FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

IMPLEMENTACIÓN DE LOS SERVICIOS DE RESPALDO Y MESA DE AYUDA EN UN ENTORNO CLOUD PARA UNA EMPRESA IMPORTADORA

AUTOR

Rubén Darío Clavijo Pinzón

AÑO

2018

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

IMPLEMENTACIÓN DE LOS SERVICIOS DE RESPALDOS Y MESA DE AYUDA EN UN ENTORNO CLOUD PARA UNA EMPRESA IMPORTADORA

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información

Profesor Guía

MSc. Luis Santiago Criollo Caizaguano

Autor

Rubén Darío Clavijo Pinzón

Año

2018

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo, Implementación de los servicios de respaldos y mesa de ayuda en un entorno cloud para una empresa importadora, a través de reuniones periódicas con el estudiante, Rubén Darío Clavijo Pinzón, en el semestre 2018-2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Luis Santiago Criollo Caizaguano
Magister en Redes de Comunicaciones
C.I.: 1717112955

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Implementación de los servicios de respaldos y mesa de ayuda en un entorno cloud para una empresa importadora, del estudiante, Rubén Darío Clavijo Pinzón, en el semestre 2018-2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Iván Patricio Ortiz Garcés

Magister en Redes de Comunicaciones

C.I.: 0602356776

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Rubén Darío Clavijo Pinzón

C.I.: 1721329520

AGRADECIMIENTOS

Agradezco a Dios por darme la fuerza de seguir adelante día tras día, a mis padres y mi hermano por apoyarme en todo momento de mi vida, a mi novia Diana por acompañarme incondicionalmente en todo aspecto, al Ing. Santiago Criollo por su guía, ayuda y confianza depositada en mí y al Ing. Iván Ortiz por toda su colaboración para la culminación de este trabajo de titulación.

DEDICATORIA

Le dedico este trabajo de a mi hijo Misael Adrián, mi motivación para seguir adelante día tras días, para cumplir metas y superarme en la vida.

RESUMEN

El presente trabajo de titulación tiene como objetivo implementar una Mesa de Ayuda y un Sistema de Respaldos mediante herramientas basadas en tecnología *CLOUD*. Referente a la mesa de ayuda se evaluó las necesidades de los usuarios con respecto a los servicios de TI, se analizó el manejo que se llevaba en la empresa para determinar problemas y plantear soluciones, guiándose en el marco de referencia ITIL v3 se diseñó la estructura y procesos de la fase de operación del servicio, se analizó tecnologías existentes en el mercado de mesa de ayuda en la nube, se seleccionó la herramienta más óptima y se realizó su respectiva implementación.

Referente al sistema de respaldos se analizó los procesos que se efectuaban para respaldar información de servidores, bases de datos y usuarios, de tal forma se pudo determinar problemas y plantear soluciones, tomando en cuenta las recomendaciones de los marcos de referencia COBIT, Normas ISO/IEC 20000, Normas ISO/IEC 17799, INEI se diseñó una Política de Respaldos, se evaluó las tecnologías existentes en el mercado para respaldos de información en la nube, se eligió la más óptima y finalmente se implementó la herramienta parametrizada de acuerdo con la Política establecida.

Como resultado se obtuvieron una mayor satisfacción del usuario interno referente a los servicios prestados por el área de sistemas, un incremento en la efectividad de la mesa de ayuda, mayor productividad del personal de soporte técnico, mayor grado de disponibilidad de los respaldos de la información, una gestión más centralizada y la determinación en tiempo real del estado de los respaldos. Como conclusión se puede decir que la implementación de servicios como mesa de ayuda y sistemas de respaldos en cualquier organización permite garantizar la entrega de servicios de calidad a los clientes de la empresa generando un valor agregado a sus productos.

ABSTRACT

The objective of the present titling work is to implement a Help Desk and a Support System through tools based on CLOUD technology. Regarding the help desk, the needs of the users regarding the IT services were evaluated, the management carried out in the company to determine problems and propose solutions was analyzed, guided in the frame of reference ITIL v3 the structure was designed and processes of the operation phase of the service, existing technologies were analyzed in the help desk market in the cloud, the most optimal tool was selected and its respective implementation was carried out.

Regarding the backup system, the processes that were carried out to support information on servers, databases and users were analyzed, in such a way that problems could be identified and solutions could be proposed, taking into account the recommendations of the COBIT reference frameworks, ISO / Norms. IEC 20000, ISO / IEC 17799, INEI a Support Policy was designed, the existing technologies in the market were evaluated for information backup in the cloud, the most optimal was chosen and finally the parameterized tool was implemented according to the Policy established

As a result, greater internal user satisfaction was obtained regarding the services provided by the systems area, an increase in the effectiveness of the help desk, higher productivity of technical support personnel, greater availability of information backups, a more centralized management and the determination in real time of the status of the backups. In conclusion, it can be said that the implementation of services such as help desk and backup systems in any organization allows guaranteeing the delivery of quality services to the company's customers, generating added value to their products.

ÍNDICE

INTRODUCCIÓN

La empresa ecuatoriana propuesta para este tema de tesis tiene su giro de negocio en la importación y venta de equipos médicos a hospitales en el Ecuador. En los últimos años ha llegado a convertirse en una de las 5 compañías más grandes del país en el área médica, incrementando su fuerza laboral en el último año de 100 a 230 empleados. Cuenta con sucursales en las principales ciudades del Ecuador (Quito, Guayaquil, Cuenca) y Perú (Lima).

Se conoce que todos los procesos de negocios dependen de manera directa o indirecta de TI por lo tanto la empresa se ha visto en la necesidad de realizar una reestructuración tecnológica enfocada en procesos internos como los son: la implementación de una Mesa de Ayuda y de un Sistema de Respaldos de la Información en un ambiente *cloud*.

Estas implementaciones se realizarán en base a un previo diseño enfocado a diferentes marcos referenciales como lo es ITIL v3 para la Mesa de Ayuda y COBIT, Normas ISO/IEC 20000, Normas ISO/IEC 17799, INEI para el sistema de respaldos.

A continuación, se enlistan algunos casos de éxito en empresas de renombre internacional que han implementado las herramientas seleccionadas en este trabajo de titulación como lo son: la herramienta de Mesa de Ayuda SysAid y las herramientas para respaldo de información de usuarios DRUVA y para respaldos de información de servidores PHOENIX.

Uno de los grandes casos de éxito de SysAid es en la empresa **Fuji Xerox**, donde Daniel Doohan, líder del equipo de aplicaciones de BPS menciona que desde 2010, Fuji Xerox ha utilizado las innovadoras soluciones de software de SysAid para respaldar su oferta de servicios de Business Process Outsourcing. El software les brinda las herramientas para administrar su marco ITIL, lo que les permite enlaces cruciales entre incidentes, problemas y cambios, así como

informes de auditoría efectivos que pueden proporcionar a sus clientes. Es importante destacar que SysAid mantiene un alto nivel de respuesta a sus necesidades, desde su cliente y soporte de problemas hasta su equipo de desarrollo. Esto permite a FUJI XEROX ofrecer una mejor experiencia al cliente, más rápida.

Para hablar de un caso de éxito de DRUVA se lo tiene en la empresa **AVEA** la cual tiene sede en Estambul, Turquía, Avea es una empresa de telecomunicaciones en crecimiento con casi 3000 empleados. Proporcionando cobertura GSM al 98% de Turquía, Avea debe cumplir con las necesidades de redundancia y cumplimiento de datos, ya que respaldan su base de rápido crecimiento de 13,7 millones de clientes. Avea utilizó servidores de archivos locales para albergar sus datos y proporcionar redundancia, pero la compañía necesitaba una opción más escalable. Por tal motivo decidió utilizar DRUVA con lo cual consiguió: instalación en el lugar, elasticidad en la nube, funciones de seguridad multidimensionales, deduplicación del lado del cliente y optimización WAN.

Por último, se tiene un caso de éxito de PHOENIX implementado en la empresa **Phillips Distilling** la cual es una de las industrias más grandes de producción de licores en Estados Unidos, cuenta con más de 300 empleados. Antes de implementar la solución Phoenix la empresa presentaba múltiples desafíos como: compleja gestión de cinta manual, preocupación por perder hasta 7 días de datos, falta de visibilidad y control de los datos remotos de los empleados, sin manejabilidad central. Con la solución implementada la empresa consiguió una forma de eliminar su sistema de cintas heredado y gestionar de forma centralizada las copias de seguridad y el archivo de la infraestructura y los dispositivos del usuario final en la nube.

Los resultados rápidamente evidenciados con Phoenix fueron: 30 horas a la semana guardadas que se habrían gastado administrando cintas, tasa de deduplicación de 15 a 1 y restauración en minutos de directorios completos.

Alcance

El alcance de este trabajo de titulación está dividido en dos ejes fundamentales, el primero es la implementación de una Mesa de Ayuda con una herramienta en ambiente *cloud* que se basará en ciertos procesos y funciones de las fases del Ciclo de Vida de los Servicios. Los procesos que abarcará esta Mesa de Ayuda son específicamente de la fase de operación del servicio:

- Gestión de Eventos
- Gestión de Incidencias
- Gestión de Peticiones
- Gestión de Problemas
- Gestión de Acceso
- Centro de Servicio al Usuario

El segundo es la implementación de un sistema de respaldos con una herramienta en ambiente *cloud* que cumpla la Política de Respaldos a dimensionarse siguiendo lineamientos de diversos marcos referencia como COBIT, Normas ISO/IEC 20000, Normas ISO/IEC 17799, INEI.

Justificación

Actualmente la prestación de Servicios de TI que satisfagan a los clientes internos como externos de una empresa es muy importante, puesto que genera un valor agregado a sus productos. Por tal motivo una implementación de ITIL dentro de una organización ayuda a gestionar con las mejores prácticas dichos servicios.

En la empresa se quiere cumplir con los estándares de calidad para la entrega de servicios de TI, pero se ha evidenciado diversas fallas situándose la más importante en la fase de operación del servicio. Los problemas encontrados en esta fase son un mal manejo de eventos, incidentes, problemas y un bajo desarrollo en el Centro de Servicio al Usuario. Debido a esto se ve la necesidad

de implementar una mesa de ayuda basada en tecnología *cloud* que cumpla con los procesos y funciones de ITIL V3.

Esta implementación dispondrá de ventajas como: flexibilidad, costos menores en su implementación, extensas bases de conocimientos, interfaces de usuarios amigables, diferentes tecnologías como chat en línea, control remoto, entre otras.

Por otro lado, hoy en día la información es el activo más importante en cualquier organización por tal motivo es de suma importancia tener un respaldo de esta. Implementar un sistema de respaldos permite garantizar la continuidad del negocio.

Los inconvenientes evidenciados en la empresa son: no se tiene un proceso tecnificado, regulado, ni basado en estándares para la gestión de respaldos, sin contar, con políticas y lineamientos específicos a seguir. Debido a esto se ve la necesidad de implementar un sistema de respaldos basado en tecnología *cloud* que siga ciertos marcos referenciales.

Objetivos

Objetivo General

Implementar una Mesa de Ayuda y un Sistema de Respaldos mediante herramientas basadas en tecnología *cloud*, que permitan garantizar la entrega de servicios de calidad a los clientes de la empresa generando un valor agregado a sus productos.

Objetivos Específicos

1. Diseñar los servicios de TI requeridos de acuerdo con ITIL V3 y el Modelo de Respaldos de la Información lineado a marcos de referencia como COBIT, Normas ISO/IEC 20000, Normas ISO/IEC 17799, INEI.

2. Implementar una herramienta de Mesa de Ayuda basada en tecnología *cloud* de acuerdo con un previo análisis de las tecnologías existentes en el mercado.

3. Implementar un Sistema de Respaldos mediante una herramienta basada en tecnología *cloud* de acuerdo con un previo análisis de las tecnologías existentes en el mercado.

1. Capítulo I. Marco Teórico

1.1 ITIL v3

"ITIL V3 es un estándar internacional de mejores prácticas en la Gestión de Servicios Informáticos" (Guzmán, 2012, pág. 540). Por medio de ITIL se busca la mejora en la calidad de la Gestión de Servicios de TI. Para entender de mejor forma qué funciones cumple ITIL es necesario conocer el concepto de qué es un servicio y qué es valor del servicio**.**

- **Servicio**

  "Un servicio se puede definir como un medio de entregar valor a los clientes facilitando resultados que los clientes necesitan sin la propiedad de costes y riesgos específicos" (Arqueros, 2013).

- **Valor de Servicio**

  Es el resultado por el que el cliente está dispuesto a pagar. En este proceso intervienen dos factores: Utilidad (funcionalidad que ofrece un producto o servicio para satisfacer una necesidad particular) y Garantía (confirmación que un producto o servicio cumplirá con los requisitos acordados). De tal modo el valor de un servicio de TI se crea por la combinación de utilidad y garantía.

En la figura 1 a continuación se puede observar los componentes que forman el valor de un servicio.

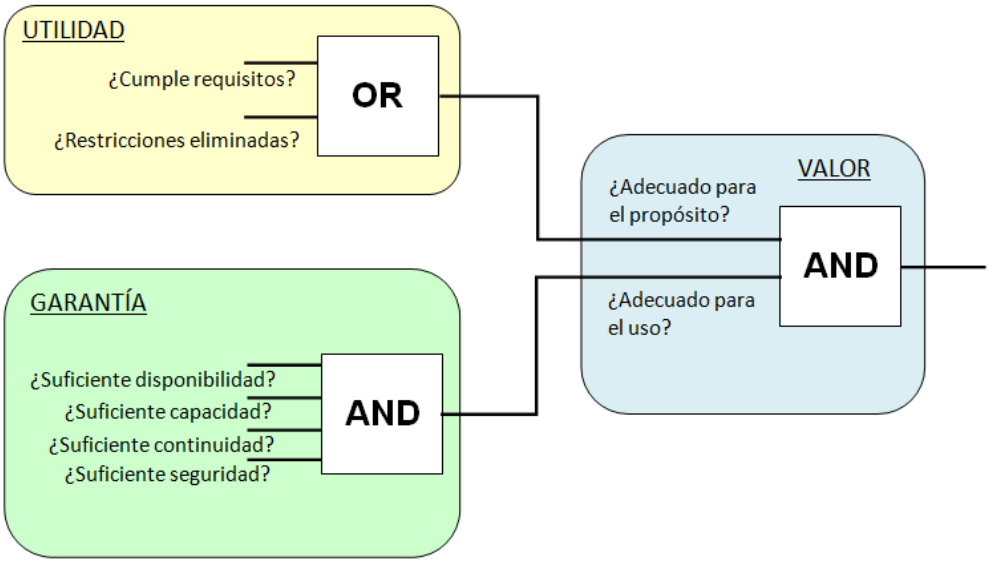


Figura 1. El valor del servicio

Tomado de: Arqueros, 2013.

1.1.1 Clasificación del Ciclo de Vida de un Servicio según ITIL v3

ITIL v3 divide el Ciclo de Vida de un Servicio en cinco fases, observe figura 2

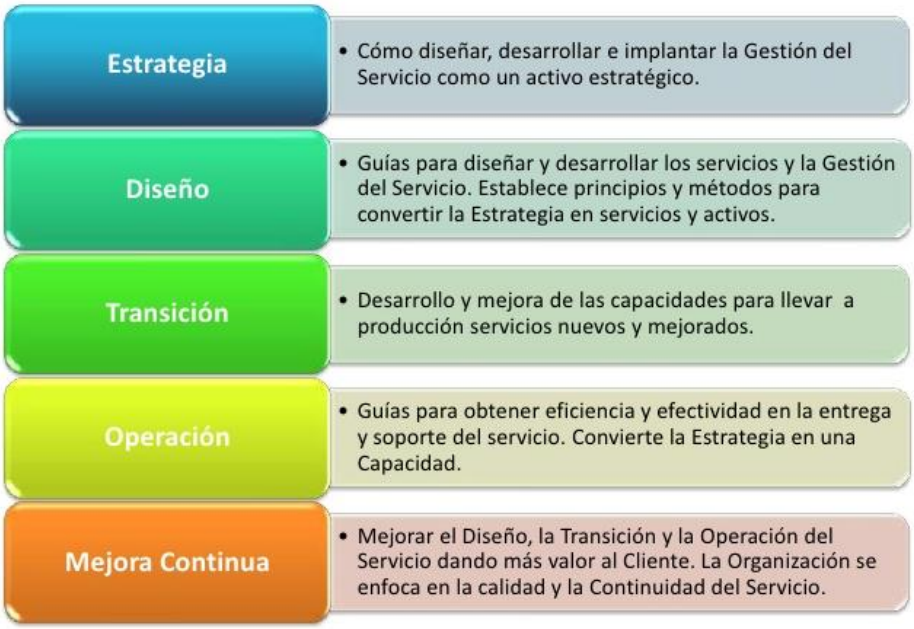


Figura 2. Ciclo de Vida de los Servicios

Tomado de: Tecnofor, s.f.

Para el estudio de las fases mencionas ITIL ha desarrollado 26 procesos operacionales y 6 funciones. Las fases que se toman en cuenta son: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua. En la figura 3 a continuación se puede observar cada fase mencionada con sus respectivos procesos y funciones, los procesos son de color anaranjado y las funciones de color azul.

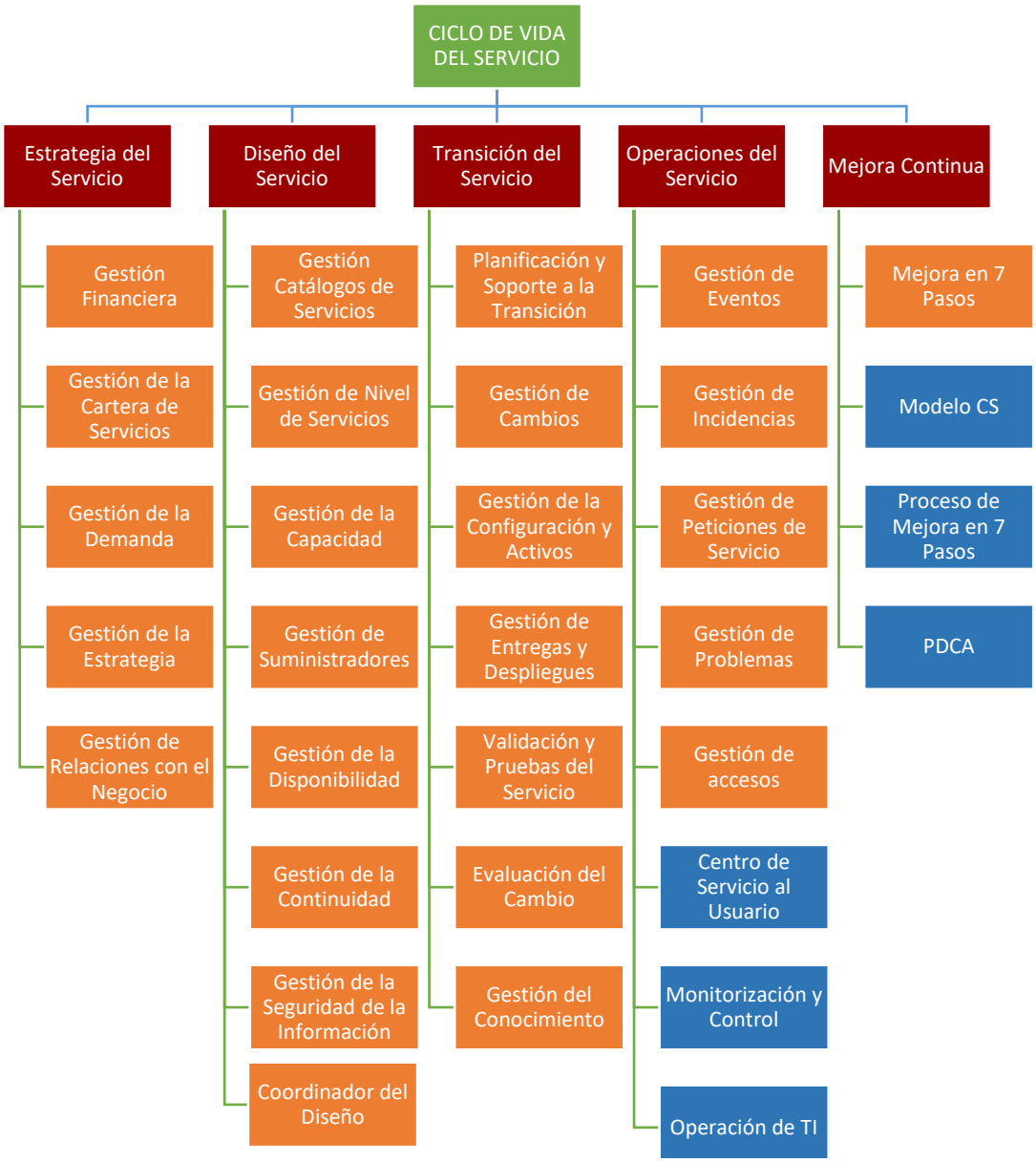


Figura 3. Procesos y Funciones ITIL V3

Adaptado de: Rondanelli, 2013.

1.1.2 Operación del Servicio

Es la cuarta etapa del ciclo de vida del servicio y se la debe vincular con: Brindar un Servicio de Valor (helppeople cloud, s.f.).

“Esta fase desarrolla y explica en detalle la realización y el control de las actividades necesarias para lograr la excelencia operacional a diario, así como el desarrollo de procesos para apoyar tanto el servicio como su realización” (helppeople cloud, s.f.).

El fin de esta fase es brindar, soporte y gestión de los servicios**.** Es una fase crítica ya que aporta valor al cliente y su meta es cumplir con el SLA. Los objetivos de esta fase son la coordinación de: procesos, funciones y actividades. Esta fase comprende 5 procesos y 3 funciones.

1.1.2.1 Fase de operación del servicio: propósito y objetivos

Propósito

- Coordinar y llevar a cabo las actividades y procesos necesarios para entregar y administrar servicios de TI a niveles acordados (SLA) para los usuarios y clientes comerciales (Office of Government Commerce, 2007, p. 33).
- Encargada de la gestión diaria de la tecnología que se emplea para entregar y apoyar servicios. (Office of Government Commerce, 2007, p. 33).

Objetivos

- Conservar la confianza en TI por medio de la entrega y soporte efectivos y eficientes de los servicios de TI acordados (Tecnol, 2012).
- Disminuir el impacto de interrupciones en las actividades del día a día del negocio (Tecnol, 2012).
- Garantizar la entrega de servicios de TI sólo a los usuarios que están autorizados para recibirlos (Tecnol, 2012).

1.1.2.2 Fase de operación del servicio: alcance y valor para el negocio

Alcance

Se basa en la ejecución de todas las actividades continuas que se requieren para entregar y apoyar los servicios. Esto abarca: los servicios, procesos de gestión de servicios, tecnología y gente (Office of Government Commerce, 2007, p. 33).

Valor para el negocio

- Disminuye el coste para la empresa al evitar trabajos no planificados
- Las interrupciones de actividades disminuyen en tiempo y frecuencia.
- Se da la mejora de servicios continuos en otros procesos de ITIL gracias a que se obtiene resultados operacionales e información valiosa.
- Logra cumplir las metas y objetivos dispuestos en la política de seguridad de la organización.
- Entrega un acceso eficiente a los servicios estándar.
- Entrega un fundamento para operaciones automatizadas (Office of Government Commerce, 2007, p. 34).

1.1.2.3 Comunicación en la fase de operación del servicio

Comunicación

La comunicación es un pilar fundamental para la prevención y resolución de problemas en la fase de operación. Dicha comunicación se debe dar entre departamentos de TI, usuarios, clientes internos y los equipos de operación (Office of Government Commerce, 2007).

Los tipos de comunicación incluyen:

- Comunicación operacional de rutina.
- Comunicación entre turnos.
- Informes de desempeño.
- Comunicación en proyectos.

- Comunicación relacionada con cambios.
- Comunicación relacionada con excepciones.
- Comunicación relacionada con emergencias.
- Capacitación en procesos y diseños de servicios nuevos o personalizados.
- Comunicación de estrategia, de diseño y de transición a equipos de operación del servicio.

1.1.2.4 Fase de operación del servicio: herramientas/apoyo/documentos

- Base de datos de errores conocidos (KEDB)
- Autoayuda, solución remota.
- Scripts de diagnóstico.
- Herramientas/apoyo/documentos de telefonía de Distribución automática de llamadas (ACD)]/ Respuesta interactiva de voz (IVR)/ Integración de telefonía y computación (CTI).
- Administración de flujos de trabajo.

1.1.2.5 Roles de la fase de operación del servicio

- Propietario del Servicio.
- Usuario del proceso.
- Dueño y gerente del proceso (gestión de incidentes, gestión de problemas, cumplimiento de solicitudes, gestión de eventos, gestión de accesos).
- Analistas (de primera, segunda y tercera línea – de problemas – de cumplimiento de solitudes).
- Personal (*service desk*, gestión técnica y de aplicaciones, gestión de operaciones de TI).
- Gerente del *service desk*, supervisor del *service desk*, analista del *service desk*, super usuario.

- Gerente/Líder de equipo técnico, analista/arquitecto técnico, operador técnico.
- Gerente de operaciones de TI, líder de turno, analista de operaciones de TI, operador de TI.
- Gerente/líder de equipo de gestión de aplicaciones, analista/arquitecto de aplicaciones.

1.1.2.6 Gestión de Eventos

1.1.2.6.1 Propósito y Objetivo del Proceso

Propósito

Localizar eventos, darles sentido y definir la acción de control más acorde para el mismo. De tal forma la gestión de eventos es la base del monitoreo y control operativo (Office of Government Commerce, 2007).

Objetivos

- La detección de eventos se puede emplear como una base para automatizar muchas actividades rutinarias de Gestión de operaciones, por ejemplo, ejecutar scripts en dispositivos remotos o enviar trabajos para su procesamiento o incluso equilibrar dinámicamente la demanda de un servicio en múltiples dispositivos para mejorar el rendimiento (Office of Government Commerce, 2007).

- Por medio de esto se puede obtener una comparativa entre el desempeño de operación real contra los estándares de diseño y acuerdo de niveles de servicio (SLA) (Office of Government Commerce, 2007).

- Entregar una base sólida para la disponibilidad de los servicios, ayuda a la creación de informes y es un aporte importante para la mejora continua (Office of Government Commerce, 2007).

1.1.2.6.2 Alcance y Actividades del Proceso

Alcance

“La gestión de eventos se puede aplicar a cualquier aspecto de la gestión del servicio que necesite ser controlada y que pueda ser automatizada” (Office of Government Commerce, 2007).

Actividades del proceso

- Notificar evento.
- Detectar el evento.
- Registrar evento.
- Primer nivel de filtrado y correlación de evento.
- Establecer significancia del evento.
- Segundo nivel de correlación de evento.
- ¿Se requieren otras acciones?
- Seleccionar respuesta.
- Revisar acciones.
- Cerrar evento. (Tecnol, 2012).

1.1.2.6.3 Conocimiento general sobre el proceso: términos clave

Evento

Es un cambio de estado que tiene importancia para la gestión del servicio de TI u otro elemento de configuración. El término también se utiliza en el sentido de una alerta o notificación creada por cualquier servicio de TI, elemento de configuración o herramienta de monitoreo. Típicamente, los eventos requieren que el personal de operaciones de TI tome acciones y a menudo conllevan a que se registren incidentes (Office of Government Commerce, 2007, p. 374).

Alerta

Una advertencia de que se ha alcanzado un umbral, algo ha cambiado o se ha producido una falla. Las alertas a menudo son creadas y administradas por las

herramientas de administración del sistema y son administradas por el proceso de administración de eventos (Office of Government Commerce, 2007, p. 362).

Tipos de eventos

- **Informativo**

  Son en los cuales no se necesita una acción y tampoco representa una excepción. Se usan normalmente como indicadores de estados ya sea de equipos, servicios o éxitos en actividades. Ejemplos: se crea un nuevo usuario en un sistema, una cola de impresión a finalizado, una transacción ha finalizado exitosamente, entre otros (Office of Government Commerce, 2007, p. 73).

- **De advertencia**

  Este tipo de evento se genera cuando un dispositivo o servicio está alcanzando un umbral máximo definido. Las herramientas adecuadas, procesos o personas son notificadas por medio de las notificaciones para lograr verificar la situación y de esa forma tomar las medidas adecuadas para evitar una excepción (Office of Government Commerce, 2007, p. 73). Ejemplos de advertencias son:

  - En un servidor el empleo de su memoria se encuentra actualmente en un 50% y va en aumentando. Si llega al 80%, los tiempos de respuesta serán demasiados largos y se incumplirá el OLA para ese departamento.
  - El ancho de banda en un enlace está llegando a un margen del 80% en la última media hora.

- **De excepción**

  Se da cuando un servicio o equipo está trabajando de forma anormal (Office of Government Commerce, 2007, p. 73) Ejemplo:

  - Un servicio se paró y el tiempo de respuesta de una transacción estándar ha reducido más de 15 segundos.
  - Un segmento de la red no responde a las solicitudes de rutina

1.1.2.7 Gestión de Peticiones de Servicio

El término 'Solicitud de servicio' se utiliza como una descripción genérica para muchos tipos de demandas que el usuario hace sobre el departamento de TI. Muchos de estos son cambios pequeños: bajo riesgo, frecuentes, de bajo costo, etc. (por ejemplo, una solicitud para cambiar una contraseña, una solicitud para instalar una aplicación de software adicional en una estación de trabajo en particular, una solicitud para reubicar algunos elementos de equipos de escritorio) o tal vez solo una pregunta solicitando información, pero su escala y naturaleza frecuente y de bajo riesgo significa que se manejan mejor mediante un proceso separado, en lugar de permitir que congestionen y obstruyan los procesos normales de Gestión de incidentes y cambios (Office of Government Commerce, 2007, p. 105).

1.1.2.7.1 Propósito y Objetivo del Proceso

Propósito

En este proceso se busca de tratar todas las solicitudes de servicio de los usuarios (Office of Government Commerce, 2007, p. 105).

Objetivos

- Entregar un canal que sirva para que los usuarios soliciten y reciban servicios estándar, de los que exista un proceso de aprobación previo y calificación predefinido.

- Orientar a clientes y usuarios sobre que procedimientos están disponibles y cuál es el procedimiento para obtener los mismos.

- Se almacena y se entrega a los usuarios los componentes de los servicios estándar solicitados (licencias, medios de software, entre otros).

- Ayudar información general, atender comentarios y quejas.

1.1.2.7.2 Alcance y Actividades del Proceso

Alcance

El proceso requerido para completar con una solicitud variará según exactamente lo que se solicita, pero generalmente se puede dividir en un conjunto de actividades que deben realizarse.

Actividades del proceso

- Recibir solicitud.
- Registrar y validar solicitud.
- Clasificar solicitud.
- Priorizar solicitud.
- Autorizar solicitud.
- Revisar solicitud.
- Ejecutar modelos de solicitud.
- Cerrar solicitud.

1.1.2.7.3 Conocimiento general sobre el proceso: términos clave

Modelo de solicitud

Algunas Solicitudes de Servicio se realizarán con frecuencia y requerirán un manejo consistente para cumplir con los niveles de servicio acordados. Para ayudar con esto, muchas organizaciones desearán crear Modelos de Solicitud predefinidos (Office of Government Commerce, 2007, p. 106).

Solicitud de servicio

Una solicitud de un usuario para información o asesoramiento, o para un cambio estándar o para acceder a un servicio de TI. Por ejemplo, para restablecer una contraseña o para proporcionar servicios de TI estándar para un nuevo usuario.

Las solicitudes de servicio generalmente las maneja un *service desk*, y no requieren que se envíe un RFC (Office of Government Commerce, 2007, p. 390).

Cumplimiento

Realización de actividades para satisfacer una necesidad o requisito. Por ejemplo, al proporcionar un nuevo servicio de TI o cumplir una solicitud de servicio (Office of Government Commerce, 2007, p. 375).

1.1.2.8 Gestión de Accesos

Proceso por medio del cual se concede a usuarios autorizados el derecho a usar un servicio, y por otro lado se bloquea el acceso a usuarios no autorizados. También llamado gestión de derechos o gestión de identidades (Office of Government Commerce, 2007, p. 126).

1.1.2.8.1 Propósito y Objetivo del Proceso

Propósito

Entregar el derecho para que los usuarios puedan emplear un servicio o grupo de servicios (Office of Government Commerce, 2007, p. 126).

Objetivos

- Hacer cumplir las políticas y acciones definidas en Gestión de seguridad y disponibilidad.

- Tener una respuesta ágil frente a las solicitudes de acceso a los servicios, de cambios de derechos de acceso o de restricción de accesos.

- Dar un seguimiento a los permisos concedidos y controlar que estos se usen de forma adecuada.

1.1.2.8.2 Alcance y Actividades del Proceso

Alcance

Es el cumplimiento de las políticas planteadas en la gestión de seguridad de la información. Asegura que los usuarios estén en el derecho de emplear un servicio, pero no se asegura que el acceso se encuentre disponible en los tiempos establecidos, dichos parámetros se proveen en la gestión de la disponibilidad (Office of Government Commerce, 2007, p. 126).

