado "TrustedHosts" propio del sistema operativo. Adicionalmente, se requiere permiso de ejecución de comandos remotos a nivel de Powershell, desde el cliente.

Previamente, se realiza la configuración del servicio FTP sobre IIS en el servidor de la CoP. Las credenciales de autenticación sobre este servidor se almacenan en variables y se envían de forma cifrada al momento de la negociación entre los hosts (ver figura 4 – 5). Una vez garantizados todos los elementos anteriores, se inicia la transferencia de archivos, usando una entrada de comandos ftp, que se encuentra almacenada en un archivo ".dat". Una vez finalizada la transferencia, se cierra la sesión con el servidor de la CoP.

Figura 5-5: Lineas para transferencia de archivos por ftp.



Fuente: elaboración propia.

5.1.3 Importación en la CoP

Una vez transferidos los archivos que contienen los datos a importar, se dispara la tarea de importación de los registros en la base de datos de la CoP. Por tratarse de un motor idéntico, incluyendo la estructura de datos, la conexión se realiza tal y como se mencionó en la sección “4.1.1. Exportación”. La diferencia radica en la naturaleza de las sentencias a ejecutar, debido a que se trata de una importación, como puede observarse en la figura 4 - 6. Inicialmente se realiza un proceso de borrado de los registros de la PYME en la CoP, con el fin de garantizar la integridad de la información y evitar la duplicidad de los datos. Posteriormente, se procede con la inserción de los registros en las tablas correspondientes. Al finalizar este proceso, se eliminan los archivos de origen.

Figura 5-6: Sentencias para importación de registros en SQLite.

```
.read 0_CoPDeletes.sql
.read CoP1_devices.sql
.read CoP2_software.sql
.read CoP3_softwareinstallations.sql
.read CoP4_tickets.sql
.read CoP5_comments.sql
.quit
```

Fuente: elaboración propia.

5.1.4 Modificación de datos

Con el fin de garantizar que los datos consignados en la CoP son anónimos, debe realizarse una modificación de la información. Una vez analizada la estructura de los datos que serán transferidos, se encuentra que los datos a modificar corresponden al nombre de máquina, dirección IP y MAC Address, para el inventario de hardware. Este proceso se realiza con la ejecución de la sentencia UPDATE correspondiente, en la base de datos de la CoP. Gracias a que la base de datos no cuenta con claves primarias o foráneas asociadas a estos campos, no se hace necesario hacer extensiva la actualización de los datos a otras tablas.

5.2 Estructura de datos

Para realizar un proceso de integración exitoso, es necesario realizar un análisis exhaustivo de la estructura de datos del origen y el destino. En este caso, es suficiente con el estudio del modelo entidad-relación de una de las bases de datos, ya que tanto las PYMEs como la CoP contarán con el mismo diccionario de datos.

Para iniciar, se realiza un proceso de exportación de la estructura de datos. El archivo resultante brinda información acerca de los objetos contenidos en la base de datos, tablas, campos, tamaños y tipos.

De conformidad con la información que se desea compartir con la comunidad de práctica, y después de realizar un análisis detallado del diccionario de datos, se identifican 5 tablas fundamentales para el proceso de integración:

- Devices: Contiene el inventario de hardware.
- Software: Contiene el listado de aplicaciones encontradas a nivel de compañía.
- Software_installations: Contiene el inventario de software instalado a nivel de máquina.
- Tickets: Contiene la información de encabezado de los incidentes de IT.
- Comments: Contiene los comentarios realizados a lo largo de la vida del incidente de IT. De esta tabla solo se exportan los registros que se marcan como “públicos” en la aplicación a nivel de PYME.

Con esta información identificada, se alimenta el proceso de integración.

Una vez superada la fase de integración, los usuarios podrán autenticarse en el servidor que contiene la CoP, para consultar reportes, incidentes y soluciones de todos los miembros. Es tarea del usuario aprovechar las bondades de la información que cada actor aporta a la CoP.

6. Conclusiones y recomendaciones

6.1 Conclusiones

Gracias a la labor realizada para obtener los resultados del presente trabajo, fueron identificados varios aspectos relevantes, relacionados con la administración de IT, la seguridad y la participación de los administradores de IT en CoP. Estas conclusiones surgen después de realizar una reunión de retrospectiva con las áreas de IT de las compañías involucradas, a manera de resumen del caso de estudio realizado:

- La PYME realiza procesos de administración de IT que normalmente responden a acciones correctivas, debido a que no cuentan con una cultura de prevención que los motive a usar herramientas de monitoreo y generación de alertas.