Actividades del proceso

- Solicitar acceso.
- Verificar.
- Proporcionar privilegios.
- Verificar y monitorear el estado de identidad.
- Registrar y dar seguimiento de acceso.
- Eliminar o restringir privilegios.

1.1.2.8.3 Conocimiento general sobre el proceso: términos clave

Acceso

Se refiere al nivel y alcance de la funcionalidad o los datos de un servicio que un usuario tiene derecho a usar (Office of Government Commerce, 2007, p. 127).

Identidad

Se refiere a la información sobre ellos que los distingue como individuos y que verifica su estado dentro de la organización. Por definición, la identidad de un usuario es única para ese usuario (Office of Government Commerce, 2007, p. 127).

Privilegios

Se refieren a la configuración actual mediante la cual un usuario tiene acceso a un servicio o grupo de servicios. Los derechos típicos, o niveles de acceso,

incluyen leer, escribir, ejecutar, cambiar, eliminar (Office of Government Commerce, 2007, p. 127).

Grupos de servicio

La mayoría de los usuarios no usan un solo servicio, y los usuarios que realizan un conjunto similar de actividades usarán un conjunto similar de servicios. En lugar de proporcionar acceso a cada servicio para cada usuario, es más eficiente poder otorgar a cada usuario - o grupo de usuarios - acceso a todo el conjunto de servicios que tienen derecho a usar al mismo tiempo (Office of Government Commerce, 2007, p. 127).

Servicio de directorio

se refiere a un tipo específico de herramienta que se usa para administrar acceso y derechos (Office of Government Commerce, 2007, p. 127).

1.1.2.9 Gestión de Incidente

Es el proceso encargado de todos los incidentes que se produzcan en la organización; entre esto se incluye fallas, preguntas o consultas informadas por los usuarios, esta gestión se da por parte del personal de TI o automáticamente detectadas e informadas por las herramientas de monitoreo de eventos (Office of Government Commerce, 2007, p. 86).

1.1.2.9.1 Propósito y Objetivo del Proceso

Propósito

Restablecer el funcionamiento normal del servicio lo más rápido posible y minimizar el impacto adverso en las operaciones comerciales, asegurando así que se mantengan los mejores niveles posibles de calidad y disponibilidad del servicio. La 'operación de servicio normal' se define aquí como operación de servicio dentro de los límites del SLA (Office of Government Commerce, 2007, p. 86).

Objetivos

- Certificar que los métodos fijados sean empleados para responder, analizar, documentar, informar y gestionar de forma continua incidentes, de una manera rápida y eficiente.

- Aumentar el descubrimiento de incidentes para el negocio y personal de soporte de TI.

1.1.2.9.2 Alcance y Actividades del Proceso

Alcance

El alcance llega a todo incidente que interrumpa o que pueda llegar a interrumpir un servicio. Abarca eventos notificados en forma directa por usuarios, a través del *service desk* o través de una interfaz desde Gestión de Eventos a las herramientas de Gestión de Incidentes (Office of Government Commerce, 2007, p. 86).

Actividades del proceso

Las actividades que se deben realizar para una correcta gestión de incidentes son las siguientes:

- Identificar incidente
- Registrar incidente
- Clasificar incidente
- Priorizar incidente
- Diagnóstico inicial
- Escalar incidente
- Investigar y diagnosticar
- Resolver y recuperar
- Cerrar incidente

1.1.2.9.3 Conocimiento general sobre el proceso: términos clave

Escalas de tiempo

- En cada etapa de la Gestión de Incidentes deben definirse las escalas de tiempo, considerando factores como objetivos globales de respuesta y resolución previamente definidos en los SLA.
- De acuerdo con la prioridad del incidente las escalas de tiempo variarán.
- Deben ser de conocimiento para todos los grupos de soporte (Office of Government Commerce, 2007, p. 87).

Incidente

Una interrupción no planificada de un servicio de TI o una reducción en la calidad de un servicio de TI. La falla de un elemento de configuración que aún no ha impactado al servicio también es un incidente, por ejemplo, la falla de un disco de un conjunto reflejado (Office of Government Commerce, 2007, p. 86).

Incidente grave

Se debe usar un procedimiento separado, con escalas de tiempo más cortas y mayor urgencia, para los incidentes 'importantes'. Una definición de lo que constituye un incidente importante debe acordarse e idealmente corresponderse con el sistema general de priorización de incidentes, de modo que se haga con el proceso principal de incidentes (Office of Government Commerce, 2007, p. 88).

Modelo de incidente

Un Modelo de Incidente es una manera de predefinir los pasos que se deben seguir para manejar un proceso (en este caso, un proceso para tratar un tipo particular de incidente) de una manera acordada. Las herramientas de soporte se pueden usar para administrar el proceso requerido esto asegurará que los

incidentes 'estándar' se manejen en una ruta predefinida y dentro de escalas de tiempo predefinidas (Office of Government Commerce, 2007, p. 87).
Este modelo incluye:

- Los pasos que se deben seguir para manejar el incidente.
- El orden cronológico de estos pasos debe tomarse con, con cualquier dependencia o procesamiento definido.
- Responsabilidades; quién debería hacer qué.
- Tiempos y umbrales para completar las acciones.
- Procedimientos de escalamiento; a quién contactar y cuándo.
- Cualquier actividad de preservación de evidencia necesaria (particularmente relevante para incidentes relacionados con la seguridad y la capacidad).

1.1.2.10 Gestión de Problemas

Es el proceso responsable de la gestión del ciclo de vida de todos los problemas. La gestión de problemas previene proactivamente la ocurrencia de incidentes y minimiza el impacto de los incidentes que no se pueden prevenir.

1.1.2.10.1 Propósito y Objetivo del Proceso

La gestión de problemas es el proceso responsable de gestionar el ciclo de vida de todos los problemas (Office of Government Commerce, 2007, p. 111).

Propósito
Evitar que ocurran los problemas y los incidentes resultantes.

Objetivos

- Eliminar los incidentes recurrentes
- Minimizar el impacto de los incidentes que no pueden evitarse.

1.1.2.10.2 Alcance y Actividades del Proceso

Alcance

Abarca los procedimientos necesarios para diagnosticar la causa raíz de los incidentes y para definir la resolución de esos problemas. También es el encargado de garantizar que la resolución se lleve a cabo a través de los procedimientos de control adecuados, especialmente Gestión de cambios y Gestión de versiones (Office of Government Commerce, 2007, p. 111).

Actividades del proceso

- Detectar problema.
- Registrar problema.
- Clasificar problema.
- Priorizar problema.
- Investigar y diagnosticar problema.
- Encontrar solución temporal.
- Registrar error conocido.
- Resolver problema.
- Cerrar problema.
- Revisar problema mayor.

1.1.2.10.3 Conocimiento general sobre el proceso: términos clave

Problema

ITIL define a un problema como la causa de uno o más incidentes.

Modelos de problema

Al igual que en la Gestión de Incidentes se puede crear un modelo para problemas recurrentes, dichos problemas pueden llegar a ser recurrentes al encontrase con que su resolución definitiva es más costosa que la aplicación en

la cual se usa. Por tal motivo tener un modelo de resolución para este tipo de problemas es útil (Office of Government Commerce, 2007, p. 112).

Error conocido

Se refiere a un problema del cual ya existe una causa raíz documentada y se tiene definido una solución temporal. Los errores conocidos se crean y administran a lo largo del ciclo de Gestión de Problemas. Así como también los errores conocidos pueden ser ubicados por el desarrollo o los proveedores (Office of Government Commerce, 2007, p. 378).

Base de datos de errores conocidos

Permitir un diagnóstico y resolución de incidentes y problemas cuando estos se repitan a través de un almacenamiento de conocimiento previos, este es el propósito de una base de datos de errores conocida (Office of Government Commerce, 2007, p. 123).

Gestión reactiva de problemas

se ejecuta generalmente como parte de la operación de servicio – y por lo tanto está cubierto en esta publicación (Office of Government Commerce, 2007, p. 112).

Gestión proactiva de problemas

e inicia en la operación de servicio, pero generalmente impulsada como parte de la mejora continua del servicio (Office of Government Commerce, 2007, p. 112).

1.2 Mesa de Servicios

Una mesa de servicios es una unidad funcional desarrollada por un conjunto dedicado de personas encargados de atender una variedad de eventos de servicio, por lo general a través de llamadas telefónicas, interfaz web o eventos de infraestructura reportados automáticamente (Office of Government Commerce, 2007, p. 198).

La mesa de servicios es de suma importancia para un departamento de TI dentro de una organización y debe ser el único punto de contacto para los usuarios de TI día a día, y se encargará de todas las incidencias y solicitudes de servicio, por lo general utilizando herramientas de software especializadas para iniciar sesión y administrar todos esos eventos (Office of Government Commerce, 2007, p. 198).

1.2.1 Justificación y Roles de la Mesa de Servicios

En la actualidad no se necesita mucha justificación para entender que una mesa de servicios es la opción preferida dentro de las organizaciones para resolver problemas de TI de primera línea. Los beneficios son los siguientes:

- Mejor servicio al cliente, percepción y satisfacción.
- Mayor accesibilidad a través de un único punto de contacto, comunicación e información.
- Mejor calidad y rapidez en la respuesta a las solicitudes de los clientes o usuarios.
- Mejora del trabajo en equipo y la comunicación.
- Enfoque mejorado y un enfoque proactivo para la prestación de servicios.
- Un impacto comercial negativo reducido.
- Infraestructura y control mejor administrados.
- Mejor uso de los recursos de soporte de TI y mayor productividad del personal comercial.
- Información de gestión más significativa para el apoyo de decisiones.

1.2.2 Objetivos

“El objetivo principal de *service desk* es restablecer el "servicio normal" a los usuarios lo más rápido posible. En este contexto, la "restauración del servicio" se entiende en el sentido más amplio posible” (Office of Government Commerce, 2007, p. 199). Esto puede abarcar la solución de un error técnico, cumplir una

solicitud de servicio o responder una consulta, en fin, todo lo que sea requerido para permitir que los usuarios vuelvan a funcionar satisfactoriamente.

Las responsabilidades específicas incluirán:

- Registrando todos los detalles relevantes de solicitud de incidente / servicio, asignando códigos de categorización y priorización.
- Proporcionar investigación y diagnóstico de primera línea
- Resolviendo esas incidencias / solicitudes de servicio que pueden.
- Aumento de incidentes / solicitudes de servicio que no pueden resolver dentro de escalas de tiempo acordadas.
- Mantener a los usuarios informados sobre el progreso.
- Cerrando todos los incidentes resueltos, solicitudes y otras llamadas.
- Realización de llamadas / encuestas de satisfacción del cliente / usuario según lo acordado.
- Comunicación con los usuarios: mantenerlos informados sobre el progreso del incidente, notificándoles sobre cambios inminentes o interrupciones acordadas, etc. (Office of Government Commerce, 2007, p. 199).

1.2.3 Estructura organizacional de la Mesa de Servicios

Existen muchas formas de estructurar y ubicar una mesa de servicios, a continuación, se analizarán las principales, pero en realidad esto depende de la necesidad de la organización, bien pudiendo ser una combinación de las listadas a continuación.

1.2.3.1 Service Desk Local

La mesa de servicios se encuentra ubicada dentro o físicamente cerca de la comunidad de usuarios con la que trabajo. Por lo general ayuda a la comunidad de usuarios y entrega una presencia visible, que a algunos usuarios les gusta, pero en muchos casos es ineficiente y costoso para los recursos debido a que el personal técnico está atado esperando para tratar incidentes cuando el volumen

y la tasa de llegada de llamadas no justifiquen esto (Office of Government Commerce, 2007, p. 200).

Sin embargo, sí existen razones por la de implementar una Mesa de Servicio Local:

- Lenguaje y diferencias culturales o políticas
- Diferentes zonas horarias
- Grupos especializados de usuarios
- La existencia de servicios personalizados o especializados que requieren conocimientos especializados
- VIP / estado de criticidad de los usuarios.

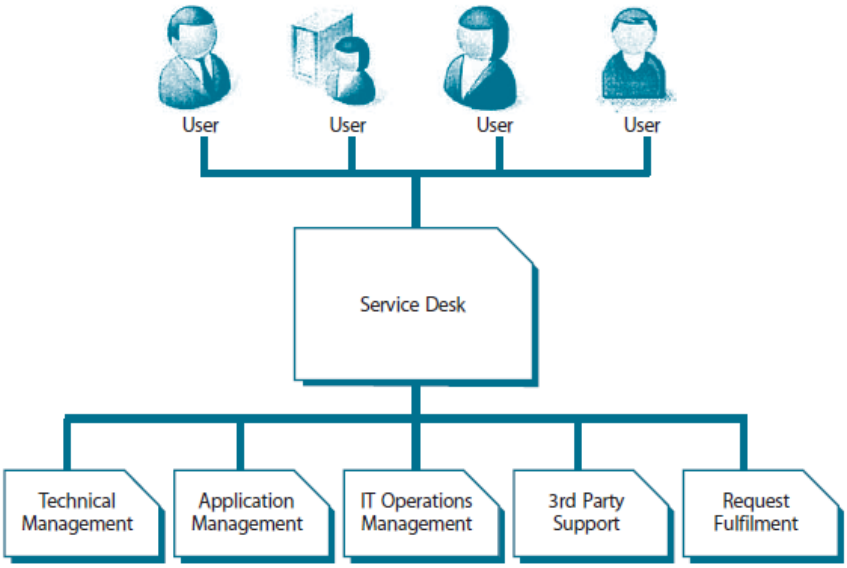


Figura 4. Mesa de Servicios Local

Tomado de: Office of Govemment Commerce, 2007, p. 201.

1.2.3.2 Mesa de Servicios Centralizada

Una posibilidad valida también es reducir el número de mesa de servicios locales en una región combinándolos en una sola ubicación o un pequeño conjunto de ubicaciones. Esto permite ser más eficiente y rentable dado que hay una disminución en la sobrecarga de staff desaprovechándose y además para

los eventos que requieran niveles más altos de habilidades (que comúnmente son los menos frecuentes), no se necesita uno en cada ubicación, sino que se puede consolidar también a través de una segunda línea de soporte centralizada (Office of Government Commerce, 2007, p. 201)

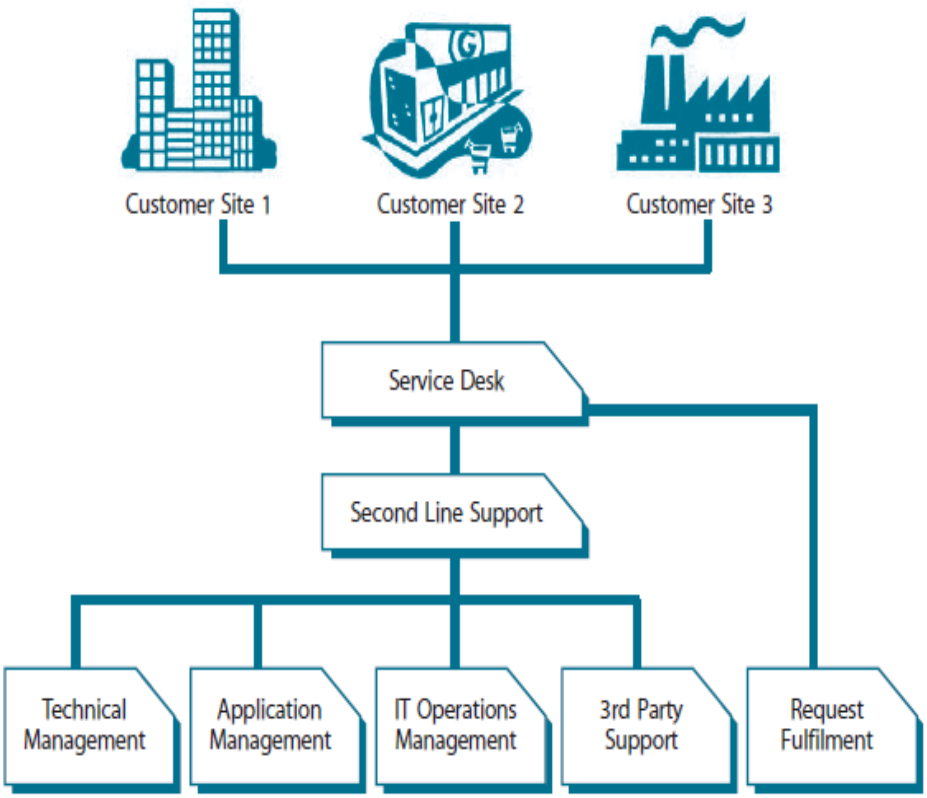


Figura 5. Mesa de Servicios Centralizada

Tomado de: Office of Govemment Commerce, 2007, p. 202.

1.2.3.1 Mesa de Servicios Virtual

Apoyándose en el uso de la tecnología y las herramientas y soluciones de soporte construidas para las corporaciones y empresas, es posible que éstas logren dar la impresión de poseer un *service desk* centralizado cuando de hecho, el personal esté disperso o localizado en diferentes ubicaciones geográficas y/o estructurales. Valiéndose de metodologías y procedimientos como el "*Trabajo en Casa"*, grupos de soporte secundarios e incluso outsourcing. Para un *service desk* que obedezca a esta estructura es importante tener en

cuenta los aspectos que aseguren la consistencia y uniformidad en la calidad del servicio y los términos culturales (Office of Government Commerce, 2007, p. 203).

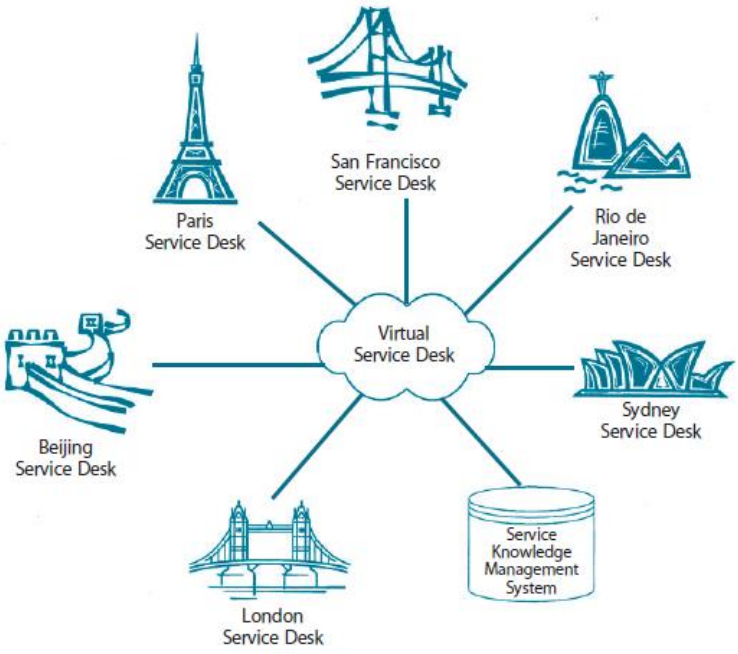


Figura 6. Mesa de Servicios Virtual

Tomado de: Office of Govemment Commerce, 2007, p. 203.

1.3 Computación en la nube (*CLOUD*)

En pocas palabras, la computación en la nube es la entrega de servicios informáticos: servidores, almacenamiento, bases de datos, redes, software, análisis y más, a través de Internet ("la nube"). Las empresas que ofrecen estos servicios informáticos se denominan proveedores de servicios en la nube y, por lo general, cobran por los servicios de computación en la nube en función del uso, de forma similar a cómo se le factura el agua o la electricidad en el hogar (Microsoft Azure, s.f.).

1.3.1 Usos de la computación en la nube

Los primeros servicios de computación en la nube tienen apenas una década, pero ya una variedad de organizaciones, desde pequeñas empresas emergentes hasta corporaciones globales, agencias gubernamentales y organizaciones sin

fines de lucro, están adoptando la tecnología por todo tipo de razones. Estas son algunas de las cosas que puedes hacer con la nube:

- Crea nuevas aplicaciones y servicios
- Almacenar, realizar copias de seguridad y recuperar datos
- Alojar sitios web y blogs
- Transmitir audio y video
- Entregar software bajo demanda
- Analiza datos para patrones y haz predicciones

1.3.2 Principales beneficios de la computación en la nube

La computación en la nube es un gran cambio respecto de la forma tradicional en que las empresas piensan sobre los recursos de TI. A continuación, se enumeran 6 razones comunes por las que las organizaciones recurren a los servicios de computación en la nube:

I. **Costo:** la computación en la nube elimina el gasto de capital de comprar hardware y software y configurar y ejecutar centros de datos en el sitio: los racks de servidores, la electricidad durante las 24 horas para la energía y la refrigeración, los expertos en TI para administrar la infraestructura. Se suma rápido.

II. **Velocidad:** la mayoría de los servicios de computación en nube cuentan con autoservicio y bajo demanda, por lo que incluso una gran cantidad de recursos informáticos se pueden aprovisionar en minutos, generalmente con solo unos pocos clics del mouse, brindando a las empresas mucha flexibilidad y eliminando la presión de la planificación de capacidad.

III. **Escala global:** los beneficios de los servicios de computación en la nube incluyen la capacidad de escalar elásticamente. En la nube, eso significa entregar la cantidad correcta de recursos de TI, por ejemplo, más o menos

potencia de computación, almacenamiento, ancho de banda, justo cuando sea necesario y desde la ubicación geográfica correcta.

IV. **Productividad:** los centros de datos en el sitio suelen requerir muchos "racks y apilamientos": instalación de hardware, parches de software y otras tareas de administración de TI que requieren mucho tiempo. La computación en la nube elimina la necesidad de muchas de estas tareas, por lo que los equipos de TI pueden dedicar tiempo a lograr objetivos comerciales más importantes.

V. **Rendimiento:** los mayores servicios de computación en la nube se ejecutan en una red mundial de centros de datos seguros, que se actualizan regularmente a la última generación de hardware informático rápido y eficiente. Esto ofrece varios beneficios sobre un solo centro de datos corporativo, incluida la latencia de red reducida para aplicaciones y mayores economías de escala.

VI. **Confiabilidad:** la computación en la nube hace que la copia de seguridad de datos, la recuperación ante desastres y la continuidad del negocio sean más fáciles y menos costosas, porque los datos pueden reflejarse en múltiples sitios redundantes en la red del proveedor de la nube.

1.3.3 Tipos de servicio en la nube

La mayoría de los servicios de computación en la nube se dividen en tres grandes categorías: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (Saas).

I. **Infraestructura como servicio (IaaS):**

La categoría más básica de servicios de computación en la nube. Con IaaS, alquila infraestructura de TI -servidores y máquinas virtuales (VM), almacenamiento, redes, sistemas operativos- de un proveedor de la nube en una base de pago por uso (Microsoft Azure, s.f.).

II. Plataforma como servicio (PaaS):

La plataforma como servicio (PaaS) se refiere a los servicios de computación en la nube que ofrecen un entorno bajo demanda para desarrollar, probar, entregar y administrar aplicaciones de software. PaaS está diseñado para facilitar a los desarrolladores la creación rápida de aplicaciones web o móviles, sin preocuparse por la configuración o administración de la infraestructura subyacente de servidores, almacenamiento, redes y bases de datos necesarias para el desarrollo (Microsoft Azure, s.f.).

III. Software como servicio (SaaS)

El software como servicio (SaaS) es un método para entregar aplicaciones de software a través de Internet, bajo demanda y generalmente por suscripción. Con SaaS, los proveedores de la nube alojan y gestionan la aplicación de software y la infraestructura subyacente, y se encargan de cualquier mantenimiento, como actualizaciones de software y parches de seguridad. Los usuarios se conectan a la aplicación a través de Internet, generalmente con un navegador web en su teléfono, tableta o PC (Microsoft Azure, s.f.).

1.4 Sistema de Respaldos

Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos el fin de disponer de un medio para recuperarlos en caso de su pérdida.

El objeto de casi todo el respaldo de la información consiste en crear una copia de los datos, con el fin de llegar a restaurar un archivo o aplicación específicos debido a un desastre o tras la pérdida de los datos. Por tal motivo, la copia de seguridad es el camino de cumplir el objetivo de proteger los datos. Un factor

muy importante es la comprobación de dichos *backups*. Permitir la restauración más delante de los datos respaldados es la utilidad en sí de realizar copias de seguridad. Para garantizar el objetivo de proteger los datos se deben comprobar los respaldos periódicamente (Fellows, 2008).

Existen varias operaciones que aseguran proteger los datos existentes en un sistema: el archivado y la copia de seguridad. El archivado es una copia de los datos primarios, que se guarda a largo plazo y tiene costos bajos ya que se lo realiza por lo general en cintas. Por otro lado, se tiene a la copia de seguridad que es una copia secundaria de datos, que por lo general es más costosa porque utiliza métodos de protección (Fellows, 2008).

1.4.1 Almacenamiento en la Nube

Los respaldos en la nube es una tendencia que en estos últimos años ha sido adoptada por diversas organizaciones y usuarios a nivel global puesto que permite la disponibilidad de la información en cualquier ubicación y momento. La elección de un proveedor que brinde estos servicios es una tarea que con lleva un grado de dificultad y de análisis previo, puesto que existen un gran número de marcas en el mercado (Oliveros, 2007).

Consejos notables que considerar para implementar respaldos en la nube:

- No se debe entregar toda la confianza a la disponibilidad de los servicios en la nube.
- La información se encuentra en servidores de terceros, al final no se sabe quién tiene control sobre los datos.
- Este servicio debe ser un método adicional a la forma de respaldar información.
- Siempre debe existir un cifrado de datos por seguridad.

1.4.1.1 Nube Pública

Las nubes públicas son el modelo más general de efectuar la informática en la nube. Los recursos de la nube (almacenamiento, servidores) son propiedad de otro proveedor de servicios en la nube, que los administra y ofrece a través de Internet. Microsoft Azure es considerado como un claro ejemplo de este tipo de nube (Microsoft Azure, s.f.).

El proveedor es el propietario y administrador de toda la infraestructura subyacente, software y hardware. Por medio de un navegador administra su cuenta y accede a los servicios. A menudo, las implementaciones de nube pública se emplean para entregar almacenamiento, correos electrónicos web, entornos de desarrollo y aplicaciones de office en línea (Microsoft Azure, s.f.).

Los puntos importantes que contiene este almacenamiento público son:

- Precios menores.
- No requiere de un mantenimiento contante.
- Garantiza que no exista inconvenientes en los servidores

1.4.1.2 Nube Privada

Esta herramienta es de uso exclusivo para una compañía la nube privada utilizara servicios externos alojándose en un distribuidor las empresas que utilicen esta herramienta pueden ser las instituciones financieras donde se realiza operaciones esenciales para la compañía es importante que la empresa cambie su organización dependiendo a carencias del departamento de tecnología de información. Las empresas pueden tener varias organizaciones estas dependerán de su infraestructura pueden ser medias o grandes (Microsoft Azure, s.f.).

Las ventajas que ofrece esta herramienta son:

- Flexibilidad complementando las necesidades de cada empresa.
- Seguridad los recursos son individuales controlando así la seguridad de la empresa a la que se está prestando el servicio.
- Escalabilidad

1.4.1.3 Nube Híbrida

Es la combinación de las dos infraestructuras tanto la pública como la privada, este beneficio toma como resultado la utilidad de los dos recursos denominándolo “lo mejor de ambos mundos” (Microsoft Azure, s.f.).

Los datos y las aplicaciones tanto de las privadas como de las públicas pueden moverse entre las dos nubes. La nube hibrida brinda servicios como: el ser segura, flexible y posee confidencialidad para la empresa, esto ayuda a los informes financieros cubriendo de una manera amplia las necesidades que requerirá una empresa. Emplea los recursos informáticos para satisfacer las necesidades del personal de la empresa esto se puede ver evidenciado en el correo electrónico web (Microsoft Azure, s.f.).

Entrega las siguientes ventajas:

- Existe confidencialidad en su infraestructura.
- Utiliza procesos adicionales dependiendo la necesidad de la empresa.
- Se paga el servicio que se utilizó esto genera que tenga mayor rentabilidad.
- Cambia cargas gradualmente

La elección del tipo de nube que se desee usar depende de las necesidades que disponga cada empresa.

1.4.2 Tipos de respaldos de datos

1.4.2.1 Copia de seguridad completa

Ante cualquier proceso de respaldo de la información siempre se comienza con una copia de seguridad completa. Todos los archivos y carpetas se copiarán en su totalidad. Si se trabaja con este tipo de copia las siguientes veces que se realizará un respaldo se copiará nuevamente todo (Kyocera, 2017).

Generalmente las copias de seguridad completas son usadas en el respaldo inicial, para que los respaldos siguientes se utilicen métodos como copias incrementales o diferenciales. Las copias completas pueden ser programadas a realizarse cada cierto tiempo en combinación con las copias incrementales que son más seguidas (Kyocera, 2017).

Una copia de seguridad online completa tomará mucho tiempo, dependiendo de la cantidad de archivos que tengas. A veces, puede tardar incluso varias semanas hasta que todos los archivos se copian. Es por eso que es importante no confiar solo en la copia de seguridad online, sino tener también con una copia de seguridad local de todos los archivos (Kyocera, 2017).

Ventajas de copias de seguridad completas:

- Restauración más fácil al tener todos los datos disponibles.
- Los datos se respaldan en un solo bloque de copia de seguridad.
- Se tiene un control más cómodo de las versiones.

Desventajas de copias de seguridad completas:

- Espacio de almacenamiento considerablemente grande.
- La red debe manejar anchos de banda muy grandes.
- Es muy demorada, no se debe trabajar con este tipo de copia diariamente.

1.4.2.2 Copia Incremental (copia incremental diferencial)

Es la técnica de mayor uso para copias de seguridad en línea por su eficiencia transfiriendo archivos en internet (Kyocera, 2017).

La copia incremental copiará todo archivo que haya sido modificado desde la última copia de seguridad, sin tomar en cuenta si esta fue incremental o completa. El objetivo principal de esta técnica es disminuir el tiempo entre copias de seguridad, requiriendo menos datos para realizar las copias (Kyocera, 2017).

Ventajas de las copias de seguridad incrementales:

- Copias de seguridad más rápidas, al tratarse de menos datos.
- Menor espacio de almacenamiento.
- Se puede disponer de versiones.
- Menos ancho de banda.

Desventajas de copias de seguridad incrementales:

- Se demora más en la restauración.
- Siempre se va a necesitar una copia de seguridad completa previa.
- Para realizar las recuperaciones se van a necesitar todas las copias de seguridad incrementales y la copia de seguridad inicial completa.
- Más tiempo es restaurar un archivo específico.
- No debe fallar la recuperación de la copia inicial completa.

1.4.2.3 Copia de Seguridad Diferencial (copia incremental acumulativa)

A diferencia de la incremental después del tercer respaldo, se vuelve a realizar una copia completa (Kyocera, 2017). Se puede decir que las copias de seguridad diferenciales son copias de seguridad incremental de una forma acumulativa. Las ventajas de las copias de seguridad diferenciales:

- Menos espacio de almacenamiento.
- Para restaurar la información solo se necesita la primera copia completa y la última copia diferencial.
- Varias versiones.

Desventajas de copias de seguridad diferenciales:

- En comparación con la incremental es más lenta.
- Necesita más espacio de almacenamiento que la incremental.
- Siempre se necesita una copia inicial completa.
- Restauración más lenta que la incremental.

1.4.3 Riesgos que corren los Datos

Los riesgos que corren los datos pueden ser por diferentes tipos de interrupciones como pueden ser: averías en la red, problemas eléctricos, fallos de hardware o software, errores humanos, incendios, inundaciones, entre otros. Que a pesar de que no las empresas no pueden evitar esto si pueden estar preparados ante cualquier incidente. A continuación, se encuentran los riesgos a los cuales se encuentran inmersos los sistemas de Información

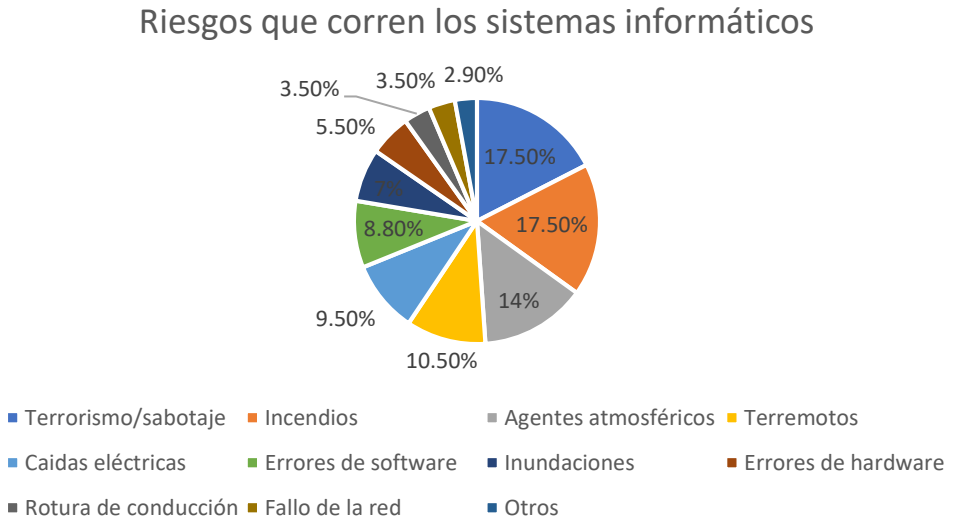


Figura 7. Riesgos que corren los datos.

Adaptado de: IBM, 2017.

1.4.4 Metodología de Respaldos

Para la elaboración de la política de respaldos se consideraron los siguientes marcos de referencia.

1.4.4.1 COBIT® 4.0

El IT Governance Institute fue el encargado del diseño y la elaboración de COBIT® 4.1, en primera instancia como un recurso educacional enfocado a directores ejecutivos de información, para la dirección general, y para los profesionales de administración y control de TI (IT Governance Institute, 2007).

COBIT es un marco que trabaja perfectamente con COSO e ISO17799, también tiene la característica de incorporar aspectos fundamentales de otros estándares relacionados, en su marco de trabajo emplea dominios y procesos, así también con estructura manejable y lógica presenta las actividades.

En su estructura cuenta con 34 procesos genéricos, cada uno es abarcado en cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) con esto se obtiene un campo general de control, gestión y medición de procesos.

Referente a los respaldos de la información, el marco lo menciona en el proceso **DS11.5 Respaldo y restauración**, el mismo que dice lo siguiente:

> “Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad” (IT Governance Institute, 2007).

2. Capítulo II. Análisis de la situación actual de la Mesa de Ayuda y del Sistema de Respaldo de Información en la empresa.

En este capítulo se analizará a detalle la situación actual de cómo se está manejando la mesa de ayuda en la empresa, con respecto a qué se hace referente con las solicitudes de usuarios, eventos, incidentes, cómo se trata los problemas, gestiones de acceso, cuál es la estructura y qué procesos son llevados a cabo por la mesa de ayuda.

Se realizará un caso de uso de cómo se manejan estos servicios en la actualidad, se listará los servicios que prestan el área de TI, los proveedores de tecnología con los que trabajada la empresa, se estudiará los principales incidentes para catalogarlos como problemas, se listará los equipos de tecnología empleados en el área de TI, se verificarán que sistemas de alarmas se cuentan para notificación de eventos en los sistemas, se realizará encuestas a los usuarios para medir el nivel de satisfacción que tienen con respecto a la mesa de ayuda, por último de acuerdo a lo analizado se planteará los problemas encontrados y cómo se mejorarán dichos servicios.

Por otro lado, referente al sistema de respaldos se analizará cómo se están realizando los *backups* actualmente, que datos son considerados críticos, cómo se maneja la información de los servidores, aplicaciones y usuarios, con qué frecuencia se realiza los *backups*, se estudiará si existe un plan de contingencia para la restauración de la información en casos de pérdidas de datos, por último, se planteará los problemas presentados actualmente y cómo se va a mejorar dichos servicios.

2.1. Situación actual Mesa de ayuda

2.1.1. Esquema de atención actual

El Área de Mesa de Ayuda se encuentra formada por el gerente de sistemas y por un grupo de técnicos especializados en diferentes áreas de TI, de los mismos tres personas tienen conocimiento especializado de la herramienta ERP y su respectivo soporte, y tres personas son responsable de infraestructura y de soporte al usuario en temas varios.

La atención hacia los colaboradores internos se lleva a cabo a través de la recepción de solicitudes vía telefónica, por correo electrónico, o de forma directa. La solicitud o incidente receptado es designado a un técnico de acuerdo con su tipo:

- ERP
- Infraestructura, servidores y redes
- Soportes varios a usuario
- Impresoras

Una vez asignado el personal encargado a cada tipo de solicitud o incidente este procede a atender el mismo ya sea de forma local con el usuario o de forma remota por medio de una herramienta que permita esto como; Skype Empresarial o TeamViewer, en la cual el técnico toma control remoto de la máquina del usuario que levantó el caso para poder solucionar este.

Sí llega a la solución este continua con el registro en un documento compartido con todo el grupo de la mesa de ayuda, donde los datos a guardarse son; usuario solicitante, fecha, incidente, solicitud a resolver, procedimiento realizado para la solución y fecha de solución. Por otro lado, si no es resuelto, el caso es escalado a un proveedor externo. Este proceso detallado se puede observar en la figura 8 más a continuación.

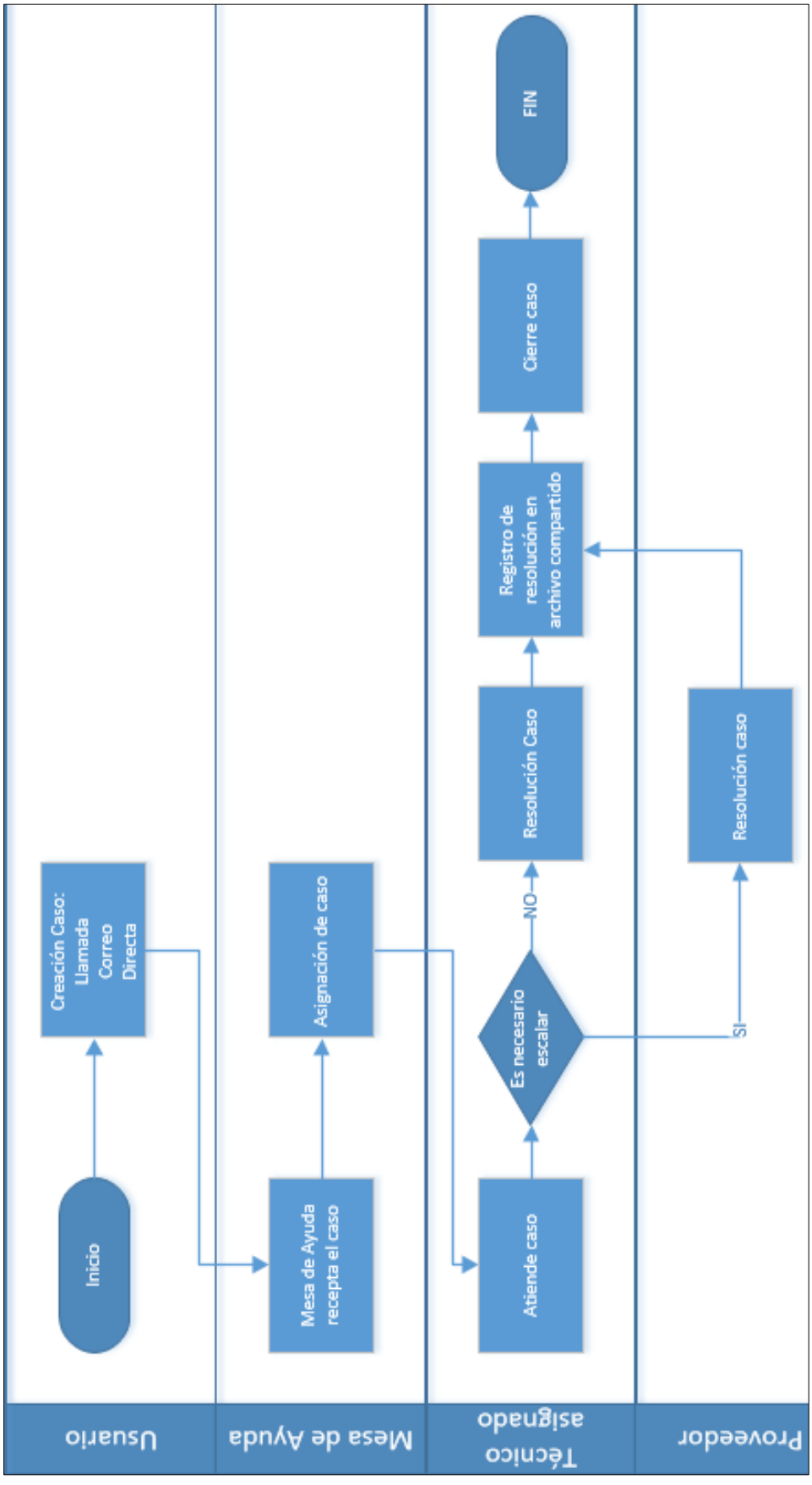


Figura 8. Diagrama de flujo atención al usuario por parte de la mesa de ayuda.

2.1.2. Servicios de TI en la empresa.

Gracias al crecimiento que ha tenido la empresa en los últimos años se ha visto un amplio interés e inversión en disponer de servicios de TI a la vanguardia para sus colaboradores. Los servicios de TI prestados actualmente son los siguientes:

- ✓ Microsoft Dynamics GP 2016 como ERP de la empresa (*Enterprise Resource Planning)* que significa “sistema de planificación de recursos empresariales”. El cual se encarga de operaciones internas de la empresa, las mismas que son: ventas, inventario, compras, contabilidad, proveedores, cuentas por pagar, clientes, cuentas por cobrar, activos fijos.

- ✓ Microsoft Office 365, todos los usuarios de la empresa cuentan con licencias para este servicio, con el cual se brinda correo electrónico en la nube por medio Exchange Online, almacenamiento en la nube con OneDrive y la gama completa de ofimática en las computadoras personales.

- ✓ Servicio de VoIP a través de una central telefónica Elastix ubicada en el Centro de Datos de la empresa en la matriz Quito, y tres centrales telefónicas Grandstream ubicadas en cada sucursal de la empresa; Guayaquil, Cuenca, Lima.

- ✓ Servicio de videollamadas entre sucursales a través de POLYCOM, el mismo que es un sistema interactivo que trabaja sobre LAN.

- ✓ Servicio de impresión con equipos XEROX en un esquema outsourcing.

- ✓ Gama Cisco Meraki donde se brindan los servicios de:
    - Conectividad tanto a nivel LAN como WAN por medio de Firewalls, Switchs y Puntos de Acceso inalámbrico.
    - Seguridad por medio de cámaras de videovigilancia IP.
    - Conectividad a la red por medio de VPN.

- ✓ Servicio de control asistencia por medio de equipos de marca ZKTeco y de su software de gestión ZKAccess 3.5 y ZKTimeNet 3.0

- ✓ Servicios de antivirus tanto a nivel de usuarios como a nivel de servidores por medio de ESET.

2.1.3. Proveedores de TI de la empresa.

De acuerdo con lo mencionado en la sección anterior se dispone de diversos proveedores para el manejo de los servicios de TI prestados en la empresa, a continuación, en la Tabla 1 se puede observar una lista de estos.

Tabla 1.

Proveedores de servicios de TI de la empresa.

Nombre del proveedor	Servicio
AltioraCorp.	Microsoft Dynamics GP 2016
Binaria Sistemas	Microsoft Office 365
Binaria Sistemas	Servicio de impresión
ABPRO7.0	Sistema POLYCOM
Infolink	Centrales Telefónicas
Comware S.A.	Soluciones Meraki
Soluciones Integrales Megacore	Biométricos
ESET	Antivirus
Cloud360	Máquinas virtuales en la nube

2.1.4. Peticiones de servicio frecuentes.

En el análisis realizado en la empresa se ha detectado solicitudes de servicio frecuentes por parte de los usuarios, las mismas que en la actualidad no se encuentran catalogadas de forma correcta, ni se tiene un esquema a seguir para el personal de TI de la mesa de ayuda. A continuación, en la Tabla 2 se observa las peticiones de servicios frecuentes del ERP.

Tabla 2.

Peticiones de servicios frecuentes del ERP.

SOLICITUD	ACCIONES QUE REALIZAR	ACTOR
Reportes	Formateo de la data e inserción	Área Comercial, Contabilidad, Logística
Aplicativos nuevos	Desarrollo y acoplamiento de aplicativo nuevo con GP	Área de Asuntos Regulatorios
Creación de nuevo usuario en GP	Se crea usuario y clave para la herramienta	Usuario con autorización de su línea de supervisión
Dar privilegios de acceso a un usuario	Se da permisos a módulos nuevos del GP	Usuario sin ninguna aprobación de su línea de supervisión
Mantenimiento y actualización de base de datos	Reindexación, reducción de BD, revisión de logs, depuración de usuarios que acceden a la BD	Gerente de Sistemas
Levantar ambiente paralelo de GP para pruebas	Traslado de la data actual a un sistema nuevo de configuración de GP con data clonada	Área de contabilidad

Tabla 3.

Peticiones de servicio frecuente de infraestructura.

SOLICITUD	ACCIONES QUE REALIZAR	ACTOR
Creación de usuario nuevo para la empresa	Se crea usuario nuevo en AD, se asigna licencia de Office365	Talento Humano
Asignación de recursos físicos a nuevo usuario	Se configura computador a nuevo usuario	Talento Humano
Creación de pin para imprimir	En sistema de gestión de las impresoras se establece nuevo pin	Talento Humano
Creación de extensión telefónica nueva	En la central se crea la nueva extensión para el usuario	Talento Humano
Registro de usuarios nuevo en el biométrico	Se registra huellas y tarjeta de acceso en biométricos	Talento Humano
Creación de buzones compartidos	Se crea buzón compartido entre usuarios solicitantes	Área que requiera

SOLICITUD	ACCIONES QUE REALIZAR	ACTOR
Creación de pst	Se realiza un archivo pst del buzón requerido	Usuario que requiera
Creación de carpetas compartidas	Se crea la carpeta compartida en el servidor de archivos	Usuario que requiera
Reporte de asistencia del biométrico	Se saca un reporte de la herramienta ZKAccess 3.5	Talento Humano
Acceso a la red de la empresa fuera de la oficina	Se configura VPN en máquina del usuario	Usuario que requiere
Instalación de algún software nuevo	Se instala el software en máquina del usuario	Usuario que requiere
Configuración de correo en teléfono móvil	Se configura correo en aplicativo del celular	Talento Humano
Reporte de antivirus	Se saca un reporte del análisis de ESET	Gerente Sistemas
Mantenimiento de computadoras	Se realiza un mantenimiento preventivo periódico a nivel de SW y HW a las computadoras de usuarios.	Gerente Sistemas
Mantenimiento de servidores	Se realiza un mantenimiento preventivo periódico a nivel de SW y HW a los servidores.	Gerente Sistemas

2.1.5. Incidentes frecuentes.

Con respecto a los incidentes estos son variados, pero de igual forma se pudo observar los incidentes de mayor ocurrencia y su clasificación de acuerdo con sí son del ERP o de infraestructura, estos dos tipos de clasificación son los que más ocurren en la empresa por lo cual se ha considera dividirlos así.

Esto se puede observar en la tabla 4 y tabla 5 a continuación, en donde se encuentran los incidentes clasificados por: ERP o infraestructura.

Tabla 4. Incidentes con mayor ocurrencia de Infraestructura.

INCIDENTE	ACCIONES QUE REALIZAR
No llegan correos al Outlook	Se verifica conexión a internet, se verifica cambios de clave recientes
Outlook no se abre	Se finaliza tareas, se abre en modo de pruebas, se corren actualizaciones
No se conecta a wifi	Se verifica configuraciones del sistema RADIUS
No llega la impresión	Se verifica conexión hacia el servidor de impresiones, se verifican GPO de impresión
No se abre NITRO PDF	Se finaliza tarea de NITRO PDF corrompidas
No se abre sistema ECUAPASS	Se verifica actualizaciones de JAVA y actualizaciones de los navegadores
No se abre sistema USHAY	Se verifica actualizaciones del aplicativo
Falla de algún controlador	Se corre herramienta de actualización de controladores
Teléfono de VoIP no realiza llamadas	Se verifica conexiones físicas del teléfono, se verifica configuraciones de la extensión del usuario
Lentitud en programas de Office	Se actualizan programas, se analiza el tipo de archivos que presentan problemas
No se conecta a la VPN	Se verifica configuraciones de autenticación RADIUS, se verifica configuraciones en Firewall
Se pierde señal en llamadas de POLYCOM	Se verifica enlaces de red hacia las sucursales
No se conecta a SKYPE Empresarial	Se actualiza SKYPE, se verifica cambios de contraseñas
Se desconectan las impresoras a color	Se verifica conexiones IP hacia la impresa de red a color
No llegan correos al celular	Se verifica cambios de contraseñas recientes
Documentos encolados en la impresora	Se eliminar en la cola de impresión del servidor documentos que estén ocasionando problemas.

Tabla 5.

Incidentes con mayor ocurrencia del ERP.

INCIDENTE	ACCIONES QUE REALIZAR
No se puede ingresar al GP	Se verifican conexiones, cambios de claves
Sesión de GP bloqueada	Se bota al usuario del aplicativo
Se cortan contabilizaciones	Se realiza los scripts correspondientes en la base de datos
Se pasman documentos de ventas, pagos, recepciones	Se revisa las tablas correspondientes en la basa de datos
Lentitud en servidor de aplicativo de GP	Se revisa enlaces, transacciones que se estén realizando

2.1.6. Problemas frecuentes.

Como se pronunció en el capítulo 1 un problema es la ocurrencia repetitiva de incidentes, por tal motivo de todos los incidentes analizados que ocurren diariamente en la empresa, se observó algunos que deben considerarse como problemas, pero que actualmente no tienen dicho trato, ya que no se llegue al origen de la raíz de dichos incidentes y estos se repiten continuamente. En la tabla 6 a continuación se establecen dichos problemas.

Tabla 6.

Problemas descubiertos actualmente.

PROBLEMA	DESCRIPCIÓN
Lentitud en programas de Office	Incidente frecuente, a pesar de disponer de máquinas de buenas prestaciones procesadores Intel Core I5 o superiores, RAM de 8 GB o superior. El proceso de actualizar el sistema de Office no resuelve este incidente. Este llega a convertirse en un problema del cual actualmente no se llega a una solución definitiva.

PROBLEMA	DESCRIPCIÓN
Se pierde señal en llamadas de POLYCOM	Incidente frecuente, las acciones realizadas son; revisión de conexiones, enlaces, configuraciones. Dichas acciones no resuelven el incidente.
Lentitud en servidor de aplicativo de GP	Los usuarios se quejan constantemente de la lentitud del aplicativo GP, esto se intenta resolver revisando uso actual de CPU del servidor, corriendo scripts para depurar la base de datos, revisando enlaces hacia el aplicativo, pero no se llega a una solución definitiva para el mismo.

2.1.7. Eventos registrados.

En el esquema actual de la mesa de ayuda no se tiene un manejo de eventos establecido, se cuenta con herramientas de análisis de sistemas tales como:

- ✓ PRTG NETWORK MONITOR, con el cual obtiene notificaciones de eventos ocurridos con el estado actual de los servidores y de los enlaces de datos.

- ✓ Sistema de Gestión Meraki, con el cual, a parte de las configuraciones de los equipos de red, también entrega notificaciones de alerta de los equipos, tanto de firewalls, puntos de acceso, cámaras.

- ✓ Un procedimiento almacenado que cuando ocurre un fallo en el respaldo de las bases de datos notifica vía correo al administrador de la base de datos, lo que hace este procedimiento almacenado es analizar el estado final del respaldo en SQL Server verificando si hubo falla o se finalizó correctamente.

- ✓ Sistema de notificaciones del sistema de impresión por medio del software YSOFT de Binaria Sistemas, en este se notifican cuando está por acabarse un tóner, o un consumible está por acabarse.

Sin embargo, a pesar de disponer de estos programas de control y notificación de eventos, no se tiene un proceso a seguir cuando ocurren los mismos, no se tiene una designación establecida del personal de TI para su resolución. Como se menciona en ITIL v3 se debería crear un esquema de eventos, con lo cual se facilita la tarea de seguimientos de estos eventos. Todos estos cambios serán considerados en el Capítulo 3.

2.1.8. Resultado análisis Mesa de Ayuda Actual.

Como se puede notar en el esquema actual hay algunos problemas detectados en la forma de atención al cliente:

- No existe un medio de creación de casos para los usuarios que sea interactivo entre el personal de TI de la mesa de ayuda y los usuarios en sí. La forma actual de creación de casos es poco eficiente al realizarla por medio de llamadas telefónica, correo electrónico o de forma directa.

- No existen reglas de enrutamiento de los registros de eventos hacia técnicos responsables de acuerdo con categorías.

- No existe una base de datos de conocimiento óptima para una consulta de soluciones posibles, puesto que esto actualmente se maneja de manera muy general en un archivo de Excel.

- El usuario no tiene un seguimiento de su caso, y la forma de interactuar con el usuario acerca de un caso es a través de correo electrónico, forma poco eficiente puesto que los técnicos al tener gran cantidad de correos se les hace casi imposible dar seguimiento a uno específicamente.

- No hay una encuesta al cierre del caso para establecer el grado de satisfacción del usuario una vez resuelto su inconveniente o solicitud.
- No existe manejo de problemas.
- No se tiene definido un catálogo de servicios de TI, donde los usuarios de manera pública estén al tanto de a qué servicios tienen acceso.
- No se tiene definido acuerdos de nivel de servicios.
- No se tiene definido tiempos de respuestas a incidentes, problemas que debe cumplir la mesa de servicios en atenderlos.
- No se tiene establecido modelos de incidentes, problemas.
- No existen métricas de medición del trabajo realizado por el personal de la mesa de servicios.
- No existe configurado un correcto escalamiento de los casos
- No se tiene un medio para obtener reportes del trabajo de la mesa de ayuda.
- No se tiene un control de inventario de los servidores y computadoras de usuario final.
- No se dispone de un sistema para anunciar eventos a los usuarios.

2.1.9. Análisis comparativo con ITIL.

De acuerdo con el análisis realizado se puede realizar un análisis comparativo respecto a ITIL v3, donde el objetivo es establecer en qué grado se cumple las prácticas recomendadas por este marco referencial, y qué falta mejorar e implementar en dicha mesa de ayuda. Esta comparación se puede observar en la tabla 7.

Tabla 7.

Análisis comparativo de ITIL v3 con mesa de ayuda actual de la empresa.

	Elementos	Empresa		Observación
		SI	NO	
ITIL V3	**Estructura Organizacional ITIL**	X		Falta de madurez en la organización
	Catálogo de servicios		X	Los usuarios no conocen que servicios ofrece TI
	Acuerdos de nivel de servicio (SLA)		X	No están definidos tiempos de respuesta
	Acuerdos de nivel de operación (OLA)		X	No está definido
	SLR		X	No está definido
	Gestión de Incidentes	X		Se maneja de forma poco eficiente
	Gestión de Peticiones de servicios	X		Se manejan de forma poco eficiente
	Gestión de Problemas		X	No está definido
	Gestión de Accesos		X	No está definido
	Gestión de eventos		X	No está definido

2.2. Situación actual del Sistema de Respaldos

Es importante conocer una descripción general del giro del negocio de la empresa. La empresa ecuatoriana se dedica a la importación de equipos e insumos médicos de diferentes proveedores a nivel mundial, para su posterior venta y distribución de la mercadería en hospitales, clínicas y laboratorios clínicos del Ecuador y Perú. Debido al negocio de la empresa maneja información crítica de diferentes ámbitos como:

- Área Financiera: se maneja información de traspasos, diarios, transacciones presupuestarias, transacciones bancarias, lotes, depósitos bancarios, activos fijos, entre otros.

- Área de Ventas: se maneja información de clientes, prospectos, vendedores, transacciones de cuentas por cobrar, transacciones de pedidos de venta, transacciones de facturación.

- Área de Compras: se maneja información de proveedores, transacciones de compras, transacciones de cuentas por pagar, entre otros.

- Área de Comercio Exterior: se maneja información de proveedores, artículos, transacciones de artículos, entre otros.

La información mencionada en su totalidad es manejada por el sistema ERP (Microsoft Dynamics GP) de la empresa. Por tal motivo, todos estos datos son gestionados en distintas bases de datos de la herramienta Microsoft SQL Server. Adicional se maneja información de otras áreas que, a pesar de no intervenir de forma directa con el ERP, también cuentan con información valiosa en los servidores como lo son las Áreas de Tecnología de la Información, Talento Humano y Servicio Técnico:

De lo escrito se puede aclarar que dicha información no es solo manejada por los sistemas informáticos, sino que también la manejan de forma individual los usuarios en sus computadoras personales. Por tal motivo, se puede diferenciar tres tipos de información a respaldar:

- Información de servidores.

- Información de bases de datos.

- Información de usuarios.

En el análisis efectuado se determinó que solo se están realizando respaldos de la información de bases de datos y usuarios, dejándose de lado la información de servidores que manejan datos vitales para la empresa.

2.2.1. Proceso de Respaldos de Información de Usuarios

Los respaldos son obtenidos solo cuando se va a renovar de computador al colaborador, se realiza un copiado de su información a un disco duro externo, a continuación, dicha información es copiada en el nuevo computador asignado, una vez finalizado el traspaso de información los datos son copiados del disco duro externo hacia discos duros rígidos que se los tiene almacenados en el Área de Sistemas. En estos discos duros rígidos, se coloca una etiqueta la cual lleva el nombre de los usuarios de los que se tiene información, fecha del respaldo y el responsable del personal de TI que lo realizó. En la figura 8 a continuación, se puede observar una foto de los discos rígidos mencionados.

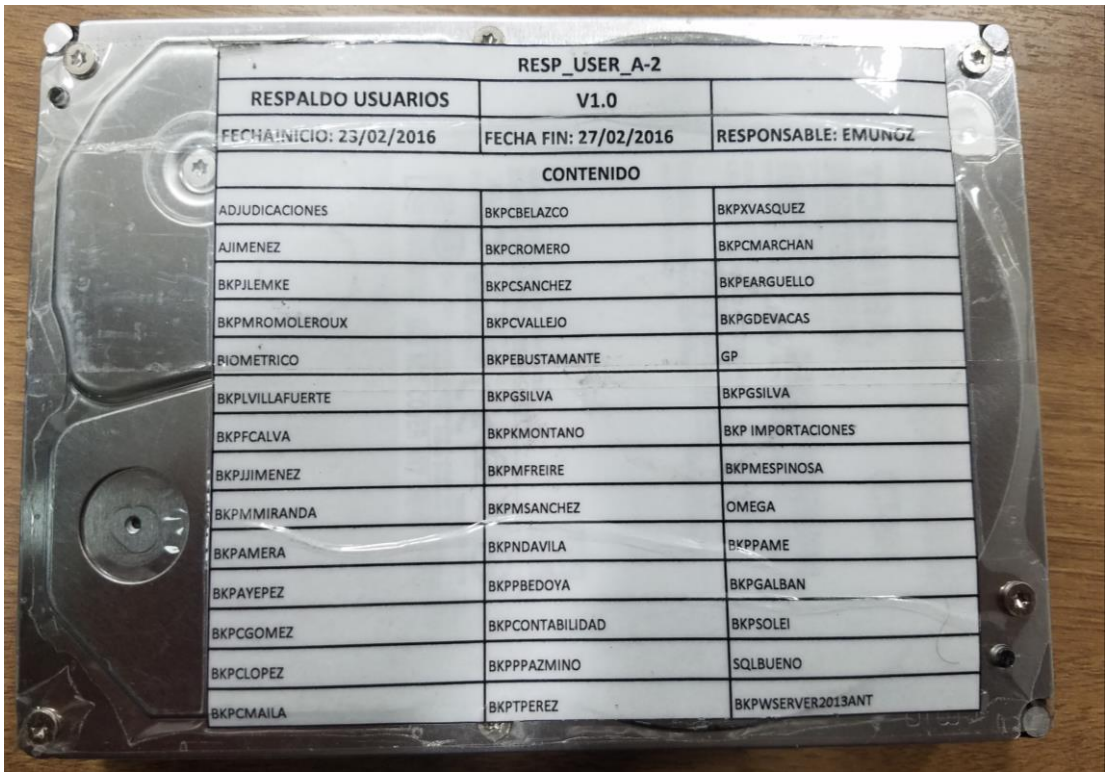


Figura 9. Discos duros rígidos con información de usuarios.

En la figura 10 a continuación se representa el proceso descrito de cómo se respalda actualmente la información de los usuarios.

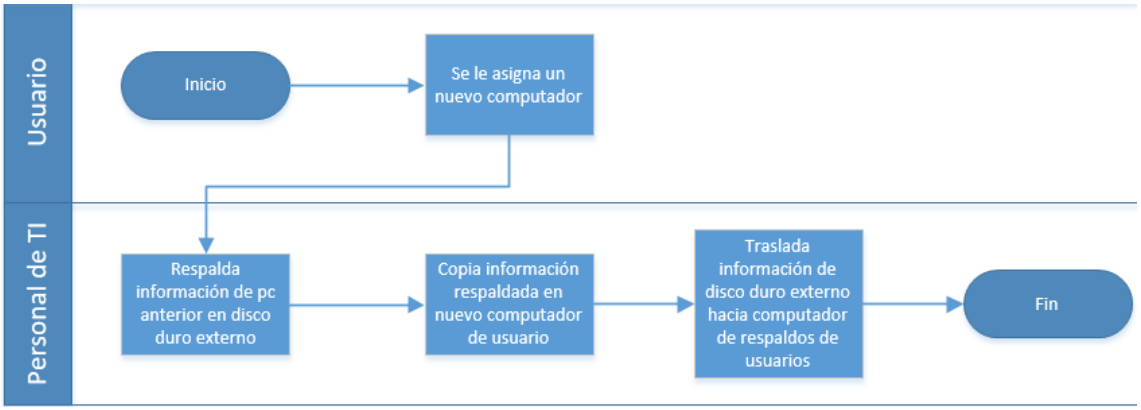


Figura 10. Flujo respaldo de información de usuarios.

Es claro que en este proceso no hay una política ni un sistema definido para respaldar la información a seguirse, como, por ejemplo:

- No se tiene definida cual es la información crítica de cada usuario que debería respaldarse

- No se tiene definida una frecuencia de cada cuanto respaldar la información de los usuarios, sino que este proceso se da cada que se va a renovar una computadora al usuario.

- El proceso de respaldar la información de cada usuario es poco eficiente, tiene extensos tiempos de realización, puesto que se debe realizar una triple copia de datos; una hacia el disco externo en primera instancia, después hacia el computador nuevo asignado al usuario y finalmente hacia el computador donde se almacenan los respaldos de usuarios.

- No se tiene redundancia de los respaldos puesto que estos solo se encuentran resguardados en la computadora de cada usuario y en el computador de respaldos de la empresa, ante uno de todos los tipos de riesgos que corren los datos mencionados anteriormente, estos se encuentran desprotegidos ya que solo se tiene una copia local.

- El acceso a los respaldos de cada usuario solo lo tiene el área de TI de la empresa.

2.2.2. Respaldo de Información de base de datos

En esta sección se dará a conocer cuál es la Política de respaldos que maneja actualmente la empresa en cuanto a las bases de datos y cómo se lleva a cabo la misma.

2.2.2.1 Política actual de respaldos de bases de datos de la empresa

a) Todas las bases de datos deberán de contar con la documentación de respaldo y recuperación. La misma que será controlada por el jefe de TI, para verificar que esté clara y completa, se deberá verificar:

    1) El reemplazo de base de datos y/o la implementación de la base en casos emergentes en otros servidores físicos.
    2) La versión del motor de BD y el sistema operativo.
    3) Ubicación de los respaldos.
    4) Horario de ejecución y copia del respaldo.

b) Todos los respaldos deberán de estar claramente identificados, con etiquetas que indiquen como mínimo:

    1) Nombre de la base de datos.
    2) Fecha del respaldo.
    3) Deberá de estar comprimido.

c) Se realizará una revisión periódica de los respaldos:

    1) Fecha del respaldo.
    2) Tamaño del respaldo.
    3) Pruebas de efectividad del respaldo.

d) Los sitios donde se almacenan los respaldos deberán de ser seguros y fuera del ambiente de servidores, puesto que si se encuentra en el mismo lugar ante un evento también se perderá el respaldo.

e) Se realizarán respaldos completos y copias hacia la ubicación segura de los mismos.

f) Los respaldos serán diarios, previendo la conservación de estos respaldos por un periodo de tiempo estipulado.

g) Se efectuarán pruebas de recuperación de las copias de respaldo por parte del administrador de base de datos al menos cada 30 días y serán supervisadas por el jefe de sistemas.

   Estas pruebas servirán para constatar que se puedan obtener de forma correcta información para así garantizar su propósito.

h) Las pruebas se deberán de formalizar en un acta escrita y firmada por los responsables.

i) Los procedimientos de respaldo y copia serán automáticos.

2.2.2.2 Descripción de los pasos para cumplir política actual de respaldos

a) Programar la ejecución de los respaldos en el servidor de base de datos, el script que ejecutará los respaldos se halla programado para ejecutarse todos los días a las 2 am, estos respaldos serán almacenados de forma local en la dirección E:\respaldosTemBD.

b) La copia del respaldo realizado desde el servidor de base de datos hacia el servidor de respaldos, esta copia se llevará a cabo todos los días automática a las 3 am. El servidor destinado para los respaldos será ANUBIS, este proceso se lo realizará mediante el programa de copias de seguridad COBIAN.

c) En el servidor de base de datos se contará con respaldos de hasta dos días, por lo que se cuenta con una tarea programa que se encarga de realizar la limpieza de *backups* con el fin de no agotar el espacio en disco duro.