- Un sistema de monitoreo y administración de incidentes de IT le permite al administrador de IT tener un control más detallado sobre su área, además de darle mayor visibilidad dentro de la compañía, ya que le permite generar indicadores de gestión y proponerse metas en períodos de tiempo.

- Se encontró que el administrador de IT en una PYME considera que las herramientas de monitoreo son costosas además de que pueden degradar el rendimiento de su IT. Esta opinión se logra desvirtuar gracias al análisis de opciones de sistema de monitoreo presentado en este trabajo.

- El administrador de IT evita participar en CoP debido al tiempo que puede tomarle dicha tarea. Adicionalmente, percibe poco valor de retorno debido a la ausencia de cultura de gestión del conocimiento. Este aspecto logra superarse gracias a un sistema automático de integración con una CoP a partir de su propio sistema de monitoreo y gestión de incidentes de IT.

- La preocupación más sobresaliente a la hora de mencionar la posibilidad de conformar un proceso de integración con una CoP, radica en la confidencialidad de la información. Sin embargo, presentando los argumentos técnicos que soportan la seguridad de la información y el carácter anónimo de la misma, se mitiga ampliamente este riesgo.

- El sistema de monitoreo y administración de incidentes de IT le permite al administrador de IT tener un control más detallado sobre su área, además de darle mayor visibilidad dentro de la compañía, ya que le permite generar indicadores de gestión y proponerse metas en períodos de tiempo.

6.2 Recomendaciones

Gracias a los hallazgos obtenidos en el presente trabajo, a nivel técnico, se sugiere realizar un ejercicio similar a escala mayor, con el fin de identificar posibles eventos erróneos debidos a la concurrencia sobre la base de datos. El sistema de integración fue realizado para una plataforma Microsoft, sin embargo, en trabajos futuros podría analizarse la posibilidad de presentar un modelo genérico que sea independiente del sistema operativo sobre el que corre la aplicación de monitoreo. Por último, y no menos importante, la sensibilización de la comunidad de IT que forma parte de las PYMEs debería formar parte de una estrategia de política pública, reconociendo que esta población conforma un porcentaje alto de las compañías de la región.

A. Anexo: Diccionario de datos

CREATE TABLE "comments" ("id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, "ticket_id" integer NOT NULL, "body" text NOT NULL, "created_at" datetime, "updated_at" datetime, "created_by" integer, "is_public" boolean DEFAULT 't', "attachment_location" varchar(255), "attachment_content_type" varchar(255), "attachment_name" varchar(255), "is_purchase" boolean DEFAULT 'f', "is_labor" boolean, "is_inventory" boolean DEFAULT 'f', "collaborator_id" integer, "remote_id" integer, "comment_type" varchar(255) DEFAULT 'response' NOT NULL);

CREATE TABLE "devices" ("id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, "name" varchar(50) NOT NULL, "type" varchar(50), "description" varchar(80), "server_name" varchar(50), "domain" varchar(50), "uuid" varchar(50), "manufacturer" varchar(50), "model" varchar(50), "os_serial_number" varchar(70), "windows_product_id" varchar(50), "serial_number" varchar(75), "ip_address" varchar(15), "mac_address" varchar(50), "operating_system" varchar(64), "version" varchar(50), "windows_user" varchar(50), "primary_owner_name" varchar(50), "memory" integer, "management_oid" varchar(75), "up_time" varchar(50), "last_boot_up_time" datetime(30), "service_pack_major_version" integer(3), "service_pack_minor_version" integer(3), "number_of_licensed_users" integer(3), "number_of_processors" integer(3), "processor_type" varchar(50), "created_on" datetime, "updated_on" datetime, "kernel" varchar(255), "page_count" integer, "install_date" datetime, "device_type" varchar(255), "current_user" varchar(255), "bios_version" varchar(255), "location" varchar(255), "online_at" datetime, "offline_at" datetime, "asset_tag" varchar(255), "manually_added" boolean DEFAULT 'f', "bios_date" date, "c_purchase_price" float, "c_purchase_date" date, "b_name" varchar(50), "b_location" varchar(255), "b_device_type" varchar(255), "b_asset_tag" varchar(255), "b_manufacturer" varchar(50), "b_model" varchar(50), "b_primary_owner_name" varchar(50), "b_serial_number" varchar(75), "warning_alert_count" integer DEFAULT 0, "error_alert_count" integer DEFAULT 0, "open_ticket_count" integer DEFAULT 0, "auto_tag" varchar(255), "dn" varchar(255), "user_tag" varchar(255), "exclude_tag" varchar(255), "last_scan_time" datetime, "spice_version" integer, "vpro_level" integer(4) DEFAULT 0, "last_backup_time" datetime, "user_id" integer, "user_primary" boolean DEFAULT 'f', "swid" varchar(255), "product_categories" varchar(255), "domain_role" integer DEFAULT -1, "b_description" varchar(80), "site_id" integer, "reported_by_id" integer, "ip_comparable" integer DEFAULT 0, "scan_state" varchar(255), "last_qrcode_time" datetime, "mdm_service_id"