2.2.2.3 Procedimiento para copiar respaldos de base de datos hacia el servidor de respaldos.

El proceso para realizar el copiado de los respaldos de las bases de datos se lo puede definir en la ejecución de los siguientes pasos:

1. Se realiza los respaldos diarios a las 2 am de las bases de datos mediante un JOB ejecutado en Microsoft SQL Server Management Studio.

2. Dichos respaldos se guardan localmente el servidor de la base de datos llamado OSIRIS con IP: 192.58.1.19 en el directorio E:\respaldosTemBD.

3. Mediante el software *Cobian BackUp 11 Gravity,* se realiza la copia de los respaldos obtenidos por el Script hacia un servidor de respaldos de base de datos local. El nombre del servidor donde se almacenan las copias de los respaldos de BD se llama Anubis con IP: 172.16.0.2. En la figura 11 a continuación se puede observar la configuración de Cobian.

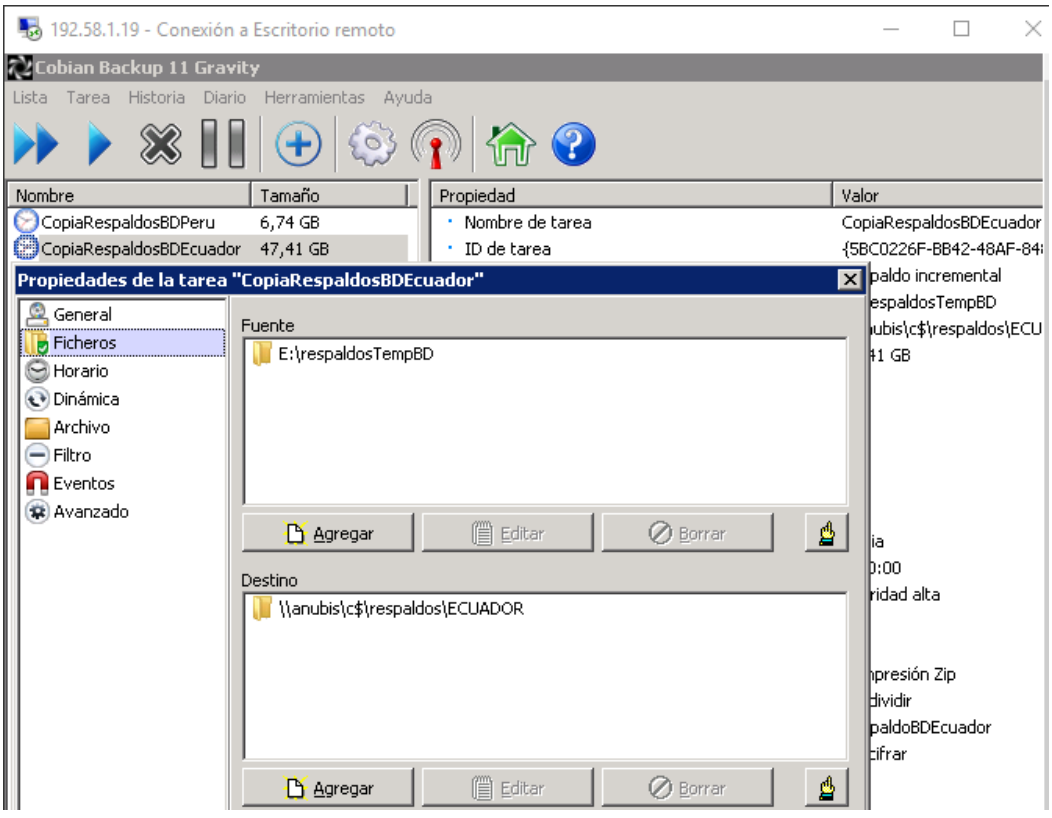


Figura 11. Copias de respaldos en Cobian.

2.2.2.4 Descripción de los servidores de la empresa

En tabla 8 a continuación se tiene una descripción de los servidores que dispone la empresa, en los datos se tiene; el sistema operativo, la aplicación que corre en cada uno, el nombre, si dispone o no de SQL y por último si es virtual o no.

Tabla 8.

Servidores de la empresa.

SISTEMA OPERATIVO	APLICACIÓN	NOMBRE	VIRTUAL
W. SERVER 2008 R2 ENTERPRISE X64	SAP BO - BUSINESS INTELIGENCE	HORUS	NO
W. SERVER 2012 R2 STANDARD X64	ACTIVE DIRECTORY	SMDSERVER	NO
W. SERVER 2008 R2 STANDARD X64 SP1	Servidor Correo Exchange 2010	MAILSERVER	NO
W. SERVER 2008 R2 STANDARD X64 SP1	Aplicativo GP 2010	TERSERVICE	NO
W. SERVER 2012 R2 DATACENTER	Biométricos y PRTG	THANATOS	NO
CENTOS 5	FIREWALL & Gateway Servidores	fw-simed.simed-ecuador.com	NO
W. SERVER DATACENTER 2007 X64 SP2	HyperV - SERVIDORES VIRTUALES	ORION	HYPER V

SISTEMA OPERATIVO	APLICACIÓN	NOMBRE	VIRTUAL
W. SERVER 2008 R2 STANDARD X64	SERVER ANTIVIRUS ESET	SRVRESET	SI
W. SERVER 2003 ENTERPRISE SP2	BASE DATOS GP ANTIGUO	SERVERHP	SI
W. SERVER 2008 R2 STANDARD X64	SIAP RECURSOS HUMANOS & Progress 360	ICARO	SI
W. SERVER 2008 R2 STANDARD X64 SP1	SQL Server para GP 2013 ECUADOR	OSIRIS	SI
W. SERVER 2008 R2 STANDARD X64 SP1	Aplicación GP 2013 PERU	OMEGA	SI
LINUX	SYMANTEC ANTISPAM	ARES	SI
W. SERVER 2008 R2 STANDARD X64	SERVER IMPRESIÓN Quito - BINARIA	SRVR_BINARIA	SI
W. SERVER 2008 R2 STANDARD X64	SERVER - OFFICE 365 (DirSynch)	SRVR_OFF365	SI
W. SERVER 2012 R2 STANDARD X64	FILE SERVER	SRVUIOFILE	NO
W. SERVER 2008 R2 STANDARD X64 SP1	SERVER IMPRESIÓN GYE - BINARIA	WIN-H6O7OS8845J	NO

Tabla 9.

Relación de servidores físicos y servidores virtuales.

Servidores Virtuales				Servidores Físicos
Hyper-V ORION 192.58.1.14	SERVER ANTIVIRUS ESET SRVRESET 192.58.1.116	Conexión con server de licencias en Internet del fabricante		SAP BO - BUSINESS INTELIGENCE Aplicativo GP 2013 Ecuador Perú HORUS 192.58.1.80
	BASE DATOS GP ANTIGUO Microsoft SERVERHP 192.58.1.10	Base de datos SQL Server con Aplicativo GP		ACTIVE DIRECTORY SMDSERVER 192.58.1.6
	SIAP RECURSOS HUMANOS & Progress 360 Siap: Desarrollo de terceros Progress 360: Desarrollo de terceros Applicación de Planificación: Desarrollo Interno ICARO 192.58.1.17	Progress - AD (Credenciales ISS vs AD) Consulta de campo Descripción por número de Cédula		Servidor Correo Exchange 2010 MAILSERVER 192.58.1.5
	SQL Server para GP 2013 ECUADOR Microsoft OSIRIS 192.58.1.19	Base de datos SQL Server con Aplicativo GP		Aplicactivo GP 2010 TERSERVICE 192.58.1.8
	Aplicación GP 2013 PERU Microsoft OMEGA 192.58.1.16	Base de datos SQL Server con Aplicativo GP		Biométricos y PRTG THANATOS 192.58.1.117
	SYMANTEC ANTISPAM Symantec ARES 192.58.1.22	Correo entrante hacia Antispam por regla de NAT de CentOS		FIREWALL & Gateway Servidores fw-simed 192.58.1.2
	SERVER IMPRESIÓN Quito - BINARIA Ysoft Binaria SRVR_BINARIA 192.58.1.23			Servicios Cloud

2.2.2.5 Resultado final del análisis al sistema actual de respaldos de la información.

De todo observado de acuerdo con el sistema actual de respaldos de servidores que se lleva en la empresa se puede notar muchas fallas, detalladas a continuación:

- Solo se respalda las bases de datos y no se le da importancia a respaldar los sistemas de la empresa, información de los servidores y configuraciones de estos.

- La política de respaldos de base de datos es muy general, no se tiene definido que información de las bases de datos son críticas, ni cuánto tiempo se demora es reestablecer los respaldos en escenarios de catástrofes o pérdida generalizada de la información.

- No se realizan comprobaciones de la integridad de los respaldos.

- No se realizan pruebas para determinar el tiempo en que se demorara restablecer dichos respaldos.

- Los respaldos solo son de forma local, todo se encuentra dentro del centro de datos. Por tal motivo, en un caso de catástrofe, no existe redundancia de dichos respaldos. Esto se debe solucionar con un tercer respaldo en la nube.

- No se dispone de una gestión centralizada de los respaldos como se podría manejar desde un servicio web en donde se dispone del detalle de cada uno de los respaldos, como lo es: tamaño, fecha, tipo, entre otros que a la hora de recuperar información son de vital importancia.

- No se cuenta con versiones de respaldos como se tendría en un respaldo basado en tecnología *cloud*.

3. Capítulo III. Diseño e implementación de la Mesa de Ayuda

El objetivo principal de este capítulo es diseñar un esquema de mesa de ayuda de acuerdo con los servicios de TI que brinda la empresa y en base a los lineamientos de las mejores prácticas planteadas por el marco de referencia ITIL v3, referente principalmente a la fase de operación del servicio.

Con la elaboración de este diseño se pretende mejorar, crear e implementar nuevos requisitos para la mesa de ayuda que se deben cumplir en base al análisis realizado de los puntos débiles, malas prácticas y manejos faltantes en el actual sistema de mesa de ayuda que brinda la empresa.

Después del diseño se realizará un análisis a diferentes proveedores en el mercado que brinden dicho servicio, en el mismo se compararan diferentes puntos como:

- Cuál es el que más se ajuste al esquema planteado.
- Una comparativa de precios entre proveedores de acuerdo con el presupuesto de la empresa.
- Tiempos de respuestas que brinden cada uno y valores agregados al servicio que estén dispuesto a otorgar.

De dicho análisis se seleccionará el más eficiente que cumpla los puntos planteados, se procederá a implementar el mismo, se configurará este siguiendo el esquema diseñado y por último se llevarán a cabo las pruebas de funcionamiento respectivo en donde se verificarán las metas propuestas.

3.1 Diseño de la Mesa de Servicios.

En el desarrollo de esta tesis se ha planteado un enfoque principalmente en la fase de operaciones del Servicio en todos sus procesos y funciones, pero para ITIL v3 todas sus fases tienen una relación directa y trabajan en conjunto, por lo cual para un correcto desarrollo de la mesa de servicios se debe previamente realizar un análisis y diseño de procesos que involucran otras fases del ciclo de vida del servicio, cabe mencionar que no es un análisis a profundidad de dichas fases, pero sí de una forma general que ayudan de gran manera al desarrollo de la mesa de servicios. Los procesos de otras fases que se analizarán son los siguientes:

1. Diseño del Servicio: en esta fase se analizará y diseñará los siguientes procesos específicamente:
    a) Gestión del Catálogo de Servicios
    b) Gestión de Nivel de Servicios

2. Transición del Servicio: en esta fase se analizará y diseñará los siguientes procesos específicamente:
    a) Gestión de Cambios
    b) Gestión de la Configuración

3.1.1. Diseño del Servicio

“Se ocupa del desarrollo y mantenimiento de un Catálogo de Servicios con los detalles, el estado, las interacciones y las dependencias, de todos los servicios actuales y de los que estén siendo preparados” (Programa Del Máster Dirección de Proyectos, 2017).

3.1.1.1 Gestión del Catálogo de Servicios de TI

Un catálogo de servicio se lo puede definir como un conjunto de descripciones de los servicios de TI que son ofrecidos a los clientes internos. El cliente debe estar en la posibilidad de consultar ese catálogo y entenderlo, por tal motivo en este catálogo no deben existir aspectos técnicos, debe estar escrito en un

lenguaje más coloquial con la finalidad que cualquier persona que leyera el catálogo de servicios pudiera entenderlo. (Máster Dirección de Proyectos, 2017).

Este es el punto de partida para el diseño de la mesa de servicios puesto que, para tratar temas como eventos, incidentes, problemas y accesos se debe conocer qué servicios de TI son los que se están brindando a los usuarios.

De acuerdo con el análisis de la situación actual de la mesa de ayuda que maneja la empresa y en referencia a los servicios de TI que se brindan a los usuarios, se encontraron los siguientes inconvenientes:

1. Existen diversos servicios de TI, pero los mismos son solo conocidos de forma técnica por el área de sistemas. No existe una publicación de dichos servicios en términos entendibles para los usuarios.
2. Faltan agregar más servicios de TI a este grupo, la clasificación es limitada.

De acuerdo con los problemas detectados, se ha planteado el siguiente Catálogo de Servicios visible en la Tabla 10, que posteriormente será publicado para el alcance y entendimiento por parte de los clientes internos de la empresa.

Tabla 10.

Catálogo de Servicios de TI.

SERVICIO	DESCRIPCIÓN
Internet	Otorgar un medio de comunicación fiable para el intercambio de información (llámese voz, datos, video) con el exterior en sus estaciones de trabajo y en sus celulares personales.
Intranet	Disponer de un sistema de comunicación y gestión para todas las áreas internas de la empresa de una forma amigable, rápida y segura para los usuarios.
Usuario en el Directorio Activo	Facilitar a los colaboradores un usuario en el directorio activo de la empresa con el cual tenga acceso a

SERVICIO	DESCRIPCIÓN
	los diferentes servicios de TI desde su estación de trabajo.
Correo electrónico	Permitir a los usuarios de la empresa el envío y recepción de mensajes, por medio una cuenta de correo electrónico institucional, con lo cual puedan desarrollar sus funciones de una forma óptima.
Servicio de impresión	Brindar al usuario el acceso a un sistema de impresión, que facilite el desarrollo de sus funciones.
Servicio de ofimática	Brindar al usuario el acceso en sus estaciones de trabajo a todo un conjunto de Ofimática (Word, Excel, PowerPoint) por medio de Office365, que facilite el desarrollo de sus funciones.
Servicio de comunicación empresarial desde estaciones de trabajo personales	Brindar al usuario un servicio de llamadas, videollamadas, intercambio de mensajes de chat entre colaboradores internos y hacia clientes externos por medio del acceso a Skype Empresaria en sus estaciones de trabajo, que facilite el desarrollo de sus funciones.
Video Conferencia	Ofrecer a los usuarios un servicio de video conferencias en salas de reuniones por medio del sistema Polycom, que permita la comunicación interna entre todos los colaboradores ubicados en las diferentes sucursales de la empresa.
Almacenamiento y compartición de información en servidor de archivos.	Brindar a todas las áreas de la empresa el acceso un servidor de archivos, donde puedan guardar información que será compartida y gestionada entre los usuarios de cada área, que facilite el desarrollo de sus funciones.
Voz sobre IP	Proporcionar de manera eficiente un sistema de llamadas internas y externas a cada usuario de la empresa por medio de teléfonos de voz sobre IP, que facilite el desarrollo de sus funciones.

SERVICIO	DESCRIPCIÓN
VPN	Brindar al usuario la facilidad de conectarse
Correo en celular	Se proporciona a los usuarios el acceso al correo institucional desde los celulares personales de cada uno
Control de Asistencia	Se brinda un servicio de control de asistencia de usuarios al área de Talento Humano por medio de biométricos instalados en todas las sucursales con la finalidad de facilitar un registro de horarios de ingreso y salida del personal.
Microsoft Dynamics GP 2016	Se proporciona a los usuarios una herramienta en sus estaciones de trabajo que se encarga de las operaciones internas de la empresa, las mismas que son: ventas, inventario, compras, contabilidad, proveedores, cuentas por pagar, clientes, cuentas por cobrar, activos fijos. Que facilite el desarrollo de sus funciones.
GENERA	Brindar de forma eficiente y unificada un sistema para la administración y gestión de nómina de personal al área de Talento Humano.
CAIMAN	Se proporciona al área de Logística un sistema que permite realizar la trazabilidad de equipos.
ARANDA	Se proporciona al área de Soporte Técnico de Equipos Médicos de la empresa una herramienta de mesa de servicios para clientes externos, que facilite el desarrollo de sus funciones.
Sistema de Importación	Se proporciona al área de Comercio Exterior una herramienta que permite realizar la planificación de la demanda de los productos.
SIMEDCORE	Se proporciona a las áreas de Compras, Comercial, Logística y Finanzas un sistema para la gestión y control de contratos, ejecución de pedidos, facturación y rentabilidad.
Sistema de Compras	Se proporciona al área de Compras un sistema que permite la gestión de requisición de compras.

3.1.1.2 Gestión de Nivel de Servicio (SLM)

La Gestión de Niveles de Servicio tiene como objetivo encontrar un acuerdo realista entre los costos de los servicios y las necesidades de los clientes, de tal forma que sean asumibles por el cliente y por la organización de TI (Faquinones, s.f.).

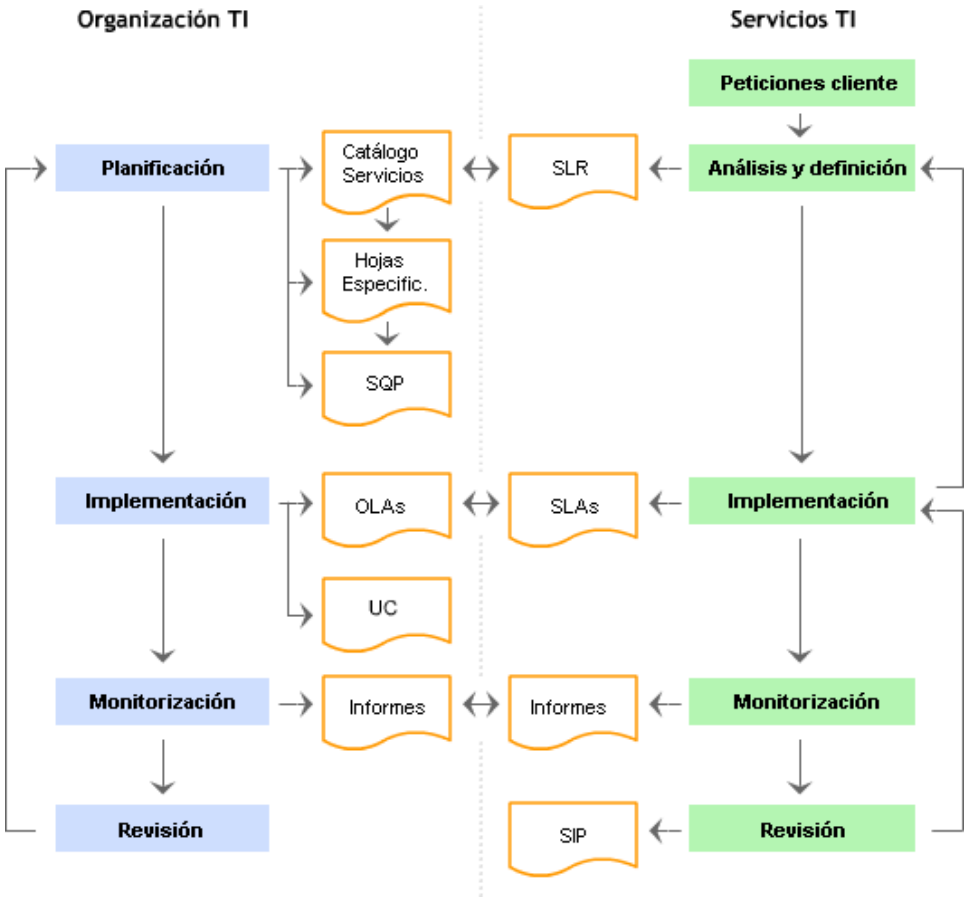


Figura 12. Gestión de Niveles de Servicio.

Tomado de: Faquinones, 2018.

Como se ha mencionó anteriormente en el presente trabajo no se realizará un análisis ampliamente detallado de esta fase, pero sí en términos generales los datos más importantes que contribuyan a una creación de mesa de servicios eficiente. Por tal motivo, una vez definido el Catálogo de Servicios de TI este va ligado directamente a definir un Acuerdo de Nivel de Servicio (SLA) entre el equipo de TI y el cliente interno de la empresa. Para la definición de este SLA se

mantuvo reuniones con los clientes involucrados en cada servicio y de esta forma definir urgencias e impactos para la determinación de prioridades de atención de estos servicios por parte de la Mesa de Ayuda.

A continuación, se establece un cuadro en donde se determinan que tipo de prioridad tiene la atención de un incidente. Esto es la relación entre la urgencia y el impacto de dicho incidente, la urgencia es determinada por el cliente que requiere la atención y el impactó fue determinado en el SLA.

Tabla 11.

Lineamientos para establecer prioridades a los incidentes.

URGENCIA	**IMPACTO**			
	Crítico	**Alto**	**Medio**	**Bajo**
Crítica	*Critica*	*Crítica*	*Alta*	*Media*
Alta	*Crítica*	*Alta*	*Media*	*Media*
Media	*Alta*	*Media*	*Media*	*Baja*
Baja	*Media*	*Media*	*Baja*	*Baja*

Tabla 12.

Impacto de los incidentes.

IMPACTO	DESCRIPCIÓN	EJEMPLO
Crítico	Indisponibilidad de un servicio que afecte a varias áreas	Sin acceso a la red Sin acceso a Internet Sin servidor de Exchange Sin aplicaciones del negocio
Alto	Indisponibilidad de servicio/s que afectan a determinadas funciones	Problemas con la red Ataque de virus
Medio	Indisponibilidad parcial de un servicio	Usuario no envía correos Aplicación no funciona correctamente. Usuario no puede imprimir
Bajo	Actividades planificadas	Instalación de algún programa.

Guiándose en la Tabla 12 se determinó con cada área los siguientes impactos para los servicios de TI, indicados en el Catálogo de Servicios.

Tabla 13.

Impactos de los Servicios de TI de la empresa.

SERVICIO	IMPACTO
Internet	Crítico
Intranet	Bajo
Usuario en el Directorio Activo	Alto
Correo electrónico	Medio
Servicio de impresión	Medio
Servicio de ofimática	Medio
Servicio de comunicación empresarial desde estaciones de trabajo personales	Medio
Video Conferencia	Medio
Almacenamiento y compartición de información en servidor de archivos.	Medio
Voz sobre IP	Medio
VPN	Medio
Correo en celular	Medio
Control de Asistencia	Bajo
Microsoft Dynamics GP 2016	Crítico
GENERA	Medio
CAIMAN	Medio
ARANDA	Crítico
Sistema de Importación	Medio
SIMEDCORE	Crítico
Sistema de Compras	Medio
BI	Alta

3.1.2. Operación del Servicio

Como ya se ha establecido parámetros importantes como lo es el Catálogo de Servicios, se ha definido Acuerdos de Nivel para dichos servicios donde se establecieron tiempos de respuesta con los que debe trabajar la mesa de

servicios. Se empezará el diseño para cada proceso de la fase de operación del servicio. A continuación, se establecerá la estructura en cuanto a la Gestión de Eventos, Gestión de Incidentes, Gestión de Problemas que se manejaran.

3.1.2.1 Diseño de la Gestión de Eventos

Para la Gestión de Eventos de acuerdo con ITIL v3 se maneja con herramientas de monitoreo, que alerten a la Mesa de Ayuda cuando se tenga un indicador de que un servicio de TI podría llegar a fallar. Con la finalidad de que el equipo de TI tome acciones preventivas hacia dicho evento para prevalecer la continuidad de un servicio. La gestión de eventos en la empresa se ha definido mediante alertas de diferentes herramientas de monitoreo para distintos servicios de TI.

Tabla 14.

Herramientas de monitoreo de la empresa.

Servicio de TI	Herramienta	Alerta	Personal encargado
Enlaces WAN	PRTG	Si el consumo de ancho de banda del enlace supera el límite configurado se envía alerta por correo electrónico.	Nivel 1: Mesa de Ayuda. Nivel 2: Jefe de Infraestructura
Estado de servidores	PRTG	Se miden consumos de CPU, memoria, almacenamiento, temperatura. Si se superan límites configurados se envía alerta por correo electrónico.	Nivel 1: Mesa de Ayuda. Nivel 2: Jefe de Infraestructura
Equipos de red	MERAKI	Si los equipos de red (Firewall, Switchs, Puntos de Acceso, Cámaras de Seguridad) presentan algún	Nivel 1: Mesa de Ayuda Nivel 2: Jefe de Infraestructura

		inconveniente que no represente el paro del servicio, se envía alerta por correo electrónico	
Impresión	YSOFT	Cuando se tiene niveles bajos de tóner, consumibles se envía alerta por correo electrónico.	Nivel 1: Mesa de Ayuda Nivel 2: Jefe de Infraestructura
Respaldo de Base de Datos	SCRIPT	Notificación en fallo de respaldo de la BD	Nivel 1: Mesa de Ayuda

De lo mencionado el proceso a seguirse para la Gestión de Eventos es el siguiente:

1. La herramienta de monitoreo emitirá una alarma de posible fallo que vaya a sufrir algún servicio de TI mencionado en la tabla 14 por medio de un correo electrónico hacia los miembros de primer nivel de la mesa de servicios, en este correo se dispondrá de datos como qué dispositivo está fallando, ubicación del dispositivo, fecha del fallo, hora del fallo, sistemas afectados y medidas correctivas a realizarse.

2. Los miembros de primer nivel de la mesa de servicios evaluarán que tipo de evento es y aplicarán las medidas necesarias para solventarlo. De no ser posible su solución, escalarán el caso.

3. Adicional la gestión de evento también consistirá en notificar a los usuarios de cuando vaya a existir algún procedimiento a realizarse por el área de sistemas que vaya a interrumpir algún servicio. Por ejemplo, mantenimiento a los servidores, entre otros. Con lo cual el usuario conocerá la indisponibilidad de un servicio.

En la figura 13 a continuación se puede observar el proceso descrito de las cuatro fases llevadas a cabo:

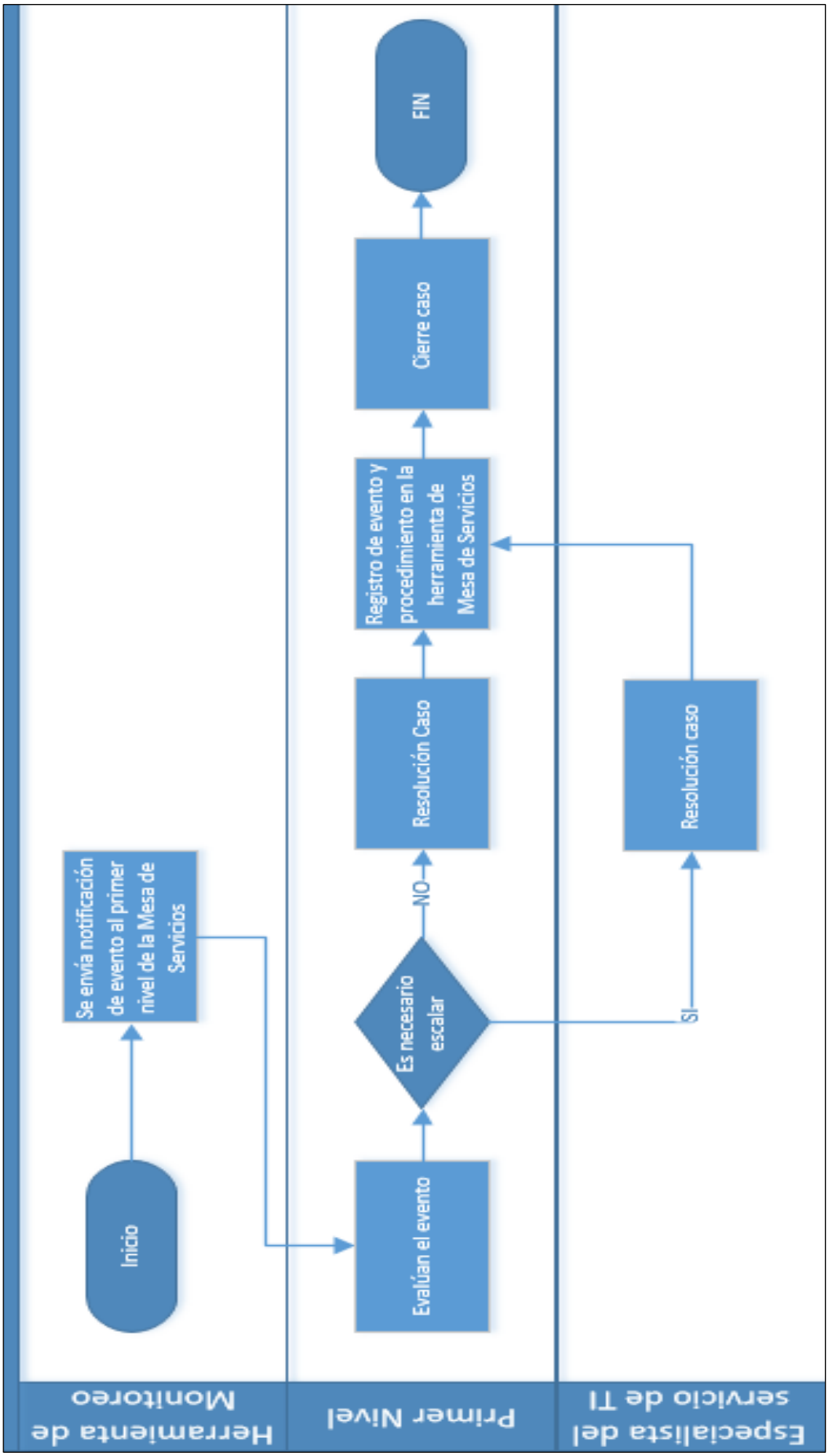


Figura 13. Flujo de trabajo Gestión de Eventos.

3.1.2.2 Diseño de la Gestión de incidentes

Este es el punto más importante en el cual trabajará la mesa de servicios que se plantea en esta tesis, puesto que en esta sección es el punto más débil que se maneja en la actual mesa de servicios de la empresa.

Por tal motivo para el diseño de la estructura que debe seguir la mesa de servicios se ha definido los siguientes ítems:

- Escalas de tiempo y priorización
- Modelos de incidentes.
- Registro de incidentes
- Categorización de incidentes
- Escalamiento de incidentes
- Resolución de incidentes
- Cierre de incidentes
- Métricas

3.1.2.2.1 Escalas de tiempo y priorizaciones

El horario de atención de la mesa de servicios será de lunes a viernes de 8:00 a 19:00. El único punto de contacto para realizar peticiones de servicio, solicitud de acceso a un servicio o incidentes será por medio del por el portal web de la mesa de servicios, al que tendrán acceso por medio de un ícono en el escritorio.

De acuerdo con el análisis realizado en la Gestión de Niveles de Servicio en donde se definió el impacto que tiene cada servicio de TI de la empresa, el

usuario al momento de registrar en el sistema una petición, solicitud de acceso o incidente debe seleccionar que tipo de urgencia tiene ya sea crítica, alta, media o baja. De acuerdo al impacto y urgencia se obtendrá las siguientes prioridades y escalas de tiempo que deben cumplirse en la mesa de servicios.

- 60 minutos (durante horas de oficina) para los incidentes clasificados con prioridad crítica.

- 120 minutos (durante horas de oficina) para los incidentes clasificados como prioridad alta.

- 240 minutos (durante horas de oficina) para los incidentes clasificados con prioridad media.

- 480 minutos (durante horas de oficina) para los incidentes clasificados con prioridad baja.

Tabla 15.

Tiempos Respuestas a Prioridades que manejará la Mesa de Ayuda.

Prioridad	Tiempos de Respuesta
Crítica	60 min.
Alta	120 min.
Media	240 min.
Baja	480 min.

3.1.2.2.2 Modelo de incidente

Muchos incidentes no son nuevos, implican lidiar con algo que ha sucedido antes y puede volver a suceder. Por este motivo, se ha planteado predefinir modelos de incidentes "estándar" y aplicarlos a los incidentes apropiados cuando ocurran.

A continuación, en la tabla 16 se observa el esquema de incidente a seguirse:

Tabla 16.

Modelo de incidente.

MODELO DE INCIDENTE Nro. _____	
Categoría del incidente:	
Nombre del incidente:	
Descripción:	
Pasos por seguir cronológicamente:	
Responsable:	
Umbral de tiempo para cumplir incidente:	
Procedimiento para escalar:	

A continuación, en la tabla 17 se ha generado a forma de ejemplificación un modelo referente a un incidente de la aplicación Microsoft Dynamics GP.

Tabla 17.

Ejemplo de modelo de Incidente para aplicación GP.

MODELO DE INCIDENTE Nro. _____1_____	
Categoría del incidente:	Aplicaciones
Nombre del incidente:	Run application error
Descripción:	Al momento de exportar a Excel un *smartlist,* no muestra datos y aparece un mensaje de GP con los siguiente: RUN APPLICATION ERROR

MODELO DE INCIDENTE Nro. _____1_____	
Pasos por seguir cronológicamente:	1. Ingresar a Excel 2. Opciones -> Avanzadas -> 3. La opción General (Omitir otras aplicaciones que usen intercambio dinámico de datos (DDE) debe estar desactivada. 4. Aceptar, salir de Excel y exportar de nuevo el *smartlist*
Responsable:	Javier Villalba (Técnico de nivel 1 de la mesa de servicios)
Umbral de tiempo para resolver incidente:	30 min.
Procedimiento para escalar:	Escalar en el siguiente orden: 1. Andrés Jurado (Especialista de TI) Si el especialista de TI no llega a la solución debe escalar a la empresa ALTIORA, proveedor de la herramienta.

Como ya se mencionó estos modelos deben estar cargados en la base de datos de conocimiento de la mesa de servicios. Deben tener acceso a estos modelos todos los miembros de la mesa de servicios y de igual forma está como responsabilidad para cada uno de ellos generar este tipo de modelos para los incidentes actuales que se tiene en la empresa y para nuevos incidentes que se vayan a generar. Con la finalidad de garantizar un tiempo de respuesta más corto, optimizar recursos y garantizar la continuidad de los servicios de TI.

3.1.2.2.3 Registro de Incidentes

Todos los incidentes deben estar completamente registrados y sellados con fecha y hora, independientemente de si se han generado a través de una llamada telefónica de la mesa de servicio o si se detectaron a través de un evento.

Se ha planteado que la herramienta que se vaya a seleccionar como mesa de servicios como mínimo debe cumplir los siguientes ítems en el registro de incidentes:

Tabla 18.

Datos que deben registrarse de un incidente.

Datos de que debe tener el registro de un incidente
Número de referencia único
Categorización de incidentes
Urgencia del incidente
Impacto del incidente
Priorización de incidentes
Fecha / hora grabada
Nombre de la persona que registra el incidente
Descripción de los síntomas
Estado del incidente (activo, en espera, cerrado, etc.)
Persona a la que se asigna el incidente
Problema relacionado / Error conocido
Actividades emprendidas para resolver el incidente
Fecha y hora de resolución
Fecha y hora de cierre.

Cabe mencionar que, por cuestiones de cultura de usuarios, al inicio de la puesta en marcha de la herramienta de mesa de servicios va a ser un poco difícil cambiar la forma en la que actualmente los usuarios levantan un incidente hacia el personal de TI, como ya se mencionó esto se da por medio de correos, llamadas telefónicas y de forma personal. Por tal motivo, es responsabilidad de cada miembro de la mesa de servicios indicar al usuario cual es la nueva forma de reportar un incidente.

3.1.2.2.4 Categorización de Incidentes

La categorización de niveles múltiples está disponible en la mayoría de las herramientas, por lo general a tres o cuatro niveles de granularidad. Por lo tanto, de acuerdo los incidentes encontrados en el Capítulo II y al catálogo de servicios creado, se ha planteado la siguiente categorización:

Categoría de primer nivel: aquí se encuentra el nivel más general como lo es *software* y *hardware*.

Categoría de segundo nivel: se ha planteado dividir en servidores, estación de trabajo, biométrico, impresoras, POLYCOM, telefonía IP y celulares

Categoría de tercer nivel: en esta sección se definirá las categorías subsiguientes a las categorías de segundo nivel tanto de *software* como de *hardware*.

A continuación, en las tablas 19 y 20 se puede observar que para los servicios la clasificación de los servicios de TI en los tres niveles mencionados. Estas categorizaciones posteriormente deben ser configurados en la herramienta de mesa de ayuda. La finalidad de esta tarea es facilitar al usuario la tarea de crear casos puesto que se va a tener de una forma clara a qué tipo de servicio corresponde, con esto también se va a poder crear reglas de enrutamiento hacia los técnicos responsables de la mesa de ayuda.

Tabla 19.

Categorización de incidentes por hardware.

Categoría de nivel 1: HARDWARE							
Nivel 2	***Servidores***	***Estación de trabajo***	***Biométrico***	***Impresora***	***Polycom***	***Teléfono IP***	***Celular***
Nivel 3	Procesador	Procesador	Lector de huellas	Tóner	Cámara	Auricular	Pantalla
	Memoria RAM	Memoria RAM	Pantalla táctil	Soporte de papel	Micrófono	Pantalla LCD	Audio
	Disco DURO	Disco DURO	Puerto de red	Alimentador de hojas		Botones	Pin de carga
	Tarjeta de red	Pantalla		Cabezal		Puerto de red	Cámara
	Gabinete	Teclado		Pantalla táctil		Audio	
	Fuente de poder	Mouse		Cristal de copiado			
		Conexiones y accesorios					

Tabla 20.
Categorización de incidentes por software.

Categoría de nivel 1: SOFTWARE							
Nivel 2	***Aplicaciones empresariales***	***Estación de trabajo***	***Biométrico***	***Impresora***	***POLYCOM***	***Teléfono IP***	*Celular*
Nivel 3	Microsoft Dynamics GP	Office	Programa ZKTIME	Programa YSOFT	No realiza videollamada	Crear extensión	Wifi
	SIMEDCORE	Adobe Reader	Reportes de asistencia	No hay conexión a impresora	No transmite contenido	Editar extensión	Correo
	Intranet	Navegadores		Documento encolado		Llamadas internacionales	
	GENERA	Correo				Rutas salientes	
	ARANDA	Wifi				Troncales	
	Sistema de Importación	Carpetas compartidas				Reportes	
	Sistema de Compras	Zoiper					
	BI	Controladores					

3.1.2.2.5 Escalamiento de Incidentes

- **Escalada funcional:** tan pronto como quede claro que el personal de soporte técnico de primer nivel no puede resolver el incidente (o cuando se han excedido los tiempos de destino para la resolución del primer punto, el incidente se lo debe reasignar al nivel de soporte superior.

  Se ha definido tres niveles de soporte que va a manejar la mesa de servicios:

  Tabla 19. Niveles para escalar incidentes

Escalamiento de incidentes	
Nivel 1:	Personal de soporte técnico
Nivel 2	Especialistas de aplicaciones empresariales
	Jefe de Infraestructura
	Administrador de Base de Datos
	Gerente de Sistemas
Nivel 3	Proveedores

- **Escalada Jerárquico:** este tipo de escalamiento se va a dar cuando el incidente sea de prioridad crítica, en este tipo de casos se debe notificar a los administradores de TI apropiados, al menos para fines informativos. También se continuará la cadena de gestión para que los gerentes superiores estén al tanto y puedan estar preparados y tomar las medidas necesarias, como asignar recursos adicionales o involucrar a proveedores encargados.

Es importante mencionar que cualquiera tipo de escalamiento que se vaya a dar la prioridad del incidente permanecerá en la mesa de servicios, esta será siempre responsable de rastrear el progreso, mantener informado a los usuarios, y, en última instancia, para el cierre de incidentes.

3.1.2.2.6 Procedimiento que realizará el personal de la Mesa de Servicios para llegar a la solución de un incidente.

- Pedir al usuario que realice actividades dirigidas en su propio escritorio o equipo remoto.
- El personal de la mesa de servicios implementará la resolución centralmente (por ejemplo, reiniciando un servidor) o remotamente usando software para tomar el control del escritorio del usuario para diagnosticar e implementar una resolución.
- Se solicitará a los grupos de soporte de especialistas que implementen acciones de recuperación específicas (por ejemplo, compatibilidad de red para reconfigurar un enrutador).
- Se solicita a un proveedor o mantenedor tercero que resuelva la falla.

3.1.2.2.7 Procedimiento que realizará el personal de la Mesa de Servicios para cerrar un incidente.

El personal de la mesa de servicios debe verificar que el incidente esté completamente resuelto y que los usuarios estén satisfechos y dispuestos a aceptar que el incidente se cierre. También tendrá que validar lo siguiente para poder cerrar un incidente, al realizar esto garantiza un manejo eficiente de todo el proceso de la gestión de incidentes:

- Categorización del cierre. Se verificará y confirmará que la categorización del incidente inicial fue correcta
- Encuesta de satisfacción del usuario. Se realizará una encuesta de devolución de llamada o correo electrónico de satisfacción del usuario para el porcentaje acordado de incidentes.
- Documentación del incidente. Se debe asegurar que el registro del incidente este completamente documentado.
- ¿Problema en curso o recurrente? Se analizará que tan seguido está ocurriendo dicho incidente para considerarlo y tratarlo como un problema.
- Cierre formal. En el portal se cerrará el incidente.

3.1.2.2.8 Métricas.

Según ITIL v3 Las métricas que se deben monitorear y reportar para juzgar la eficiencia y efectividad del proceso de Gestión de Incidentes y su operación incluirán:

- Número total de incidentes (como medida de control)
- Desglose de incidentes en cada etapa (por ejemplo, sesión, trabajo en curso, cerrado, etc.)
- Tamaño de la acumulación de incidencias actual
- Número y porcentaje de incidentes importantes
- Tiempo transcurrido promedio para lograr la resolución o elusión del incidente, desglosado por código de impacto
- Porcentaje de incidentes manejados dentro del tiempo de respuesta acordado (los objetivos del tiempo de respuesta al incidente pueden especificarse en los SLA, por ejemplo, mediante códigos de impacto y de urgencia)
- Costo promedio por incidente
- Número de incidentes reabiertos y como porcentaje del total
- Número y porcentaje de incidentes asignados incorrectamente
- Número y porcentaje de incidentes incorrectamente categorizados
- Porcentaje de incidentes que cierra la mesa de servicio sin referencia a otros niveles de soporte (a menudo denominado 'primer punto de contacto')
- Número y porcentaje de incidentes procesados por agente de *service desk*
- Número y porcentaje de incidentes resueltos de forma remota, sin la necesidad de una visita.
- Número de incidentes manejados por cada Modelo de Incidente
- Desglose de incidentes por hora del día, para ayudar a identificar los picos y asegurar la coincidencia de los recursos.

3.1.2.3 Diseño de la Gestión de Problemas

La Gestión de Problemas es una operación muy importante dentro de la fase de operación del servicio puesto que no va a permitir tratar incidentes recurrentes

con el fin de llagar a su causa raíz y obtener una solución definitiva. Para la configuración de la mesa de servicios se ha planteado el cumplimiento y configuración de los siguientes ítems:

3.1.2.3.1 Modelo de problemas.

Muchos problemas serán únicos y requerirán un tratamiento individual, pero es posible que algunos incidentes vuelvan a ocurrir debido a problemas latentes o subyacentes (por ejemplo, cuando el costo de una resolución permanente será alto y no se ha tomado una decisión).

Además de crear un registro de errores conocidos en la base de datos de errores conocidos de la mesa de servicios para asegurar un diagnóstico más rápido, la creación de un modelo de problemas para manejar tales problemas en el futuro puede ser útil. Este concepto es muy similar a la idea de los modelos de incidentes ya descritos anteriormente por lo cual será una plantilla similar.

Tabla 20.

Modelo de problemas.

MODELO DE PROBLEMA Nro. _____1_____	
Categoría del problema:	Hardware - Polycom
Nombre del problema:	Se pierde señal en llamadas de POLYCOM
Descripción:	Incidente frecuente, las acciones realizadas son; revisión de conexiones, enlaces, configuraciones. Dichas acciones no resuelven el incidente.
Pasos por seguir cronológicamente:	1) Verificar enlace de datos hacia la sucursal con la cual se está teniendo la videollamada. 2) Configurar Políticas de calidad de servicio en el firewall para priorizar paquetes UDP provenientes de los puertos 5001 y 5010 correspondientes a POLYCOM.
Responsable:	Carlos Yoncón (Jefe de Infraestructura)

MODELO DE PROBLEMA Nro. _____1_____	
Umbral de tiempo para cumplir problema:	1 hora
Procedimiento para escalar:	Si problema persiste debe escalarse al proveedor de internet • Punto Net

3.1.2.3.2 Detección de problemas.

Para la detección de problemas se realizarán las siguientes actividades:

- Sospecha o detección de una causa de uno o más incidentes por parte de la mesa de servicio, lo que provoca que se genere un registro de problemas; es posible que el técnico haya resuelto el incidente, pero no haya determinado una causa definitiva y sospeche que es probable que se repita, por lo que plantee un Registro de problemas para permitir que se resuelva la causa subyacente.

- Análisis de incidentes como parte de la Gestión proactiva de problemas, lo que resulta en la necesidad de generar un Registro de problemas para poder investigar más a fondo la falla subyacente.

3.1.2.3.3 Registro de problemas.

Independientemente del método de detección, todos los detalles relevantes del problema deben registrarse para que exista un registro histórico completo. Debe marcarse con la fecha y la hora para permitir el control y la escalada adecuados. Se debe hacer una referencia cruzada a los incidentes que iniciaron el Registro de problemas, y todos los detalles relevantes deben copiarse al registro.

Se ha planteado que la mesa de servicios a seleccionarse debe como mínimo cumplir los siguientes ítems en el registro de un problema:

Tabla 21.

Registro de problemas.

Datos de que debe tener el registro de un problema
Detalles del usuario
Detalles del servicio
Urgencia del incidente
Detalles del equipo
Fecha hora inicialmente registrada
Detalles de prioridad y categorización
Descripción del incidente
Detalles de todas las acciones de diagnóstico o de recuperación intentadas.

3.1.2.3.4 Categorización de Problemas.

Los problemas se lo catalogarán de la misma manera que los incidentes (y es aconsejable usar el mismo sistema de codificación) para poder rastrear fácilmente la verdadera naturaleza del problema en el futuro y obtener información de gestión significativa.

3.1.2.3.5 Priorización de los Problemas.

Los problemas van a manejar las mismas prioridades que los incidentes. Se usará el mismo sistema de codificación descrito anteriormente en tabla 15.

3.1.2.3.6 Cierre de Problemas.

Cuando se completa un cambio (y se revisa con éxito), y se aplica la resolución, el Registro de problemas debe cerrarse formalmente, al igual que cualquier Registro de incidentes relacionado que aún esté abierto. Se debe realizar una verificación en este momento para garantizar que el registro contenga una

descripción histórica completa de todos los eventos, y si no, el registro debe actualizarse.

El estado de cualquier registro de error conocido relacionado debe actualizarse para mostrar que se ha aplicado la resolución.

3.1.2.4 Estructura de la Mesa de Servicios

De acuerdo con la estructura de la empresa y los fines para los cuales se requiere implementar de define que la mesa de ayuda a implementarse debe ser de estructura centralizada, puesto que nos otorga las siguientes ventajas:

- ✓ Reduce los costos para la organización, utiliza una sola estructura central.
- ✓ Usuarios se encuentran distribuidos alrededor de la empresa.
- ✓ La empresa está ubicada en el centro de la ciudad.
- ✓ La asignación de presupuesto es difícil conseguir, por lo cual utilizará el *service desk* centralizado.
- ✓ Se simplifica la gestión de Servicios

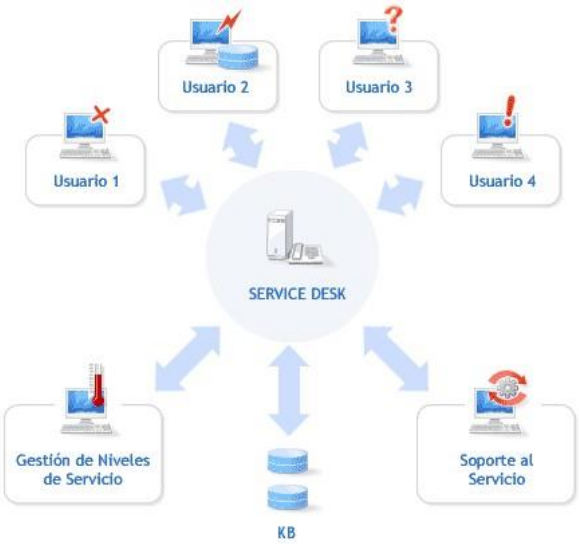


Figura 14. Mesa de ayuda centralizada

Tomado de: Infopersonal, s.f.

3.1.2.4.1 Comparativa en mejoras que debe disponer la nueva Mesa de Servicios.

A continuación, se muestra el cambio que debe tener el *service desk*

Tabla 22.

Comparativa entre service desk actual y el nuevo a implementarse.

Service desk Tradicional	Service desk Moderno
Reactivo: solo resuelve incidentes cuando el usuario lo reporta.	Proactivo: prevención de incidentes y análisis de tendencias.
Soluciona los resultados de los problemas, no las causas	Soluciona la fuente de los problemas
Personal con orientación técnica	Personal con orientación al servicio al usuario
Aislado de la organización	Integrado a la organización
Sin influencias en cuestiones externas al *service desk*	Un motivador clave y gran ayuda a las decisiones de la gerencia
Lucha para conseguir recursos	Justifica los recursos que necesita
Pasivo – Espera a los usuarios	Agresivo – Hace marketing de sus servicios
Conducido por la demanda de soporte	Conducción estratégica: La cara de TI ante los usuarios

3.1.2.4.2 Actividades que realizará la Mesa de Servicios.

Entre las actividades que va a brindar la nueva mesa de servicios tenemos las mencionadas en la fase de operación del servicio propuesta en el marco de referencia de ITIL v3:

Gestión de Eventos:

- Personal de nivel 1 estará en constante revisión de los sistemas de monitoreos de servicios de TI, con el fin dar un aviso previo a los usuarios cuando se tenga programada una tarea que vaya a parar el servicio momentáneamente como mantenimiento y actualización de servidores, depuración de bases de datos, cambios de tóner en impresoras, etc.

- El personal de nivel 1 tiene la responsabilidad de atender de forma rápida cuando llega una alerta de un evento por los sistemas de monitoreos de servicios de TI.

Gestión de Incidentes:

- Personal de nivel 1 deberá atender los incidentes registrados por los usuarios en el portal web de la herramienta de mesa de servicios en los tiempos establecidos según la prioridad que este tenga.

- El personal de nivel 1 en caso de llegar a una solución del incidente debe registrar todos los datos correspondientes en la sección de registros de incidentes de la herramienta, acto seguido dar por cerrado dicho incidente y notificar al usuario correspondiente. Finalmente debe realizar la encuesta de satisfacción al usuario.

- El personal de nivel 1 en caso de no llegar a una solución del incidente dependiendo la prioridad de este seguirá el escalamiento ya sea funcional o jerárquico hacia el nivel de soporte superior y este nivel a su vez repetirá el proceso de registro si es que llega a la solución o de escalamiento de caso contrario.

- El personal de nivel 1 en caso de que el incidente por parte del usuario no sea registrado desde el portal web de la herramienta deberá informar al usuario cuál es la nueva forma de registrar incidentes, procederá atender dicho incidente y lo registrará el mismo en el portal.

Gestión de Peticiones:

- Personal de nivel 1 deberá atender peticiones de servicios de TI siguiendo de igual forma los tiempos definidos según prioridades.
- Si la petición no se realiza desde el portal web será responsabilidad del personal de nivel 1 notificar al usuario donde es el nuevo sitio para las peticiones y deberá registrarla el mismo en el sistema.

3.1.2.4.3 Servicios adicionales que debe proveer la herramienta de Mesa de Servicios.

- Herramienta para control remoto de máquinas.
- Base de datos de conocimiento.
- Administración de los activos informáticos de la empresa.
- Proveer el mantenimiento preventivo y correctivo del hardware.
- Medición de desempeño de personal

3.2 Análisis de herramientas de Mesa de Servicio en el mercado.

En esta sección de acuerdo con el diseño planteado para una mesa de servicios que siga lineamientos de ITIL v3 y en contraste con el presupuesto de la empresa. Se realizará un análisis de los servicios actuales que se ofrecen en el mercado y la posterior elección de uno para su implementación, configuración y pruebas de funcionamiento.

3.2.2 SERVICENOW EXPRESS

Programa creado por ServiceNow (Estados Unidos). Permite gestionar los servicios de TI. Para dar seguimiento a una unidad de trabajo permite la automatización de tareas diarias. El programa es en la nube con lo que se tiene una fácil implementación y configuración. Se ha encontrado en internet

valoraciones muy altas de los usuarios, en promedio se tiene 4/5. Es considerado por muchos como un programa que posee características únicas para implementar servicios de ayuda en la nube (López, 2016). A continuación, se en listan las características más importantes y su valor comercial.

3.2.2.1 Características

- Disponible en la nube.
- Implementación rápida.
- Dispone de notificaciones y alertas.
- Proporciona gestión de cambio, incidentes y problemas.
- Permite tener un listado de todos los activos.
- Altamente escalable.
- Entrega reportes.
- Configuración de reglas para el centro de servicio.
- Maneja SLAs.
- Usuarios se autentican por medio de LDAP.
- Manejo de inventario.
- Gestión de cambios.

3.2.2.2 Valor comercial

Este producto cobra anualmente y tiene los siguientes planes dependiendo los números de usuarios de la empresa:

Tabla 23.

Valor comercial de ServiceNow Expres.

Número de usuarios	Precio anual	Servicios
50 a 150	$ 10.000,00	Todas las operaciones y funciones de la fase de operación del servicio.
150 a 250	$ 20.000,00	Ciclo de vida del servicio
250 a 500	$ 30.000,00	Ciclo de vida del servicio

3.2.3 BMC Remedy Service Request Management

Programa para manejo de tiques de mesa de ayuda en internet. Entrega al usuario un portal web para la creación de incidentes o solicitudes maneja base de datos de conocimiento (Grupo Arión, 2017).

Permite al área de TI y a otras áreas de la empresa definir sus servicios disponibles, mostrarlos en un catálogo de servicios y automatizar la resolución de casos con una interacción con los usuarios vía web. Donde se dispondrá de herramientas para la ejecución de las actividades (Grupo Arión, 2017).

3.2.3.1 Beneficios:

- Dispone de catálogo de servicios.
- Automatiza la gestión de tiques.
- Seguimiento al cumplimiento de SLAs.
- Los usuarios pueden autoayudarse con la información que tiene la mesa de ayuda.
- Minimiza la cantidad de veces de solicitudes de servicio.
- Maneja priorización de atención a casos.
- Dispone de métricas.
- Escalamiento

3.2.3.2 Valor comercial

Tabla 24. BMC Remedy Service Request Management.

Número de usuarios	**Ilimitado**
Precio anual	$ 12.000,00
Servicios	• Mesa de Servicios • Gestión de cambios • Gestión de Niveles de Servicio • Gestión de Peticiones de Servicio. • Base de Datos de Conocimiento • Gestión de Incidentes • Gestión de cambios

3.2.4 SysAid HelpDesk

SysAid considerada una de las líderes en el mercado, empleada en más de 50.000 organizaciones y 120 países alrededor del mundo. Proporciona una efectiva mesa de ayuda y también se tiene gestión de activos (García, s.f.). A continuación, se dará a conocer los beneficios que brinda la herramienta.

3.2.4.1 Beneficios

a) Diversos módulos de gestión.

b) Tiempos de respuestas óptimos.

c) Reduce tiempos de inactividad.

d) Entrega una imagen real de cómo está la mesa de ayuda.

e) Sube la productividad del área de TI.

f) No necesita recursos locales para su implementación.

g) Disponible en diversos idiomas.

3.2.4.2 Valor comercial

Tabla 25. Valor comercial SysAid.

Número de usuarios	**Ilimitado**
Precio anual	$ 3500
Servicios	• 10 administradores • Usuarios finales ilimitados () • 300 activos • Informes avanzados • Tareas y proyectos • CMDB • Paquete ITIL • Gestión de SLA • Control remoto

3.3 Comparativa de parámetros basados en ITIL entre herramientas analizadas.

Se realizó una evaluación a las herramientas que se analizaron de acuerdo con parámetros de ITIL y criterios requeridos a cumplirse que satisfagan la necesidad de la empresa. A continuación, se muestra la valoración para los parámetros de los *HelpDesk* basados en ITIL.

Tabla 26.

Valoración de parámetros de herramientas de mesa de servicios.

Valoración	***Resultado***	***Valor***
Cumple	*Sí*	*1*
No cumple	*No*	*0*

Tabla 27.

Comparativa de herramientas de mesa de servicios.

	ServiceNow	**BMC Remedy Service Request Management**	**SysAid**
Basado en procesos ITIL	Sí	Sí	Sí
Validad por las organizaciones mundiales	Sí	Sí	Sí
Tiene módulos adicionales	Sí	Sí	No
Solución basada en la web	Sí	Sí	Sí
Soporte online disponible	Sí	No	Sí
Facilidad de la instalación	No	No	Sí
Facilidad de uso y manejo	Sí	Sí	Sí
Interfaz gráfica	Sí	No	Sí
Genera gran número de reportes	Sí	Sí	Sí
Permite la creación de reportes propios	No	Sí	No

	ServiceNow	BMC Remedy Service Request Management	SysAid
Disponible en español	No	Sí	Sí
Alto nivel de seguridad	Sí	No	No
Requerimientos mínimos de infraestructura	Sí	No	Sí
Altos niveles de customización de la herramienta	Sí	Sí	No
Amplia funcionalidad de la herramienta	Sí	Sí	Sí
Gestión de la fase de operación del servicio	Sí	Sí	Sí
Gestión de la fase de estrategia del servicio	Sí	No	No
Gestión de la fase de diseño del servicio	Sí	No	Sí
Gestión de la fase de transición del servicio	Sí	No	No
Gestión de la fase de mejora continua del servicio	Sí	Sí	Sí
Número de p0arámetrso cumplidos sobre 20	17/20	12/20	14/20
Promedio	85%	60%	70%

3.4 Selección de una Herramienta de Mesa de Servicio.

De acuerdo con el análisis realizado se determinó que la herramienta SysAid es la seleccionada puesto que:

- A pesar de que el mejor puntuado es ServiceNow es una herramienta con un valor comercial muy elevado para los presupuestos que maneja la empresa.
- SysAid se maneja en base a ITIL v3 que es lo que se estaba buscando para lograr un valor agregado en la entrega de servicios de TI de la empresa.
- De todas las fases del ciclo de vida del servicio al ser una mediana empresa lo más requerido y como se plantea en esta tesis es el manejo de la fase de operación del servicio, lo cual si cumple SysAid.
- SysAid cuenta con las herramientas adicionales requeridas como control remoto de máquinas, módulo para base de conocimientos, gestión de inventarios, monitoreo y reportes.
- De acuerdo con el modelo de contrato que maneja SysAid permite la escalabilidad de la empresa.

3.5 Implementación de SysAid.

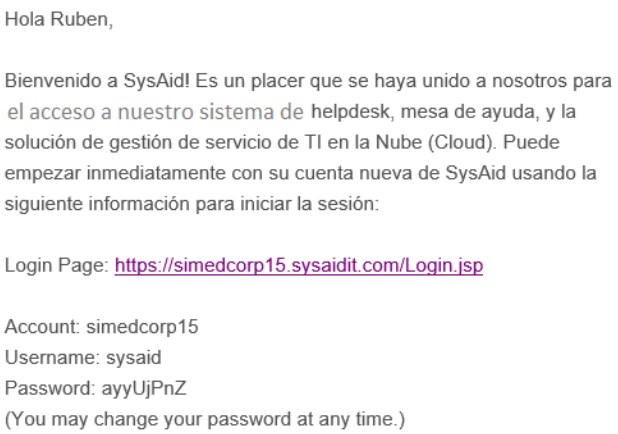
En esta sección se especificará cómo se realizó el procedimiento para la implementación de la mesa de servicios SysAid en la empresa. Se indicará que configuraciones se implementó en la herramienta de acuerdo con la estructura anteriormente planteada en cuanto a las diferentes directrices del ciclo de vida del servicio.

3.5.1 Primer ingreso al sistema

Una vez realizada la compra de la licencia de la herramienta SysAid envía un correo hacia la persona de contacto de la empresa en la cual indica los siguiente:

- URL de portal web a la que se tendrá acceso para la mesa de servicios.
- Usuario administrador
- Contraseña del usuario administrador.

Esta información se la puede observar en la figura 15 a continuación,


Hola Ruben,

Bienvenido a SysAid! Es un placer que se haya unido a nosotros para el acceso a nuestro sistema de helpdesk, mesa de ayuda, y la solución de gestión de servicio de TI en la Nube (Cloud). Puede empezar inmediatamente con su cuenta nueva de SysAid usando la siguiente información para iniciar la sesión:

Login Page: https://simedcorp15.sysaidit.com/Login.jsp

Account: simedcorp15
Username: sysaid
Password: ayyUjPnZ
(You may change your password at any time.)

Figura 15. Correo inicial de SysAid.

3.5.2 Pantalla de ingreso al sistema.

Después de acceder a la dirección indicada en el sistema se muestra la siguiente pantalla:

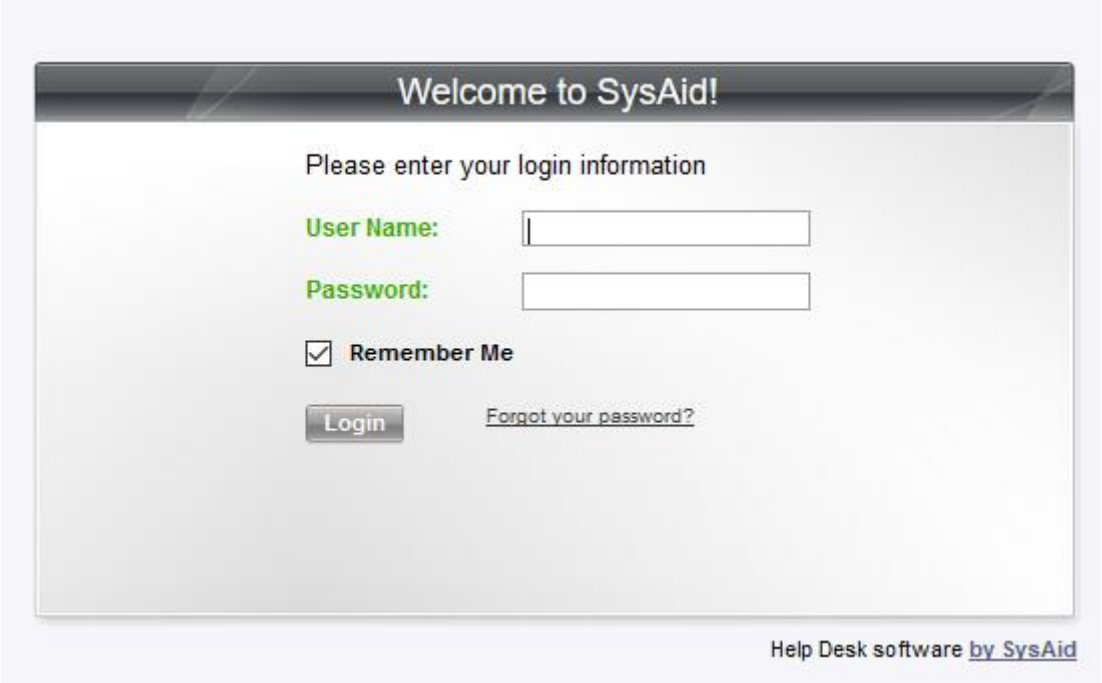


Figura 16. Módulo de acceso a SysAid.

En esta sección se deberá ingresar los datos de usuario y contraseña recibidos en el correo inicial, en la figura 17 se observa el portal de administración.