integer, "product_info_id" integer, "processor_architecture" varchar(255), "os_architecture" varchar(255), "scan_preferences" varchar(255), "raw_model" varchar(255), "raw_manufacturer" varchar(255), "raw_operating_system" varchar(255), "raw_processor_type" varchar(255), "port_scan_results" varchar(255), "vm" boolean DEFAULT 'f');

CREATE TABLE "software" ("id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, "name" varchar(255), "vendor" varchar(50), "install_date" date, "url_info_about" varchar(150), "url_update_info" varchar(150), "licenses" integer, "software_installations_count" integer DEFAULT 0, "warning_alert_count" integer DEFAULT 0, "error_alert_count" integer DEFAULT 0, "open_ticket_count" integer DEFAULT 0, "created_at" datetime, "updated_at" datetime, "display_name" varchar(255), "swgroup" varchar(255), "summary" varchar(255));

CREATE TABLE "software_installations" ("id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, "software_id" integer, "computer_id" integer, "software_license_id" integer, "product_id" varchar(150), "identity" varchar(150), "version" varchar(50) DEFAULT 'unknown', "install_date" date, "created_at" datetime, "updated_at" datetime, "license_verified" boolean DEFAULT 'f', "spice_version" integer, "license_verified_by" varchar(255), "license_verified_on" datetime, "uninstall_string" varchar(255), "from_wmi" boolean DEFAULT 'f', "network_user_id" integer, "install_location" varchar(255), "from_linux" boolean DEFAULT 'f');

CREATE TABLE "tickets" ("id" INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, "summary" varchar(50) NOT NULL, "status" varchar(255) NOT NULL, "description" text, "priority" integer, "created_at" datetime, "updated_at" datetime, "closed_at" datetime, "created_by" integer, "assigned_to" integer, "viewed_at" datetime, "reopened" boolean, "requires_purchase" boolean, "category" varchar(255), "external_id" varchar(255), "email_message_id" varchar(255), "status_updated_at" datetime, "warning_alert_count" integer DEFAULT 0, "error_alert_count" integer DEFAULT 0, "muted" boolean, "site_id" integer, "master_ticket_id" integer, "reported_by_id" integer, "due_at" datetime, "remote_id" integer, "synced_at" datetime, "sharer_id" integer, "parent_id" integer, "c_subcategory" varchar(255), "c_state" varchar(255));

B. Anexo: Archivos de integración

Archivo de Integración en Powershell:

```
#Crea las credenciales para ejecución remota
$pass = ConvertTo-SecureString “Contraseña" -AsPlainText -Force
$cred=new-object -typename System.Management.Automation.PSCredential -
argumentlist ".\administrator",$pass
#Elimina los archivos generados en la ejecución anterior en caso de que existan
del c:\Spiceworks\db\IntegracionCoP\1\CoP*.sql
cd c:\Spiceworks\db\IntegracionCoP\1
#Establece conexión con la base de datos local y ejecuta los comandos correspondientes
#para exportar los registros
type .\ScriptExport_SQLite.txt | .\sqlite3 c:\Spiceworks\db\spiceworks_prod.db
#Se realiza la transferencia del archivo concatenado por FTP
ftp -n -s:ScriptFTP.dat IP_CoP
#Ejecuta las tareas de importación en la CoP
Invoke-Command -ComputerName IP_CoP -FilePath
C:\Spiceworks\db\IntegracionCoP\1\IntegracionCoP.ps1 -Credential $cred
#Elimina los archivos generados en la ejecución anterior en caso de que existan
del c:\Spiceworks\db\IntegracionCoP\1\CoP*.sql
exit
```

Archivo de Exportación en SQLite:

```
.mode insert devices
.output CoP1_devices.sql
select * from devices;
.mode insert software
```

```
.output CoP2_software.sql
select * from software;
.mode insert software_installations
.output CoP3_softwareinstallations.sql
select * from software_installations;
.mode insert tickets
.output CoP4_Tickets.sql
select * from tickets;
.mode insert comments
.output CoP5_Comments.sql
select * from comments where is_public = "t";
.output stdout
.quit
```