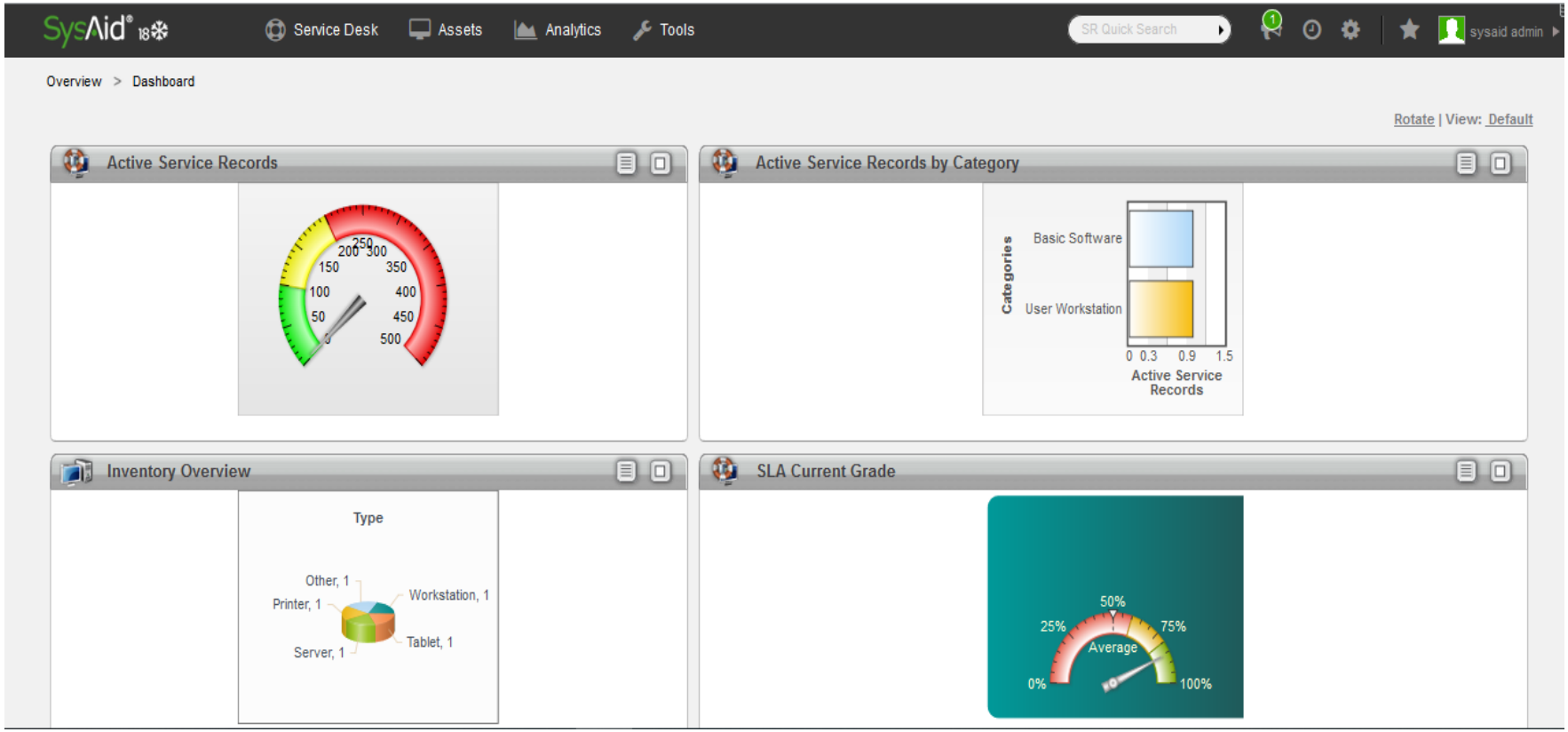


Figura 17. Portal de administración de SysAid.

El Portal de Administración es el módulo de gestión de SysAid. Se va a tener acceso tanto a diagramas y gráficos en tiempo real como a informes más detallados. También se puede diseñar informes y modificar informes existentes.

3.5.3 Configuración del Servicio de Descubrimiento Remoto de SysAid.

Como solución integral de Gestión de servicios de TI (ITSM), SysAid consta de dos componentes básicos y estrechamente integrados: *Service Desk* y *Asset Management*. La implementación de *IT Asset Management* (ITAM) puede ser un desafío en una organización de múltiples sitios, especialmente cuando ITSM se implementa como un servicio en la nube. Los intentos de descubrir y monitorear la red desde fuera de la organización encontrarán obstáculos inevitables debido a la utilización del firewall local y de la red.

Para resolver estos problemas, SysAid coloca un tipo de proxy, llamado *SysAid Remote Discovery Service* (RDS), en la red local de una rama donde se encuentran los activos. El RDS es el único nodo en la red local que se comunica directamente con el servidor o la nube de SysAid. Realiza todos los procesos de supervisión, descubrimiento de inventario, despliegue de agente e integración LDAP localmente en sitios remotos, y luego comunica todos los datos necesarios a su servidor o nube SysAid. El uso de RDS garantiza que todo el tráfico de red generado durante el descubrimiento y la supervisión de la red sea tráfico local. Esto da como resultado una reducción de la latencia de la red y el uso de ancho de banda, y una mayor confiabilidad. SysAid RDS no requiere que abra puertos en sus firewalls locales, y transmite todos los datos al servidor SysAid o a la nube a través de Internet.

3.5.3.1 Instalación del RDS

Se puede instalar RDS en tantos hosts como sea necesario para el descubrimiento y la supervisión de la red. Para este caso se realizará la instalación en un servidor físico que es usado para el sistema de biométricos (SRVBIOMETRIC01 IP: 192.58.1.4)

El proceso para realizar la instalación del RDS es el siguiente:

1. Se debe descargue el paquete de instalador apropiado. Guardar dicho archivo en el servidor que hospedará RDS.

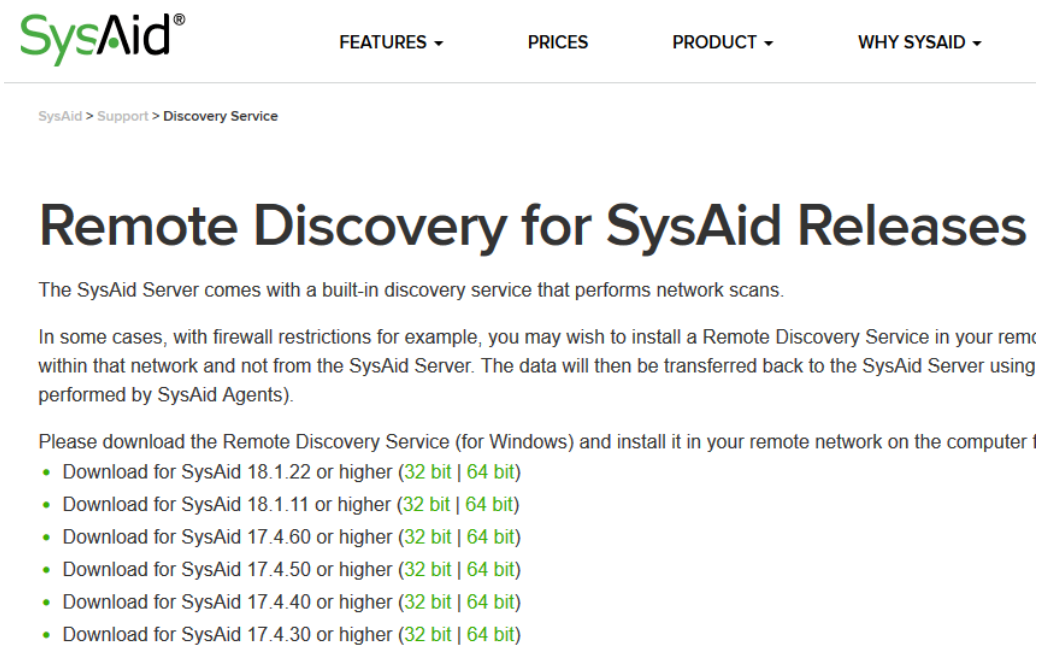


Figura 18. Archivos RDS disponibles.

La versión de SysAid con la que se está trabajando es la v18.2.13 b3 y el servidor en donde se va a instalar es de 32 bits.

4 Ejecuta el paquete de instalador.

5 En la primera página del instalador, haga clic en Siguiente.

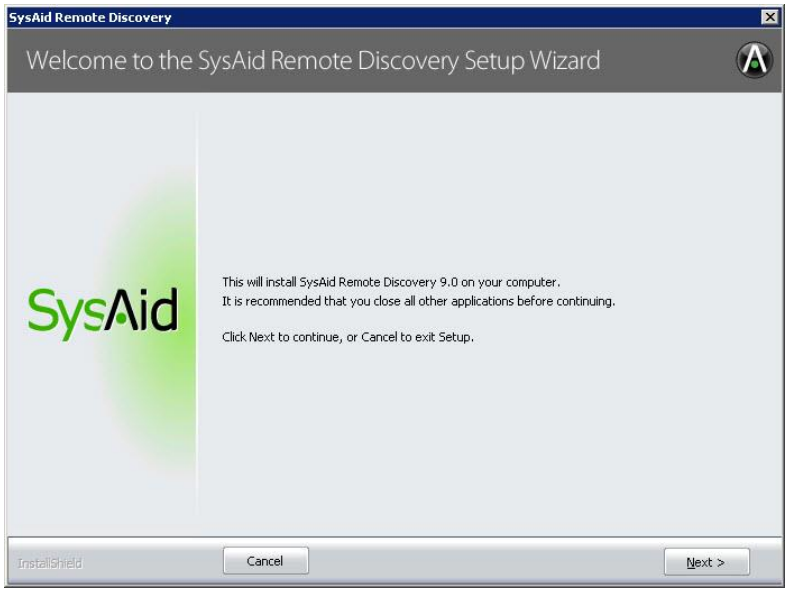


Figura 19. Pantalla de bienvenida al instalador del RDS.

6 Elija la ubicación para la instalación de RDS usando el botón Examinar, luego haga clic en Siguiente.

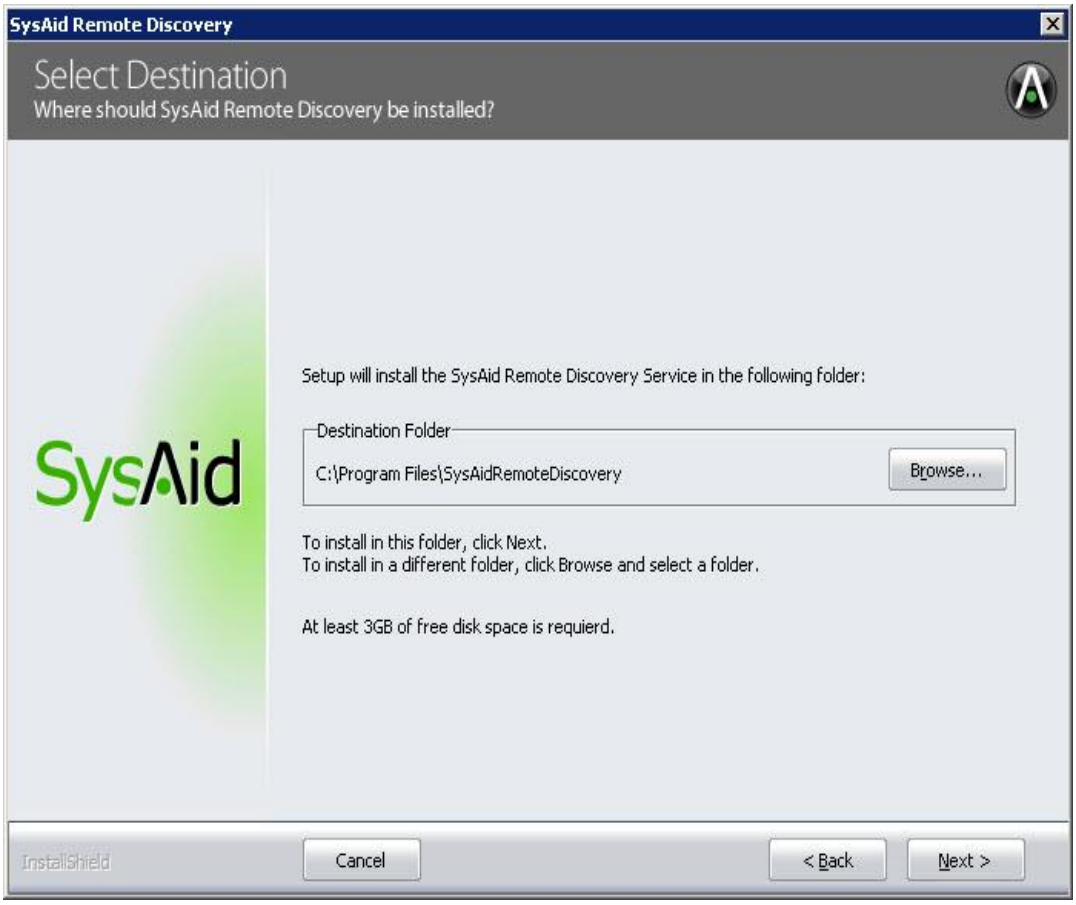


Figura 20. Selección de destino para instalación.

7 Se debe elegir si desea que el instalador RDS cree automáticamente una cuenta de usuario administrador local dedicada para RDS o se puede especificar una cuenta de usuario que tenga privilegios administrativos en esta máquina, que tiene un perfil de usuario local. Esto significa que la cuenta de usuario específica ha iniciado sesión previamente en esta máquina al menos una vez.

8 Nombre del servicio, se ingresa el nombre del nodo RDS como se prefiere que aparezca en SysAid en la lista de RDS. Este nombre selo configuró como “**SIMEDRDS**”.

9 Ingrese su ID de cuenta y URL del servidor tal como aparecen en SysAid en Configuración> Descubrimiento de red> Descargas.

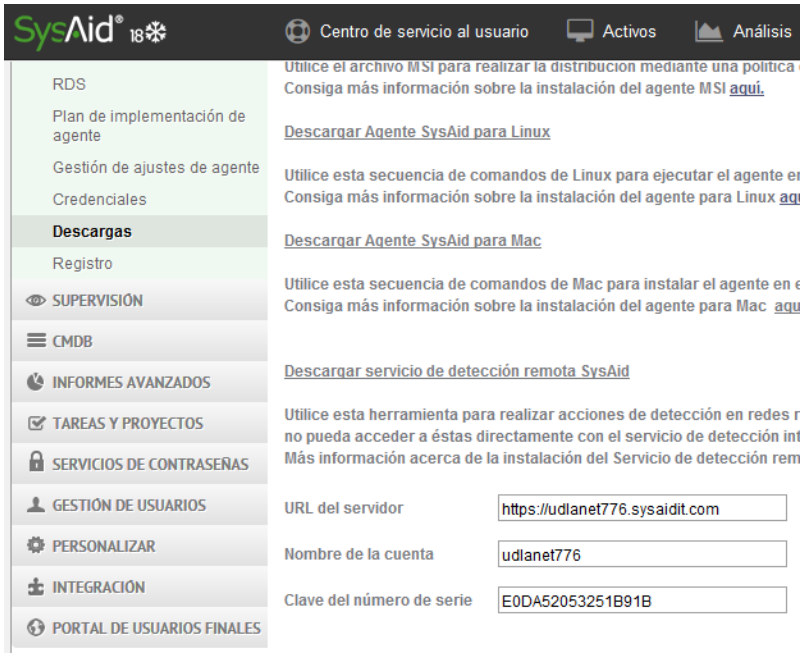


Figura 21. URL del servidor y nombre de la cuenta de SysAid.

Como se puede observar en la figura 21 el URL del servidor es **https://udlanet776.sysaidit.com** y el nombre de la cuenta es **udlanet776.**

10 Se coloca el puerto que RDS usará para aceptar las comunicaciones entrantes de los agentes implementados en la red local. Para este caso se utilizó el **puerto 8080.** Luego hacer clic en Siguiente. Estas configuraciones se pueden observar en la figura 22 a continuación:

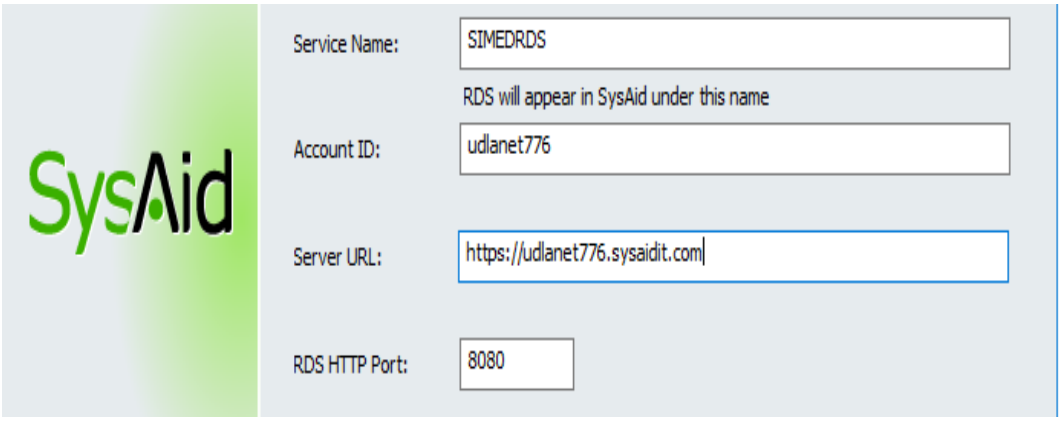


Figura 22. Información de la cuenta del RDS.

11 Se revisa la información de configuración que ingresada. Si todo está correcto, se da clic en continuar.

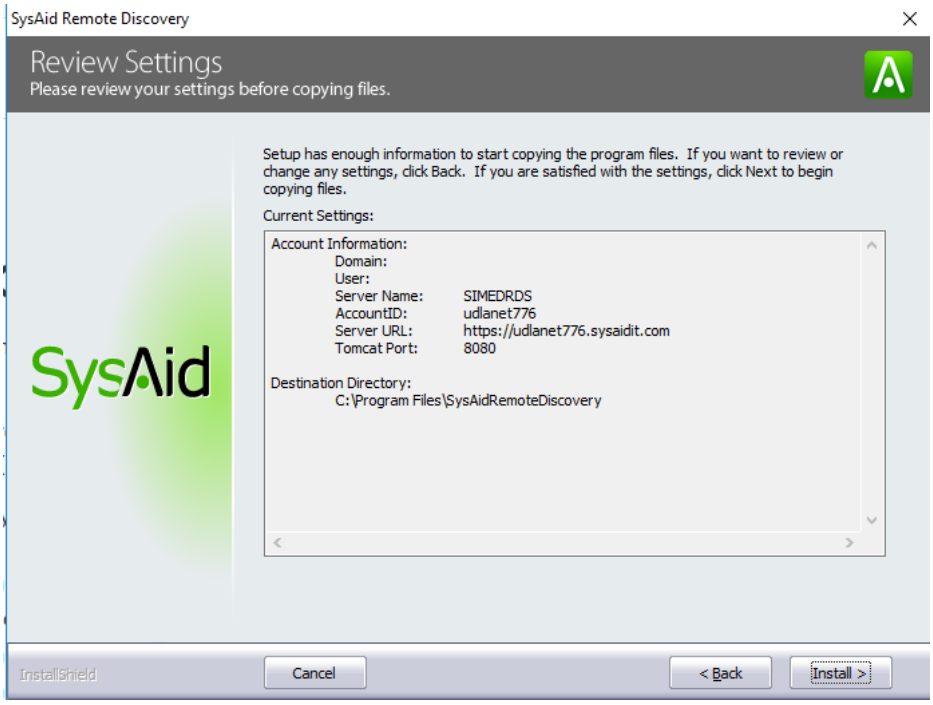


Figura 23. Revisión de la configuración del RDS.

12 SysAid instala el RDS.

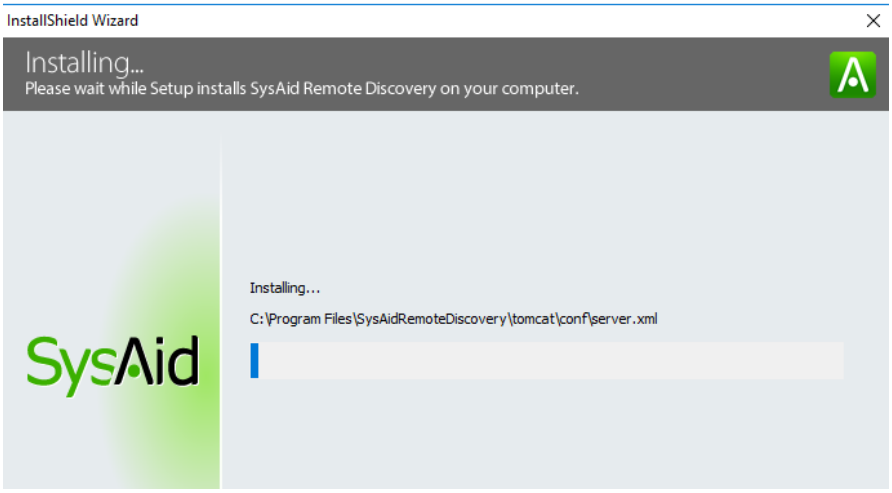


Figura 24. Instalación del RDS.

13 Cuando se completa la instalación, se abre una pantalla de instalación completa. Se da clic en finalizar para cerrar el Asistente de configuración.

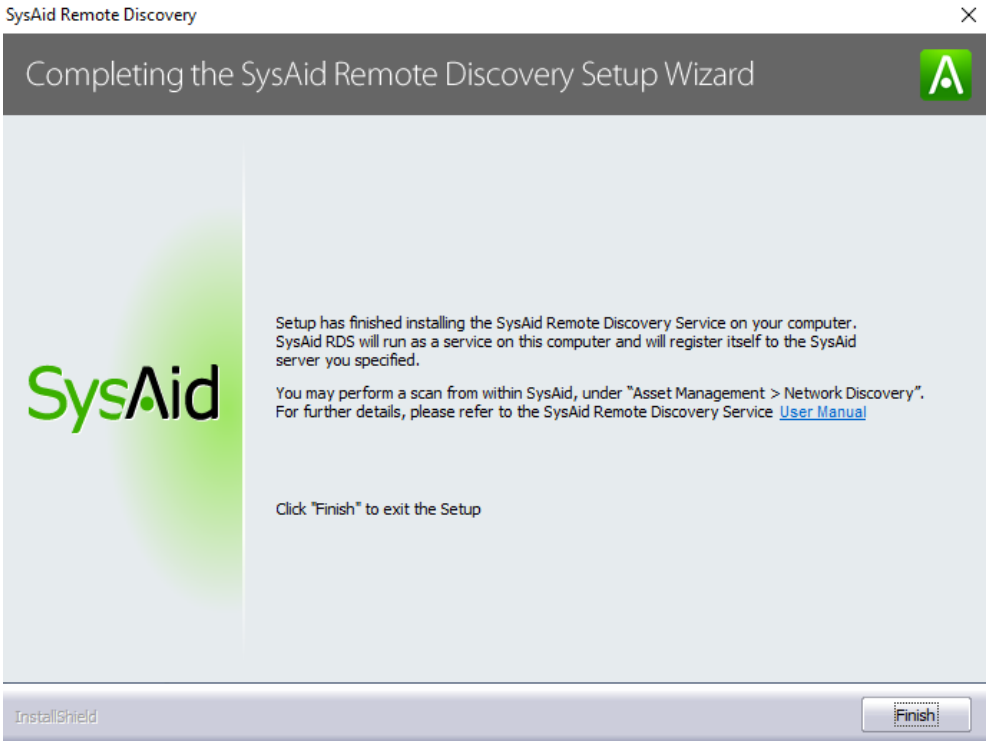


Figura 25. Finalización de la instalación del RDS.

14 El RDS que se acaba de instalar se lo puede ver el portal web de SysAid en Configuración> Descubrimiento de red> RDS.

Figura 26. Vista del nodo RDS implementado en el portal web de SysAid.

3.5.4 Credenciales para RDS

Después de instalar el RDS para que pueda existir una comunicación con SysAid deben habilitarse Credenciales que contiene toda la información necesaria para

dicha comunicación. Cuando se requiere para la autenticación, SysAid transfiere automáticamente la información al RDS en formato cifrado para garantizar la seguridad de su información confidencial.

Se deben llenar los siguientes campos para la creación de la respectiva credencial:

- Nombre: nombre seleccionado para el conjunto de credenciales. Se usó CR_SIMED
- Nombre de usuarios: se ingresa una cuenta que tenga permisos de administración dentro del dominio. Para esta configuración se utilizó SIMED\Administrador
- Contraseña: se coloca la contraseña para el activo al que se desea acceder.
- Se habilita las opciones de válido para: Windows, LDAP, SSH, SNMP

En la figura 27 a continuación se puede observar las configuraciones mencionadas para la creación de credenciales, que usará el RDS.

Figura 27. Creación de credenciales para el RDS.

3.5.5 Creación de usuarios.

Lo primero que debe hacer en SysAid es configurar los usuarios que tendrán acceso al sistema.

En SysAid, hay dos tipos de usuarios:

- Usuarios finales, quiénes pueden acceder al Portal de usuario final.

- Administradores, que pueden acceder a todas las partes de SysAid para las que se les otorga permiso.

3.5.5.1 Verificación de la configuración de usuario de SysAid

Se debe verificar en primer lugar que la configuración personal sea la correcta. Se debe hacer clic en el nombre de usuario en la esquina superior derecha y elegir la opción Mi configuración. Aquí se puede seleccionar el idioma de su elección y asegurarse de que su información personal sea correcta.

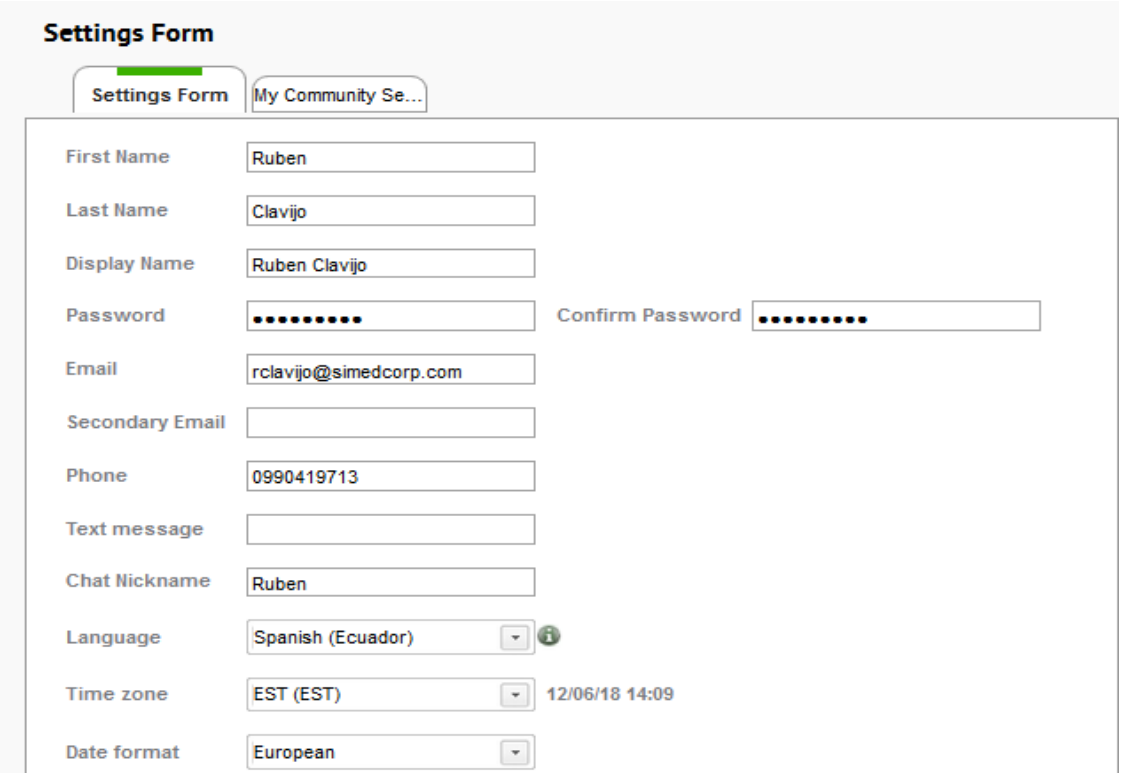


Figura 28. Configuración cuenta administrador.

A continuación, vaya a Configuración> Personalizar> Valores predeterminados de cuenta. Esta página contiene muchos de los mismos elementos que la página Mi configuración. La diferencia aquí es que estas configuraciones afectan a todos los usuarios nuevos que cree en SysAid, tanto usuarios finales como administradores.

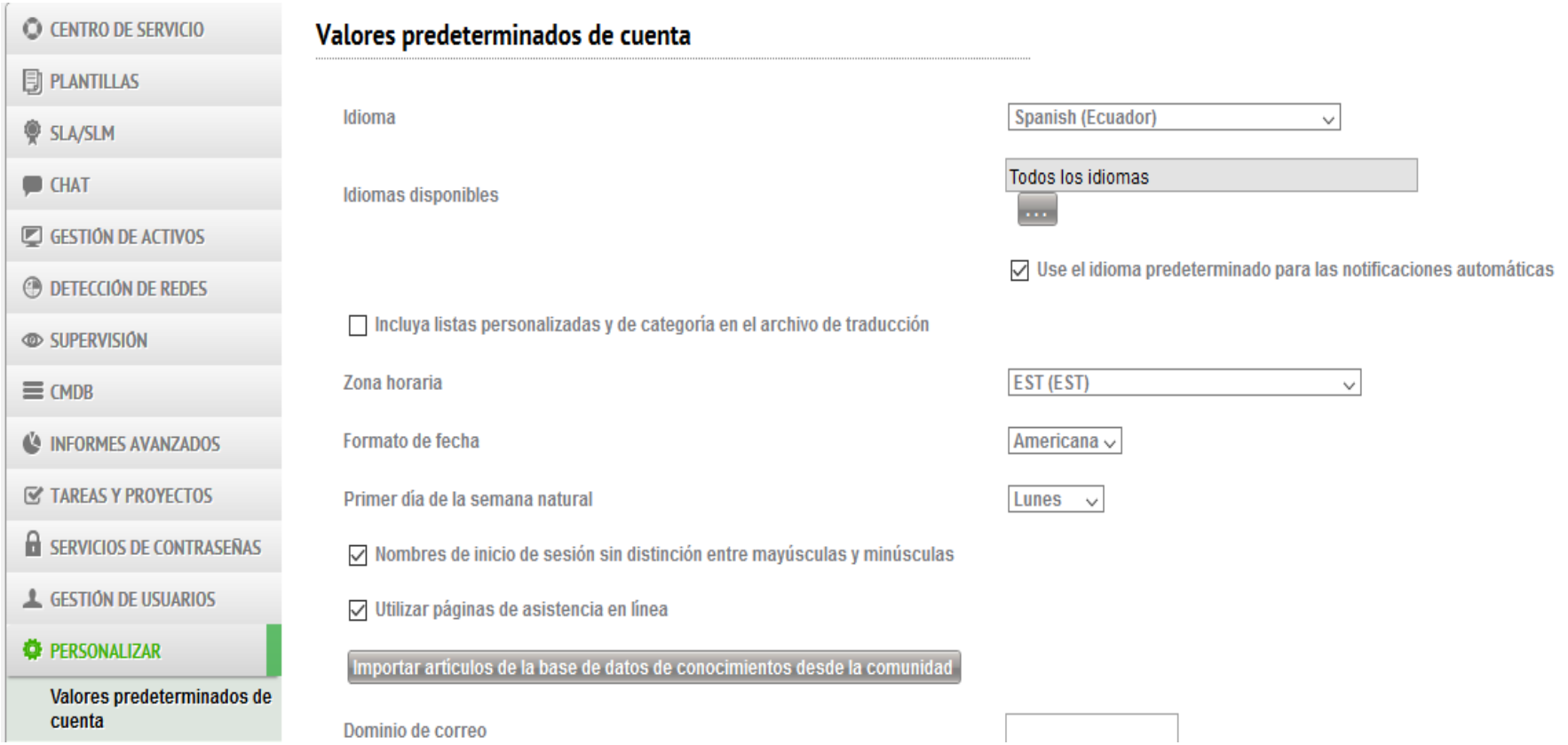


Figura 29. Personalización de cuenta.

3.5.5.2 Creación de Usuarios Finales

En SysAid existen tres formas de crear o importar usuarios finales:

a) Importar usuarios automáticamente de LDAP / AD.

b) Importar usuarios de un archivo .csv (delimitado por comas).

c) Crear usuarios manualmente.

Al disponer en la empresa actualmente ya del manejo de una estructura de usuarios a través del directorio activo será la primera opción la que se va a emplear para la importación de usuarios a la herramienta. A parte la ventaja de importar usuarios directo desde el AD son las siguientes:

- No tendrá que duplicar todos sus perfiles de usuario que ya están almacenados en el AD.

- Sus usuarios podrán autenticarse directamente a través de su AD.

- Puede habilitar el inicio de sesión único (solo Microsoft Active Directory) para que los usuarios inicien sesión automáticamente en SysAid cuando inician sesión en su computadora.

3.5.3.2.1 Para configurar la integración de LDAP:

Vaya a Configuración> Integración> LDAP.
Como se está usando en la empresa Microsoft Active Directory, se debe emplear el asistente de configuración LDAP para importar la estructura del directorio activo de la empresa. Se debe asegurar de eliminar cualquier unidad organizativa no deseada después de la importación. Hacer clic en el botón del asistente de configuración de LDAP donde se desplegará una ventana en la cual se llenarán los siguientes campos, este paso se lo realiza puesto que al realizarse una réplica del AD también se copiarán objetos no necesarios:

- **Nombre RDS**

  Este es el RDS que usará para comunicarse con el servidor LDAP. En este campo se debe seleccionar el RDS configurado en los pasos anteriores (RDS_SIMED).

- **Tipo de servidor**

  Se deja como Directorio Activo.

- **Nombre de host LDAP**

  Este es el nombre de la computadora que aloja su LDAP, en este caso la dirección IP del Directorio Activo de la empresa, el cual es 192.58.1.6.

- **Número de puerto LDAP**

  Si está utilizando una conexión no segura, por lo general es 389. Si está utilizando una conexión SSL, generalmente es 636. En este caso se utilizó el puerto 636 porque se maneja SSL.

- **Credenciales**

  Se utiliza la credencial previamente creada (CR_SIMED.)

- **Dominio**

  Este es el dominio que va a importar desde LDAP, en este caso es el dominio de la empresa (simed.com).

- **LDAP sobre SSL**

  Se marca la opción LDAP sobre SSL puesto que se usa este tipo de conexión hacia el servidor LDAP de la empresa.

- **Comprobar configuración**

  Se da clic en comprobar configuración si todo está correcto se recibe el mensaje “Conexión establecida con éxito”.

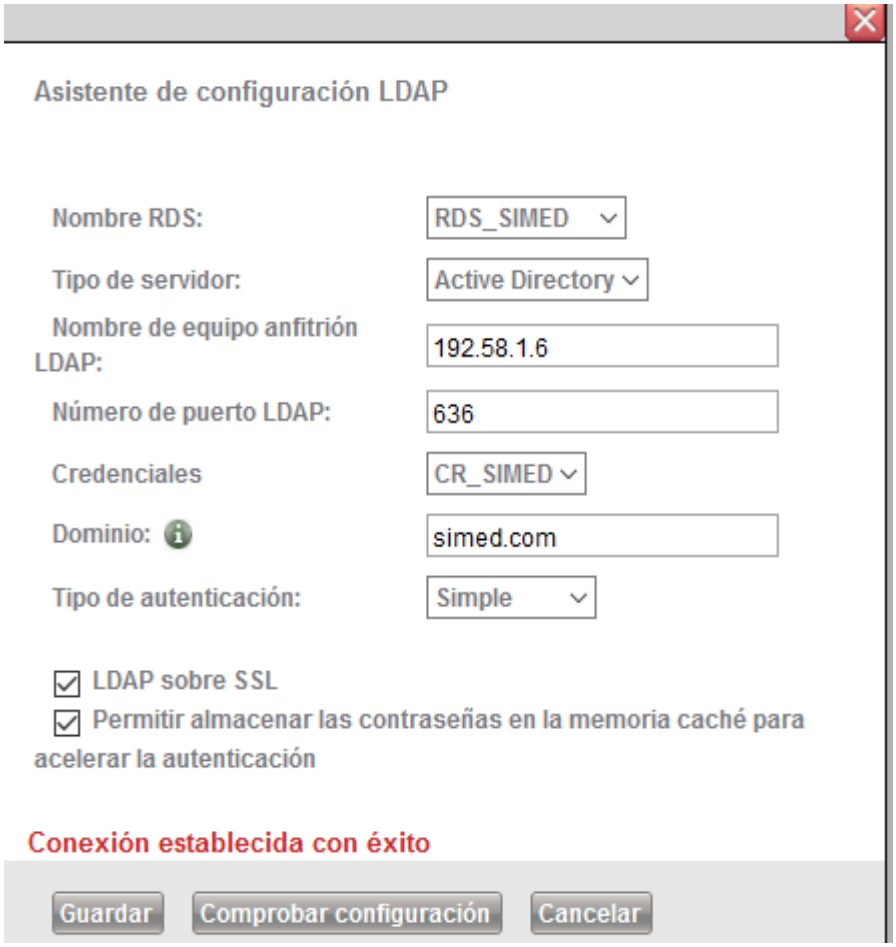


Figura 30. Configuración de LDAP.

- **Guardar configuración**

  Después de comprobar la configuración se da clic en Guardar y automáticamente se llenarán los campos de la configuración LDAP, en la figura 31 a continuación se puede observar como por defecto se llenaron los campos por defecto y además se tiene la opción de habilitar o deshabilitar opciones como:

  - Almacenar contraseñas en memoria caché.
  - Importar grupos.
  - Habilitar LDAP.
  - Programar escaneo para actualizar parámetros de LDAP.
  - Deshabilitar usuarios que no hayan sido agregados por LDAP.

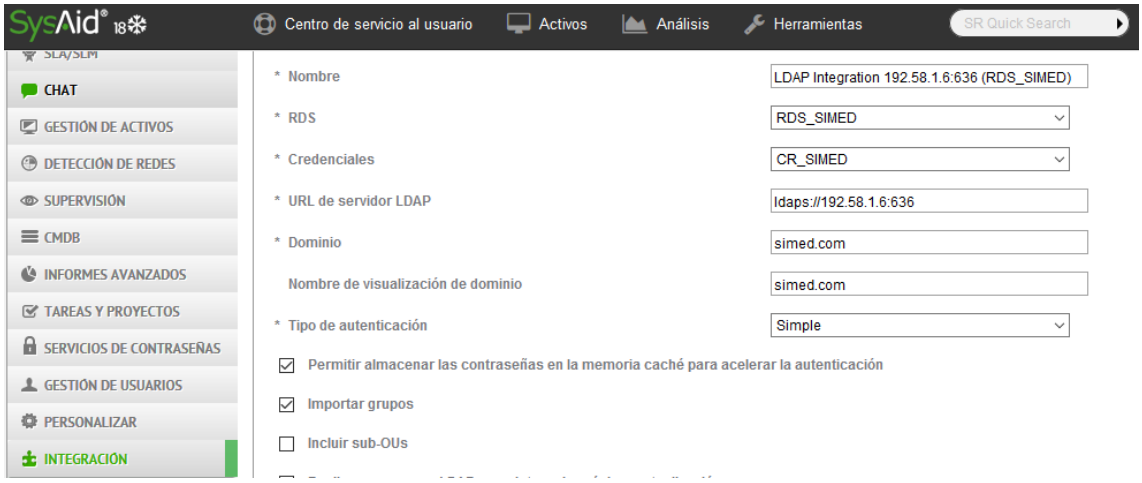
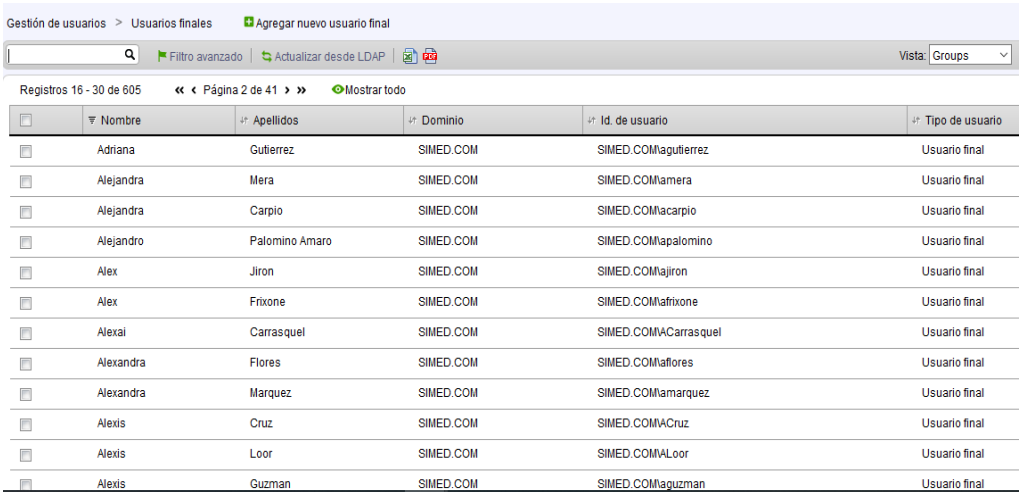


Figura 31. Configuraciones finales de la integración LDAP.

Para finalizar el proceso de la integración de LDAP se marca la opción “Habilitar integración con LDAP” y se da clic en guardar. Con la ejecución de estos queda por acabado la configuración de LDAP. Después de completar la configuración de integración de LDAP, se debe ir a Herramientas> Administración de usuarios> Usuarios finales y hacer clic en Actualizar desde LDAP. Una vez completada la importación LDAP, se debe actualizar la lista para verificar que los usuarios se importaron con éxito. En la figura 32 a continuación se puede observar que se importaron todos los usuarios del Directorio Activo de la empresa de forma exitosa, se cuenta con 41 páginas de usuarios.



Nombre	Apellidos	Dominio	Id. de usuario	Tipo de usuario
Adriana	Gutierrez	SIMED.COM	SIMED.COM\agutierrez	Usuario final
Alejandra	Mera	SIMED.COM	SIMED.COM\amera	Usuario final
Alejandra	Carpio	SIMED.COM	SIMED.COM\acarpio	Usuario final
Alejandro	Palomino Amaro	SIMED.COM	SIMED.COM\apalomino	Usuario final
Alex	Jiron	SIMED.COM	SIMED.COM\ajiron	Usuario final
Alex	Frixone	SIMED.COM	SIMED.COM\afrixone	Usuario final
Alexai	Carrasquel	SIMED.COM	SIMED.COM\ACarrasquel	Usuario final
Alexandra	Flores	SIMED.COM	SIMED.COM\aflores	Usuario final
Alexandra	Marquez	SIMED.COM	SIMED.COM\amarquez	Usuario final
Alexis	Cruz	SIMED.COM	SIMED.COM\ACruz	Usuario final
Alexis	Loor	SIMED.COM	SIMED.COM\ALoor	Usuario final
Alexis	Guzman	SIMED.COM	SIMED.COM\aguzman	Usuario final

Figura 32.Importación de usuarios desde LDAP.

3.5.5.3 Creación de Administradores

Para la creación de administradores existen dos formas; manual o convirtiendo a un usuario final en administrador.

De forma manual se debe llenar los siguientes campos:

Se dirige a Herramientas > Administradores > Crear nuevo administrador y se llena los campos: identidad de usuario, nombre de usuario, contraseña, nombre, apellido y correo.

Figura 33. Creación de administradores.

Convirtiendo a usuario final en administrador:

Se dirige a Herramientas > Usuario finales > se selecciona al usuario que será administrador del sistema y se da clic en convertir en administrador.

Figura 34. Convertir en administrador de SysAid a usuario final.

3.5.6 Configurar la integridad de correo electrónico.

SysAid admite la integración de correo electrónico para:

- Crear nuevos incidentes a partir de correos electrónicos entrantes.
- Registrando toda la correspondencia por correo electrónico relacionada con un registro de servicio específico.
- Envío de notificaciones automatizadas a usuarios finales y administradores.

Para la configuración se va a usar una cuenta de Office365 de la empresa. La cual se usa regularmente para las notificaciones de aplicaciones. La configuración de dicha cuenta se puede observar en la figura 35 a continuación:

Los campos que se debe llenar son:

- Nombre en pantalla: nombre con el que se verán los correos entrantes de notificaciones. Se ha configurado como Notificaciones SysAid.
- Dirección de correo electrónico: la dirección de correo electrónico con la cual se van a enviar los mensajes. Se ha configurado la cuenta no-reply@simedcorp.com
- Nombre del equipo anfitrión SMTP: la dirección del servidor SMTP, en este caso como se maneja Exchange Online en la empresa se debe colocar el servidor SMTP de Office365 (smtp.office365.com).
- Puerto SMTP: se debe colocar el puerto del servidor SMTP, en este caso es el puerto para Office365 (587).
- Tipo de conexión cifrada: se elige el tipo de conexión para el servidor que se maneje, en este caso al ser Office365 se maneja el protocolo SSL.
- Usuario y contraseña: se coloca un usuario y su respectiva contraseña que esté creado en el servidor de correos.

Figura 35. Integración con correo electrónico.

3.5.7 Integración de Office365 con el calendario de SysAid.

En esta sección se implementará la integración entre SysAid y Office 365 con el fin de sincronizar el calendario SysAid con el calendario de Outlook. El proceso de sincronización exporta datos de SysAid a hacia el servidor integrado. Esta característica permite disponer una visión integrada de las tareas de los técnicos tanto desde Outlook como del calendario de SysAid.

Para habilitar la sincronización con Office 365, se debe completar cada campo usando las descripciones a dadas a continuación. Después de haber ingresado la información necesaria, el administrador individual debe habilitar la sincronización desde ***Herramientas> Calendario> Mi configuración de calendario*** para completar el proceso de sincronización.

- **Protocolo:**
  Se selecciona OWA ya que es Office365.

- **URL del servidor de Exchange:**
  Este es el nombre o la dirección IP de la computadora que aloja su Exchange. Para la empresa es https://outlook.office365.com/owa/simedcorp.com

- **Nombre de dominio de red (NetBIOS):**
  Este es su nombre de dominio de red. El de la empresa es simedcorp.com

- **Nombre de usuario:**

  El usuario de Exchange u Office 365 cuya cuenta se usa para la sincronización. Para Exchange, el usuario debe tener permiso en Exchange para crear eventos en los calendarios de Outlook de los empleados.

  Para esta configuración se utilizó una cuenta de Office365 de la empresa (office8@simedcorp.com). A la cuenta seleccionada se la debe unir como miembro al grupo (Administradores de Organización), este proceso se lo realiza en el directorio activo, se puede observar la configuración de lo mencionado en la figura 23, después de unir la cuenta a este grupo se debe dar permisos en los buzones de las personas que van a ser administradores en SysAid.

  Este proceso se lo realiza en la *"Consola de administración de Exchange"* en el servidor de correo de la empresa (192.58.1.5). Sección Office365 > configuración de destinatario > buzón > en buzón al que se quiere dar permiso clic derecho y selección de la opción "administración de los permisos de acceso completo", en el cuadro siguiente se agrega a la cuenta que se va a usar para la sincronización con SysAid. Esto se puede observar en la figura 36.

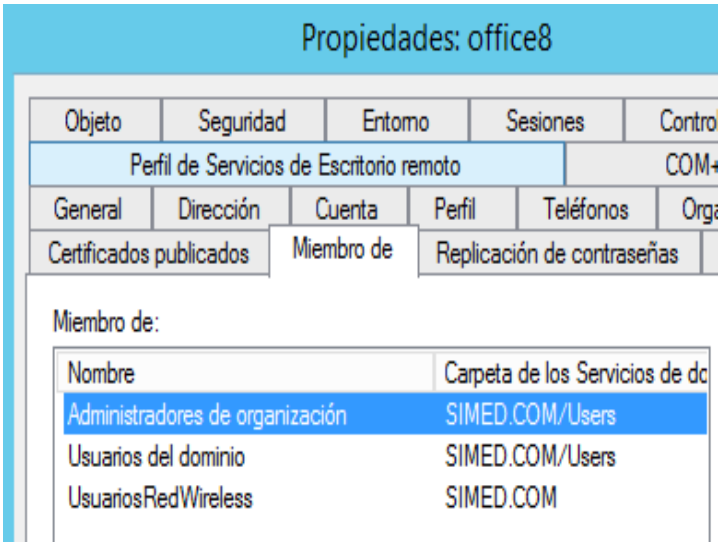


Figura 36. Unión al grupo de administradores de organización a cuenta office8.

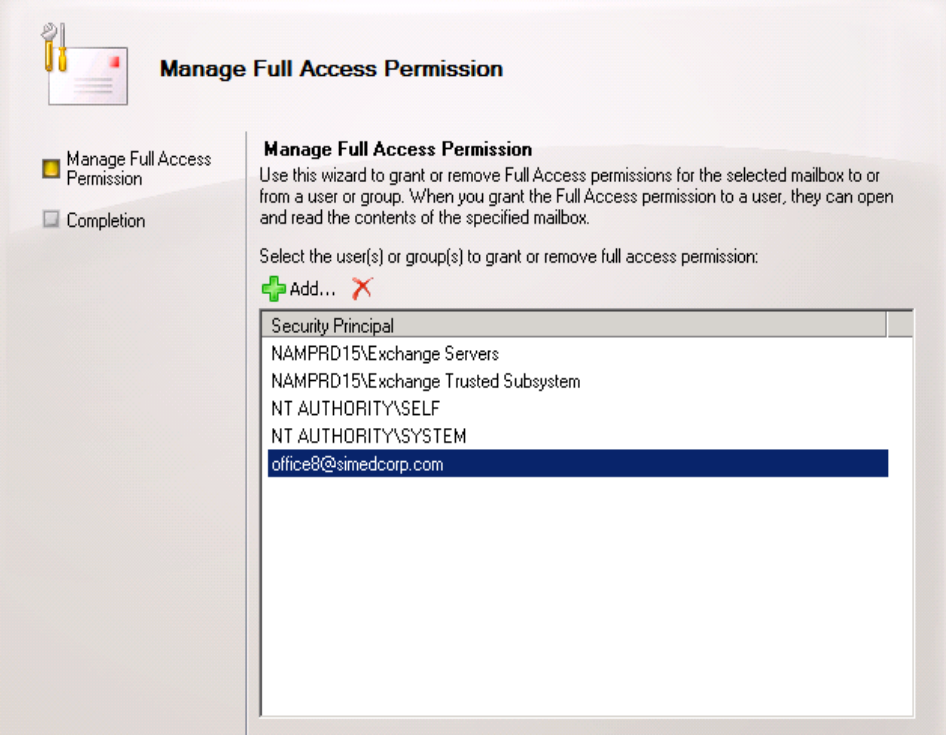


Figura 37. Configuración de permisos sobre buzón en Exchange.

- **Contraseña:**

  Contraseña para el nombre de usuario que se ha usado. Para este caso es la contraseña de la cuenta office8@simedcorp.com

- **Correo de la cuenta de sincronización:**

  Debe ir el correo de la cuenta que se va a usar para la sincronización con Exchange. (office8@simedcorp.com)

- **Habilitar la sincronización**

  Esto permite la sincronización con Exchange u Office 365 para todos los administradores que decidan hacerlo.

- **Pruebe la configuración de Exchange**

  Se tiene una opción para probar las configuraciones realizadas en donde SysAid intenta conectarse a el servidor de Exchange / Office 365 utilizando las credenciales que se han configurado. Se recibe una notificación si la conexión se establece correctamente.

El llenado de todos los campos mencionados se puede observar en la figura 38 a continuación.

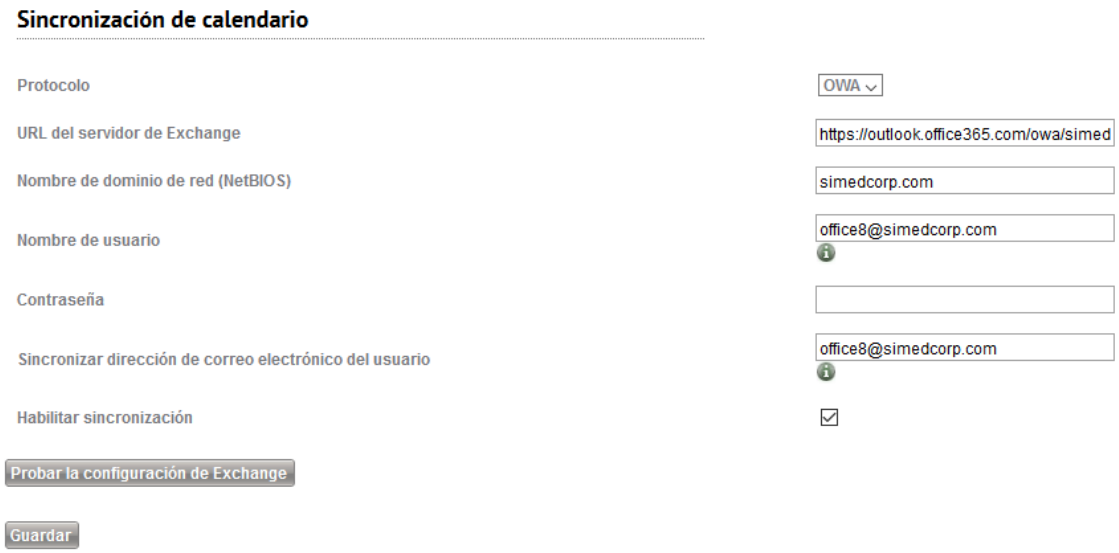


Figura 38. Configuración de la sincronización de calendario de SysAid con Office365.

3.5.8 Despliegue del agente de SysAid.

El Agente de SysAid es una aplicación del lado del cliente que reside en cada uno de sus equipos y se ejecuta silenciosamente en segundo plano (no notará ninguna diferencia de rendimiento después de que se haya instalado). Una vez desplegado, el agente de SysAid tiene muchos beneficios:

- La tecla de acceso directo de SysAid
- Importe automáticamente todas las computadoras en SysAid
- Actualiza automáticamente los perfiles de tus computadoras
- Realizar una sesión de control remoto
- Habilite la supervisión de sus computadoras (con el módulo de supervisión de SysAid).
- Ahorra el tiempo de tener que instalar el agente de computador en computador.
- Ver usuarios en línea.

3.5.8.1 Paquete de implementación MSI usando política de grupo

Una forma de implementar el Agente de SysAid en toda la red es por medio de una política de grupo. Para lo cual se necesita un paquete de implementación de MSI, para descargar este se debe ir a Configuración> Descubrimiento de red> Descargas.

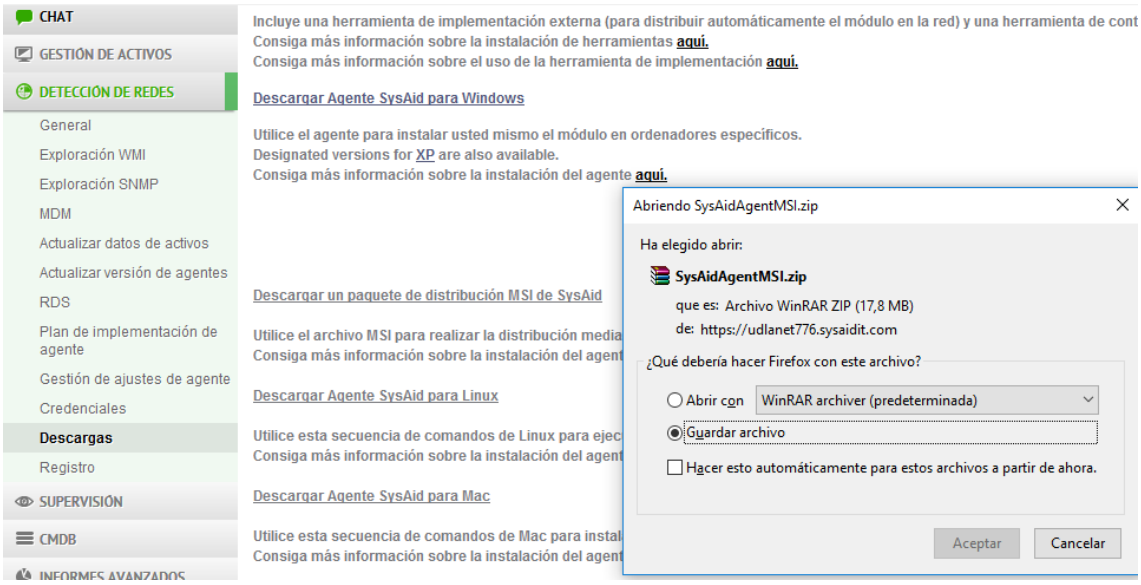


Figura 39. Descarga MSI para agente de SysAid.

Al desplegar el agente usando una política de grupo, se debe crear un archivo de configuración para incluir sus parámetros únicos. Para la creación de este se utilizó Microsoft Orca Los archivos del agente son específicos de la arquitectura. Esta opción está diseñada específicamente para la implementación de políticas de grupo. Los pasos son los siguientes:

1. Abrir SysAidAgent.msi usando Orca y hacer clic en Transformar> Nueva transformación.

2. En el panel Tablas, se debe hacer clic en Propiedad.

3. Se debe modificar al menos los parámetros ACCOUNT, SERIAL y SERVERURL, y también puede modificar los parámetros opcionales en la lista siguiente.

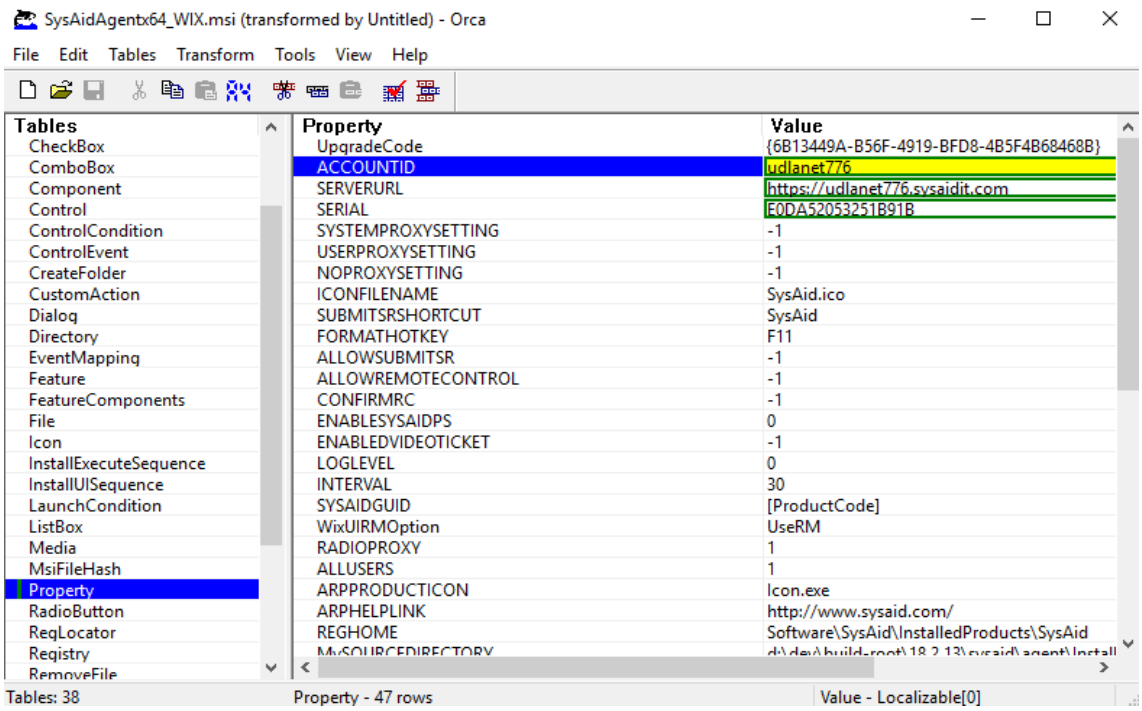


Figura 40. Modificación del paquete MSI con ORCA.

4. Al finalizar hacer clic en Transformar> Generar transformación y se guarda el archivo como SysAidAgentx86.mst para el MSI de 32 bits o SysAidAgentx64.mst para el MSI de 64 bits.

Una vez creado el archivo SysAidAgentx64.mst, este debe ser implementado a través de una política de grupo configurada en el directorio activo de la empresa, para lo cual:

1. Se abre el editor de objetos de política de grupo.
2. Se debe expandir Configuración del equipo> Configuración del software.
3. Desde el menú se da clic derecho, se selecciona Instalación de software> Nuevo> Paquete
4. Seleccionar el archivo SysAidAgent.msi. La ruta al archivo SysAid MSI y MST no debe ser local o a través de una unidad de red. Por el contrario, la ruta debe ser a través de un recurso compartido de red accesible desde cualquier lugar de la red y al que todos tengan al menos permisos de lectura.

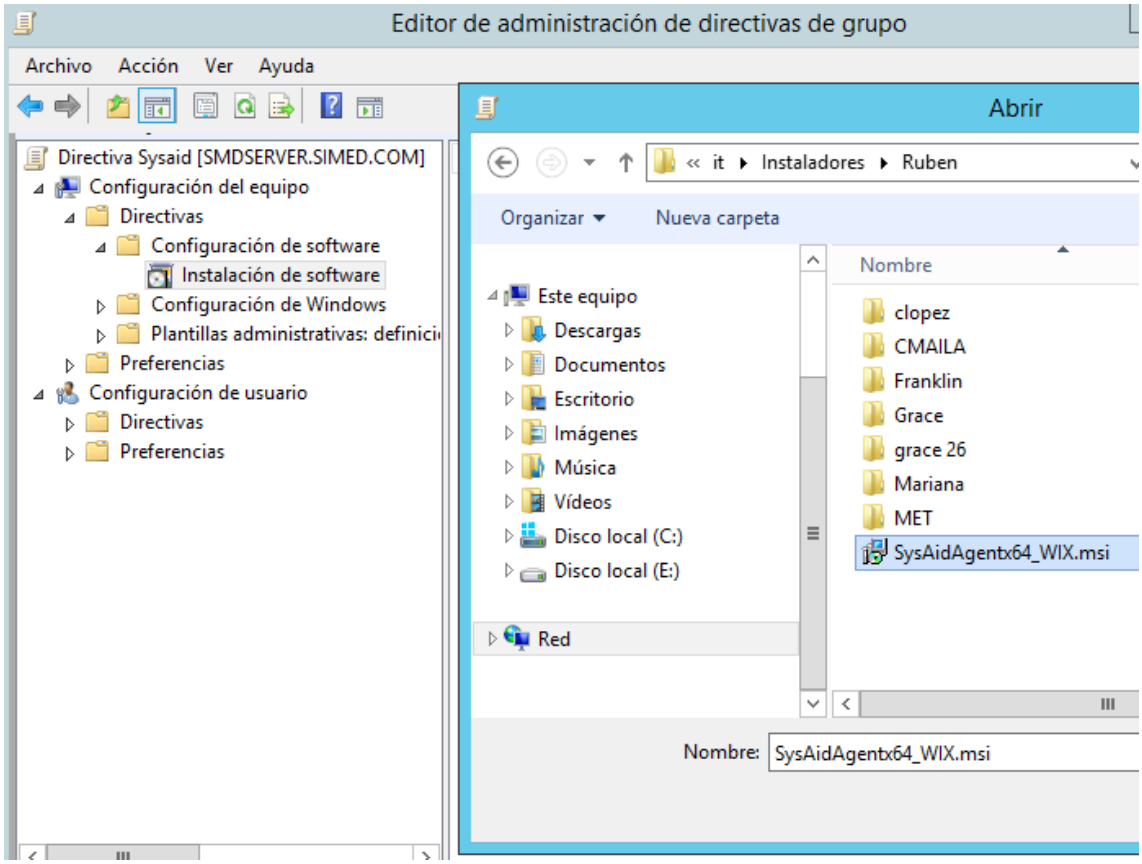


Figura 41. Selección del archivo MSI.

5. En Método de implementación, elegir Avanzado.

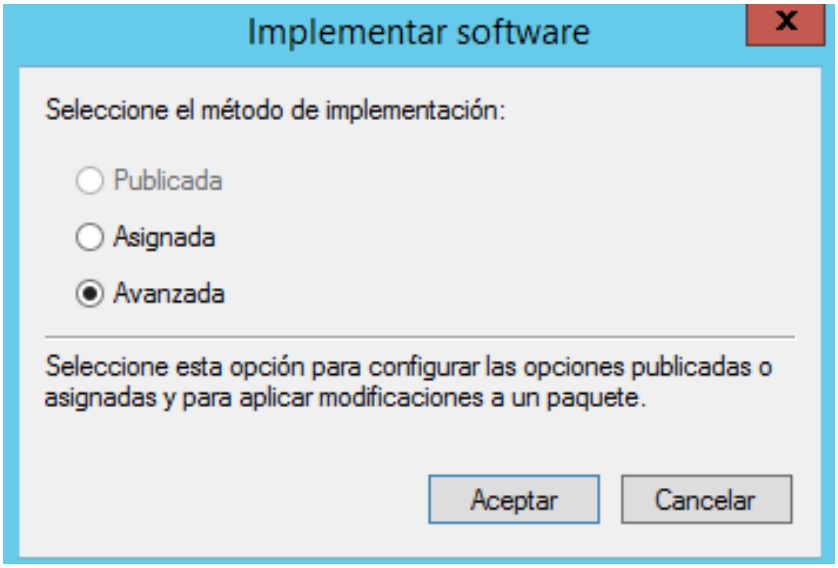


Figura 42. Método de implementación Avanzada.

6. Agregue un nombre para el paquete para una fácil identificación. En este caso se lo nombro SysAid_Agent64.

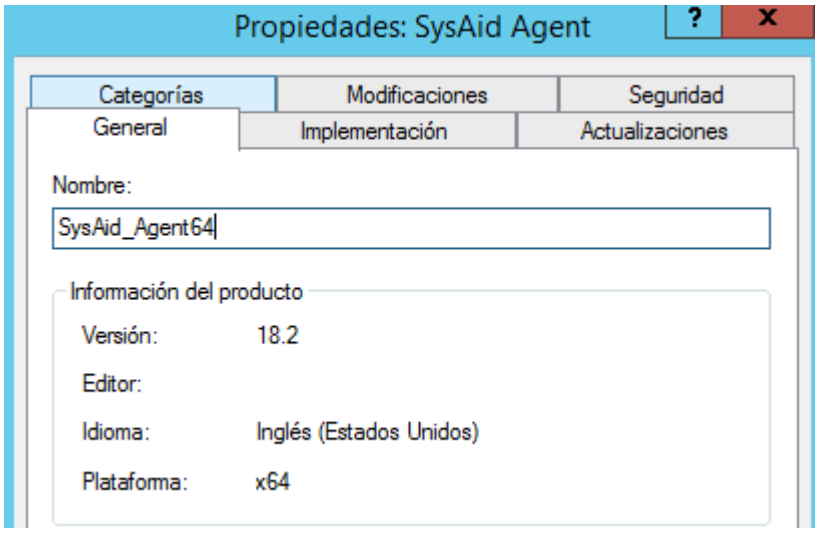


Figura 43. Colocación del nombre para el agente de SysAid.