Archivo de Transferencia FTP:

```
user usuarioftp
Contraseñaftp
bin
cd db/IntegracionCoP/1
put c:\Spiceworks\db\IntegracionCoP\1\CoP1_devices.sql
put c:\Spiceworks\db\IntegracionCoP\1\CoP2_software.sql
put c:\Spiceworks\db\IntegracionCoP\1\CoP3_softwareinstallations.sql
put c:\Spiceworks\db\IntegracionCoP\1\CoP4_Tickets.sql
put c:\Spiceworks\db\IntegracionCoP\1\CoP5_Comments.sql
quit
```

Archivo de Importación en Powershell:

```
#Actualizando la base de datos de la CoP
cd "C:\Program Files (x86)\Spiceworks\db\IntegracionCoP\1"
type .\ImportacionCoP.txt | .\sqlite3 "C:\Program Files
(x86)\Spiceworks\db\spiceworks_prod.db"
#Eliminando archivos de importación
del "C:\Program Files (x86)\Spiceworks\db\IntegracionCoP\1\CoP*.sql"
#Fin
exit
```

Bibliografía

Berkani, L., Driff, L. N., & Guessoum, A. (2013). Social validation of learning objects in online communities of practice using semantic and machine learning technique.

Business Software Alliance (BSA), (2014). The Compliance Gap. BSA Global Software Survey. USA.

CMMI Institute, (2014). Published Appraisal Results. Disponible en https://sas.cmmiinstitute.com/pars

Congreso de la República de Colombia. Ley 1341 de 2009. República de Colombia - Gobierno Nacional.

De León Sigg, M., Villa Cisneros, J. L., Vázquez Reyes, S., & Salcedo, J. A. R. (2014). Description of information technologies adoption in small enterprises using the lazy-user model: A study case. RISTI - Revista Ibérica de Sistemas e Tecnologías de la Información, 1(E1), 91-104.

Droschl, Georg (2004). Communities of Practice: An Integrated Technology Perspective. Journal of Universal Computer Science, vol. 10, No. 3. 284-293.

El Ghali, A., Tifous, A., Buffa, M., Giboin, A., & Dieng-Kuntz, R. (2007). Using a semantic wiki in communities of practice. CEUR Workshop Proceedings, 308 22-31.

Escobar, M.C., González, E. A. (2004). Métodos de Desición Multicriterio. Denarius – Revista de Economía y Administración.

Frezzo, D., Cinque, G. & Cinque, M. (2008). Use of Web 2.0 Technologies and Interaction Design to Enhance a Networking Instructor Community of Practice. Cisco Systems Inc.

Ghosh, B., & Scott, J. E. (2009). Using a community of practice to enhance data quality in a distributed healthcare information system. ACIS 2009 Proceedings - 20th Australasian Conference on Information Systems, 340-350

M.A. Abdullah and M.I,H. Bakar (2000). Small and medium enterprises in Asian Pacific countries. Huntington, NY. Nova Science Publishers.

Morgan, D. E., Banks, W., Goodspeed, D. P., & Kolanko, R. (1975). Computer Network Monitoring System. IEEE Transactions on Software Engineering, SE-1(3), 299-311.

Nie, J. (2007). A study of information technology adoption for small and medium sized enterprises strategic competitiveness. International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2007, 4337-4341.

Oficina de Comercio del Gobierno Británico (2011). ITIL – Gestión de Servicios de TI. Gobierno Británico 2011. Disponible en http://itil.osiatis.es

Olszak, C. M., & Ziemba, E. (2008). Communities of practice in knowledge management and organizational learning. Harnessing Knowledge Management to Build Communities - Proceedings of the 11th Annual Australian Conference on Knowledge Management and Intelligent Decision Support, ACKMIDS 08

Preece, J., Maloney-Krichmar, D. and Abras, C. History of Emergence of Online Communities. In B. Wellman (Ed.), Encyclopedia of Community. Berkshire Publishing Group, Sage, 2003.

Project Management Institute (PMI), (2008). Project Management Body of Knowledge (PMBOK), 4a Edición, 267, Project Management Institute, Inc, Pennsylvania, USA.

Romero, Carlos. (1996). Análisis de las Decisiones Multicriterio. 1a Edición. Isdefe.

Vásquez, Sergio. (2011). Comunidades de Práctica. Europe Business School. Educar vol. 47. 51-68.

Wenger, Étienne. (1998). Communities of Practice: Learning, meaning and indentity. Cambridge University Press.