7. Se cambia a la pestaña Modificaciones y se hace clic en Agregar.

8. Se selecciona el archivo MST creado en los pasos anteriores través de ORCA.

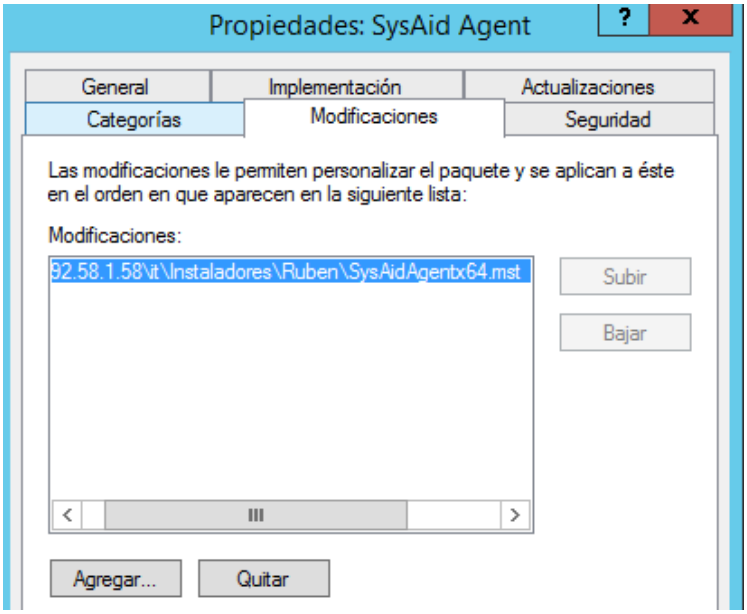


Figura 44. Selección del archivo MST.

Con la implementación de esta política de usuario el agente de SysAid se instalará en todas las computadoras de la organización.

3.5.9 Configuración de la Mesa de Servicios.

La configuración de la mesa de servicio permite controlar varias configuraciones de automatización para la mesa de servicio.

A continuación, hay una breve descripción de cada una de las páginas de configuración.

- Configuración general

  La página de configuración general contiene muchos ajustes misceláneos de la mesa de servicio. Los principales entre estos son los ajustes que controlan cuando se envían notificaciones automáticas por correo electrónico a sus usuarios finales y administradores.

- Categorías

  Los administradores y usuarios finales seleccionan la categoría de su problema cuando envían un nuevo registro de servicio. SysAid viene con una cantidad de categorías de registros de servicio preconfigurados. La pestaña de categorías le permite agregar nuevas categorías y editar categorías existentes.

- Enrutamiento

  Sirve para configurar de antemano que un administrador o grupo administrador en particular manejará una SR (generalmente un incidente o solicitud) en función de su categoría, o según el grupo de usuarios que la haya enviado. Las reglas de enrutamiento permiten especificar que todos los registros de servicio que cumplan con los criterios predefinidos se enrutan automáticamente a un administrador o grupo administrativo en particular.

- Prioridad

  Asignar prioridades a los registros de servicio garantiza que los registros de servicio se trabajen en un orden que tenga sentido para su organización. Las reglas de prioridad le permiten especificar que ciertos SR siempre reciben una prioridad particular. Por ejemplo, los problemas del servidor siempre pueden tener una alta prioridad, y los problemas de su administración ejecutiva pueden tener la más alta prioridad. Si no hay una regla de prioridad que afecte a una nueva SR, se utiliza la prioridad predeterminada de la mesa de servicio.

  También se puede usar la Matriz de Prioridad para calcular la prioridad de un SR en función de su Impacto y Urgencia. Vaya aquí para más información.

- Fechas de vencimiento

  La asignación de fechas de vencimiento a los registros de servicio permite garantizar que siempre se brinde un servicio oportuno a los usuarios. Las reglas de fecha de vencimiento permiten especificar fechas de vencimiento automáticas para sus registros de servicio en función de la categoría, la prioridad y más. El cumplimiento de las fechas de vencimiento se puede rastrear a través de informes y mediante reglas de escalamiento.

- Alertas

  Las alertas permiten especificar qué estados y prioridades activan qué alertas de colores en la lista de *service desk*.

Figura 45. Colores para alertas.

- Reglas de escalada

  - ✓ Notificarle de un registro de servicio vencido.
  - ✓ Notificando nadie trabajó en un registro de servicio activo durante más de una semana.
  - ✓ Se puede reabrir un registro de servicio que se puso en seguimiento cuando llega la fecha de seguimiento.

Se puede usar reglas de escalamiento para hacer todo esto y más opciones automáticamente. Si bien aún se puede usar SysAid sin configurar las reglas de escalamiento, se obtendrá mucho más de la mesa de servicio si se aprovecha todas las opciones de las reglas de escalación.

- Tiempos de funcionamiento

  La introducción de las horas de funcionamiento de la mesa de servicio garantizará que las fechas de vencimiento del registro de servicio se asignen solo durante las horas en que opera la mesa de servicio.

- Temporizadores

  Se especifican temporizadores para de los registros de servicio. SysAid viene con dos temporizadores predeterminados: tiempo para responder y tiempo para reparar. Pero se puede crear temporizadores personalizados para medir métricas de la mesa de servicio.

- Configuración de estado SR

  SysAid permite cambiar automáticamente el estado de un incidente cuando un cambio vinculado, problema o solicitud cambia a un estado

específico. Esta pestaña permite especificar qué estados causan que cambie el estado del incidente vinculado y qué estado recibe el incidente.

3.5.9.1 Categorías de incidentes y solicitudes.

En esta sección se configurarán las categorías planteadas para los incidentes, solicitudes y problemas que se generó en la sección Categorización de Incidentes. En síntesis, las categorías son las siguientes:

- **Categoría de primer nivel:**
  Aquí se encuentra el nivel más general como lo es *software* y *hardware*.

- **Categoría de segundo nivel**:
  Se ha planteado dividir en servidores, estación de trabajo, biométrico, impresoras, POLYCOM, telefonía IP y celulares

- **Categoría de tercer nivel:**
  En esta sección se definirá las categorías subsiguientes a las categorías de segundo nivel tanto de *software* como de *hardware*.

Para configurar las categorías ir Herramientas > Centro de servicio > Categorías, en dicha pestaña, SysAid viene con categorías por defecto que son las más generales que se aplican casi a cualquier empresa, pero para disponer de una configuración totalmente personalizada se decidió configurar categorías propias para que se ajustan a los servicios de TI de la empresa, para lo cual se procedió a eliminar todas las categorías por default de SysAid y a configuró las planteadas en el diseño.

Para crear una nueva categoría clic en Agregar nueva categoría, se abrirá una pantalla donde se debe configurar los tres niveles para la categoría.

En la figura 46 se observa la creación de la categoría “Software”, subcategoría “Biométrico” y categoría de tercer nivel “Reporte de asistencia”.

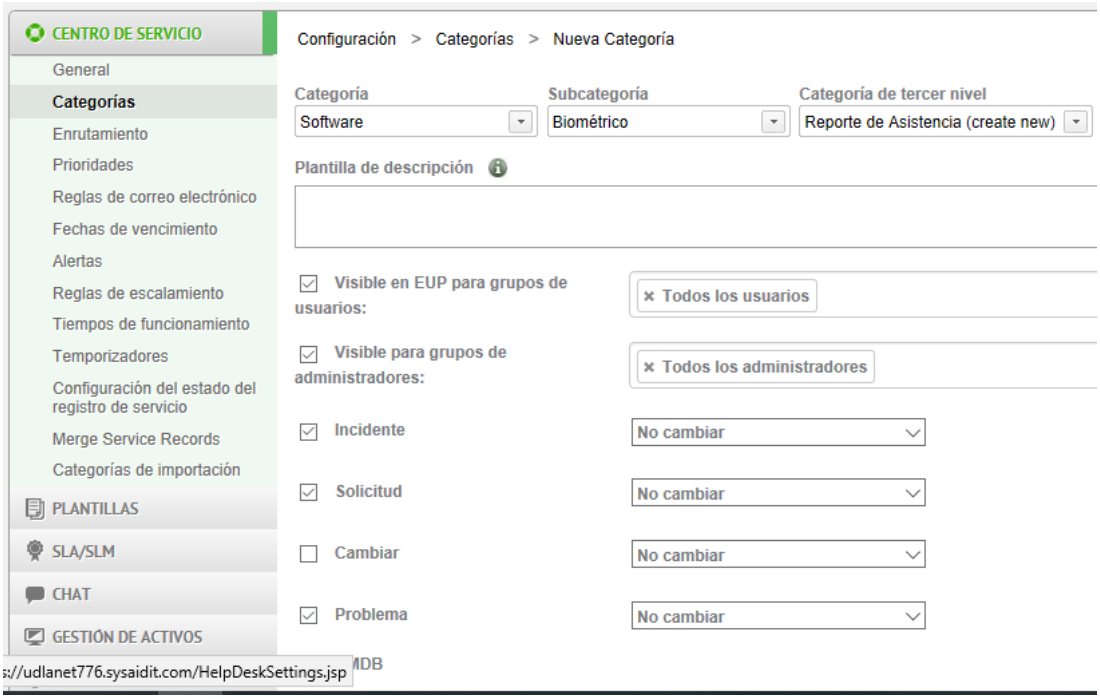


Figura 46. Creación de categorías en SysAid.

Después de haber culminado el proceso se obtiene un listado con todas las categorías creadas como se puede observar en la figura 47 a continuación.

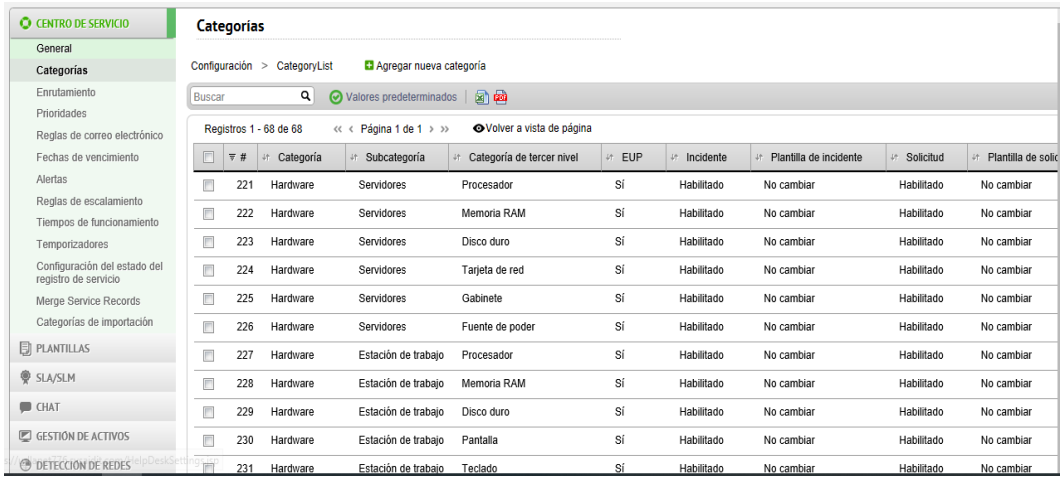


Figura 47. Vista de las categorías creadas.

3.5.9.2 Enrutamientos.

Las reglas de enrutamiento permiten a SysAid asignar automáticamente registros de servicio a los administradores o grupos de administradores sin tener que mirarlos. Esto es útil en los casos en que sabe de antemano quién trabajará en un registro de servicio específico.

El enrutamiento puede basarse en:

- Acuerdo (solo módulo SLA / SLM): este es el SLA del usuario de la solicitud.

- Compañía: esta es la compañía a la que pertenece el usuario de la solicitud del registro del servicio.

- Grupo de usuarios: este es el grupo de usuarios al que pertenece el usuario de la solicitud del registro del servicio.

- Categoría: esta es la categoría del registro de servicio.

La opción que se usó es por categoría en donde de acuerdo con esta se redirigirán el registro de servicio al técnico responsable de la mesa de servicios en base al perfil y habilidades que maneja dentro de la empresa. De acuerdo con esto las reglas de redirección van a dirigirse a los técnicos de nivel 1:

- Javier Villalba
- Rubén Clavijo
- Estefanía Jiménez

A continuación, en la Tabla 30 está colocado las responsabilidades de cata técnico según las categorías:

Tabla 28.

Enrutamiento de servicios a técnicos según categorías.

Técnico	Cargo	Categoría	Sub - Categoría
NIVEL DE SOPORTE 1			
Javier Villalba	Asistente de TI	Software	Aplicaciones empresariales
Rubén Clavijo	Asistente de TI	• Hardware • Software	• Estación de trabajo • Biométrico • Impresora • POLYCOM
Estefanía Jiménez	Asistente de TI	• Hardware • Software	• VoIP • Celular
NIVEL DE SOPORTE 2			
Andrés Jurado	Especialista de TI	Software	Aplicaciones empresariales
Carlos Yoncón	Gerente de TI	• Hardware • Software	• Servidores • Equipos de red

Para configurar el enrutamiento de registros de servicio ir a Herramientas > enrutamiento > agregar nueva regla de enrutamiento. En la nueva venta que se despliega se configura los siguientes campos:

- Se selecciona si la regla se habilitará o no utilizando la casilla de verificación. Si una regla está deshabilitada, no tendrá ningún efecto.

- Se seleccione el disparador para la regla. En este caso es por categoría.

- Se seleccione el administrador y / o grupo de administradores deseados. Por último se debe hacer clic en agregar al final de la fila.

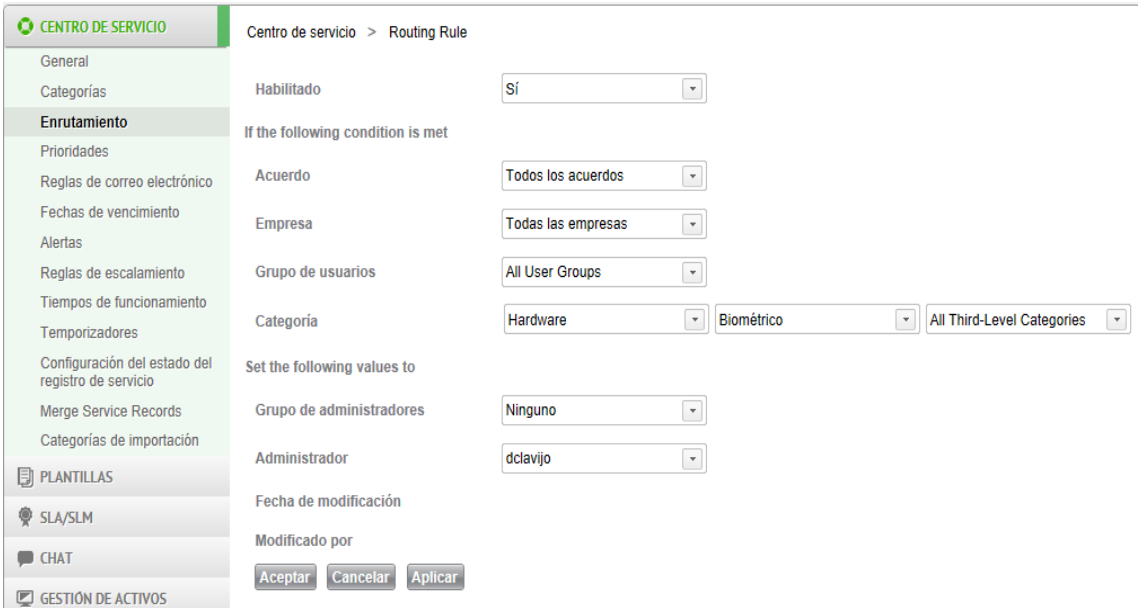


Figura 48. Regla de enrutamiento para el técnico Rubén Clavijo en la categoría Biométrico y todas las subcategorías correspondientes.

Routing Rules List

Centro de servicio > Routing Rules Add New Routing Rule

Registros 1 - 15 de 15 « ‹ Página 1 de 1 › » Volver a vista de página

Execution Order	Habilitado	Acuerdo	Empresa	Grupo de usuarios	Categoría	Subcategoría	Categoría de tercer nivel	Grupo de administradores	Administrador
1	Sí	Todos los	Todos	Todos	Software	Teléfono IP	Todos	none	ejimenez
2	Sí	Todos los	Todos	Todos	Software	POLYCOM	Todos	none	dclavijo
3	Sí	Todos los	Todos	Todos	Software	Impresora	Todos	none	dclavijo
4	Sí	Todos los	Todos	Todos	Software	Estación de	Todos	none	dclavijo
5	Sí	Todos los	Todos	Todos	Software	Celular	Todos	none	ejimenez
6	Sí	Todos los	Todos	Todos	Software	Biométrico	Todos	none	dclavijo
7	Sí	Todos los	Todos	Todos	Software	Aplicaciones	Todos	none	jvillalba
8	Sí	Todos los	Todos	Todos	Hardware	Teléfono IP	Todos	none	ejimenez
9	Sí	Todos los	Todos	Todos	Hardware	Servidores	Todos	none	cyoncon
10	Sí	Todos los	Todos	Todos	Hardware	POLYCOM	Todos	none	dclavijo
11	Sí	Todos los	Todos	Todos	Hardware	Impresora	Todos	none	dclavijo
12	Sí	Todos los	Todos	Todos	Hardware	Estación de	Todos	none	dclavijo
13	Sí	Todos los	Todos	Todos	Hardware	Celular	Todos	none	ejimenez
14	Sí	Todos los	Todos	Todos	Hardware	Biométrico	Todos	none	dclavijo

Figura 49. Listado de reglas de enrutamiento de registros de servicio.

Lo que se obtiene como resultado después de realizar esta configuración es que cuando un usuario final cree un incidente o una solicitud de servicio esta se asigne automáticamente a un técnico responsable de dicha categoría, así se automatiza el servicio.

3.5.9.3 Prioridades.

En esta sección se especificará las condiciones bajo las cuales un registro de servicio recibirá una prioridad. En SysAid se puede crear una regla de prioridad basada en:

- Acuerdo: el acuerdo es determinado por el usuario de la solicitud.
- Empresa: la empresa está determinada por el usuario de la solicitud Departamento (por ejemplo, Finanzas).
- Grupo de activos (por ejemplo, servidores).
- Matriz de prioridades para calcular automáticamente la prioridad para un registro de servicio.

De las opciones mencionadas se trabajará con la matriz de prioridades, como se mencionó anteriormente el usuario final escogerá la urgencia para el registro de servicios (crítico, alto, medio, bajo), el técnico al cual se le asigna el registro de servicio desde el portal de administrador debe seleccionar el impacto de dicho registro de servicio de acuerdo con la categoría a la que pertenezca y basado en los términos establecidos en la sección Gestión de Nivel de Servicio (SLM).

En SysAid por default vienen configuradas listas de impactos, urgencias y prioridades, pero están en inglés y manejan campos diferentes. A continuación, se muestra un ejemplo de lista de urgencias por defecto que tiene SysAid.

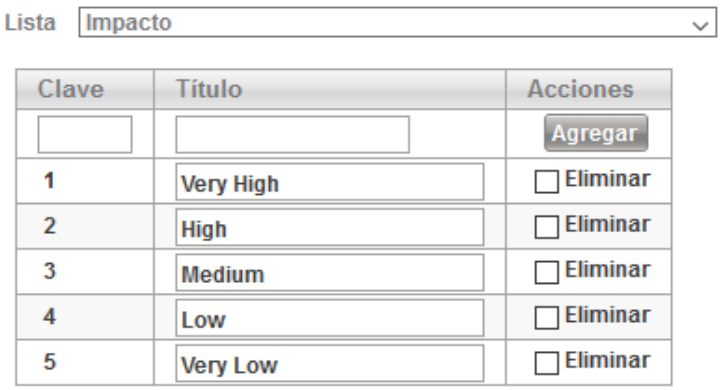


Figura 50. Lista por defecto de impacto en SysAid.

Como se puede observar existen 5 niveles de impacto, pero lo planteado en el SLM de la empresa es el manejo de 4 niveles. Por lo cual en primera instancia se debe modificar los nombres y eliminar el quinto nivel en las listas de urgencias, impactos y prioridades. Para esto ir a Herramientas > personalizar > listas > seleccionar la lista a personalizar. Después corregir nombres y eliminar el quinto nivel. En la figura 51 a continuación se muestra un ejemplo de la lista de urgencias modificada.

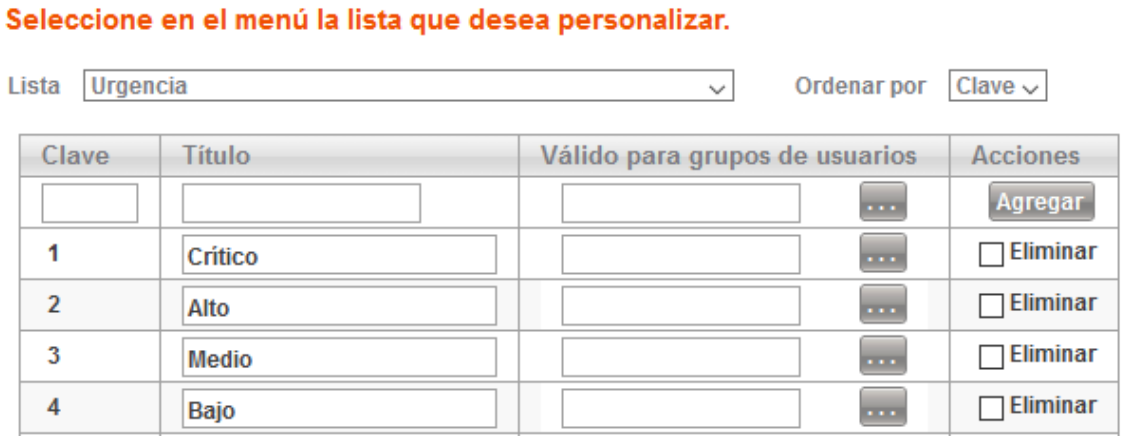


Figura 51. Modificación de lista de urgencias.

Para la configuración del cuadro de prioridades en SysAid se debe ir a la siguiente ruta Herramientas > Centro de Servicios > Prioridades una vez en esa pantalla se procede a configurar el cuadro. En la figura 52 a continuación se puede observar el cuadro de prioridades configurado en SysAid.

Habilitado	Acuerdo	Empresa	Impacto	Urgencia		Prioridad
☑	Todos los acuerdos	Todas las empresas	Todos los impactos	Todas las urgencias		Crítico
☑	Todos	Todos	Bajo	Bajo		Bajo
☑	Todos	Todos	Bajo	Medio		Bajo
☑	Todos	Todos	Bajo	Alto		Medio
☑	Todos	Todos	Bajo	Crítico		Medio
☑	Todos	Todos	Medio	Bajo		Bajo
☑	Todos	Todos	Medio	Medio		Medio
☑	Todos	Todos	Medio	Alto		Medio
☑	Todos	Todos	Medio	Crítico		Alto
☑	Todos	Todos	Alto	Bajo		Medio
☑	Todos	Todos	Alto	Medio		Medio
☑	Todos	Todos	Alto	Alto		Alto
☑	Todos	Todos	Alto	Crítico		Crítico
☑	Todos	Todos	Crítico	Bajo		Medio
☑	Todos	Todos	Crítico	Medio		Alto
☑	Todos	Todos	Crítico	Alto		Crítico
☑	Todos	Todos	Crítico	Crítico		Crítico

Figura 52. Cuadro de prioridades en SysAid.

3.5.9.4 Tiempos de funcionamiento.

Un conjunto de tiempos de operación especifica los días y horas de funcionamiento de la mesa de ayuda para la empresa.

Es importante en SysAid la configuración de esta sección puesto que las fechas de vencimiento, las reglas de escalamiento y los temporizadores utilizarán los tiempos de operación que proporcione aquí.

La configuración que se va a realizar en esta sección es de acuerdo con lo definido en la sección de Escalas de tiempo y priorizaciones donde se indica que el horario de atención será de lunes a viernes de 8:00 a 19:00.

Para esta configuración dirigirse a Herramientas > Centro de servicio > Tiempos de funcionamiento, en este seleccionar los días de funcionamiento con los horarios correspondientes, en la figura 53 se puede observar esta configuración.

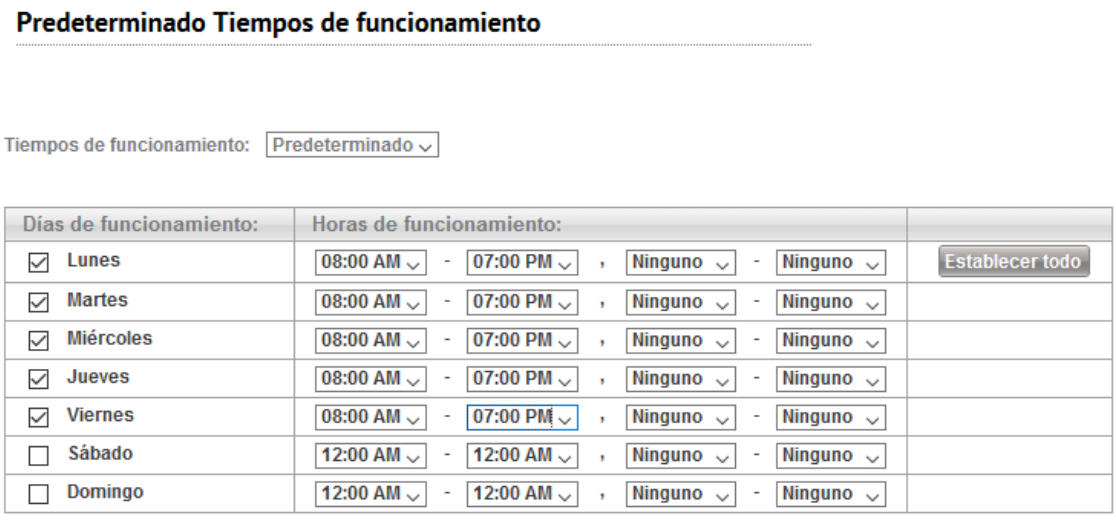


Figura 53. Tiempos de funcionamiento de la mesa de servicios.

3.5.9.5 Fechas de vencimiento registros de servicios.

Las reglas de fecha de vencimiento asignan automáticamente fechas de vencimiento a los registros de servicio. Cualquier registro de servicio que coincida con todos los requisitos en una de las reglas de fecha de vencimiento recibirá automáticamente la fecha de vencimiento que especifique.

Cálculo de fechas de vencimiento:

El cálculo de las fechas de vencimiento se basa en los tiempos de operación del acuerdo o compañía específica del usuario de la solicitud. Si, por ejemplo, se envía un registro de servicio con un período de vencimiento de 6 horas, pero solo quedan 3 horas de tiempo de operación en el día, la fecha de vencimiento será 3 horas después del inicio del siguiente día de funcionamiento.

Para la configuración de las fechas de vencimiento se basa en lo definido anteriormente en la sección Escalas de tiempo y priorizaciones, en donde se define los tiempos de respuesta y escalamiento de un registro de servicio que debe cumplir la mesa de servicios de acuerdo con la prioridad que este tenga. Para esto ir a Herramientas > Centro de servicio > Fechas de vencimiento > Agregar nueva fecha de vencimiento, en la ventana desplegada se debe seleccionar el tipo de urgencia y escribir el tiempo en horas de respuesta a los servicios que tengan esa prioridad.

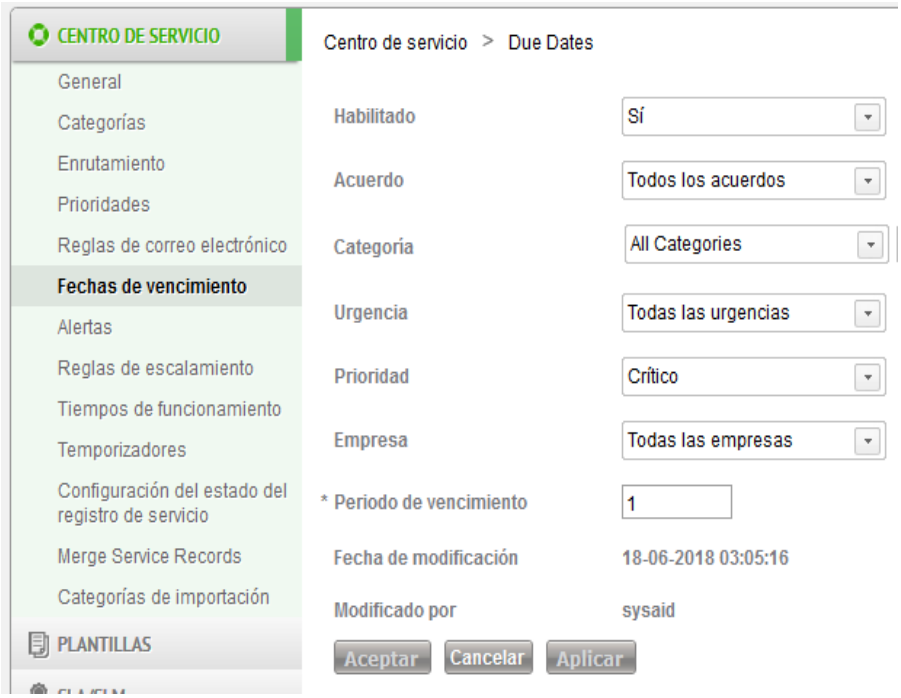


Figura 54. Configuración de tiempo de respuesta a los servicios con prioridad crítica.

Este proceso se debe realizar con todas las prioridades que se tengan definidas. Después de configurar estos tiempos al momento en que un usuario final cree un registro de servicio y este sea asignado automáticamente al técnico responsable de la mesa de servicios, el técnico en su portal de administración observará que dicho servicio asignado cuenta con una fecha de vencimiento.

En la figura 55 a continuación se puede observar los tiempos definidos en el sistema.

Registros 1 - 4 de 4

Execution Order	Prioridad	Empresa	Periodo de vencimiento
4	Crítico	Todos	1 Horas
3	Alto	Todos	2 Horas
2	Medio	Todos	4 Horas
1	Bajo	Todos	8 Horas

Figura 55. Tiempos de respuesta definidos a prioridades.

3.5.9.6 Reglas de escalamiento.

Se puede indicar los criterios según los cuales SysAid escala un registro de servicio. Esto provoca que el registro de servicio ejecuta automáticamente una acción concreta. Por ejemplo, si un registro de servicio sigue abierto después de un mes, quizá sea conveniente que SysAid lo notifique automáticamente a un administrador o grupo determinado, o que SysAid reasigne automáticamente el registro de servicio.

De acuerdo con el personal técnico de TI de la empresa los niveles de escalamiento funcional se darán de la siguiente forma como se observa en la tabla 31:

Tabla 29.

Niveles de escalamiento funcional.

Categoría	Sub categoría	Técnico de nivel 2 de escalamiento
Software	Aplicaciones empresariales	Andrés Jurado (Especialista de TI)
Hardware **Software**	• Estación de trabajo • Biométrico • Impresora • POLYCOM • VoIP • Celular • Servidores	Carlos Yoncón (Gerente de TI)

Para configurar las reglas de escalamiento ir a Herramientas > Centro de servicio > Reglas de escalamiento y dar clic en crear nueva regla de escalamiento. Se desplegará una nueva ventana donde se debe indicar:

- El nombre de la regla.
- Categoría, subcategoría y categoría de tercer nivel.
- Tipo de solicitud de servicio ya sea incidente o solicitud.
- El estado, en este caso se creará reglas para registros de servicio que tengan un estado de activo.
- El tiempo cuando se escala, este tiempo se basa al propuesto en la sección Escalas de tiempo y priorizaciones.
- Se elige al técnico al cual se va a reasignar en la solicitud o el incidente.

Para dar una idea de la configuración mencionada se realizará la regla de escalamiento para la categoría “software” con subcategoría “Aplicaciones empresariales”, que en primera instancia al ser creado un incidente en dicha categoría se le asigna al técnico Javier Villalba de nivel 1 de la mesa de servicios

y que de acuerdo con la prioridad de la misma y los tiempos de respuesta definidos (1 hora crítico, 2 horas alto, 4 medio,8 horas bajo) el escalamiento se dará cuando se llegue a la fecha de vencimiento de dicho registro, por ejemplo es decir si a 1 hora para un incidente o solicitud no se llegó a una solución se escalará al técnico especialista de TI Andrés Jurado de nivel 2 de la mesa de servicios. La configuración de esta regla se la puede observar en la figura 56.

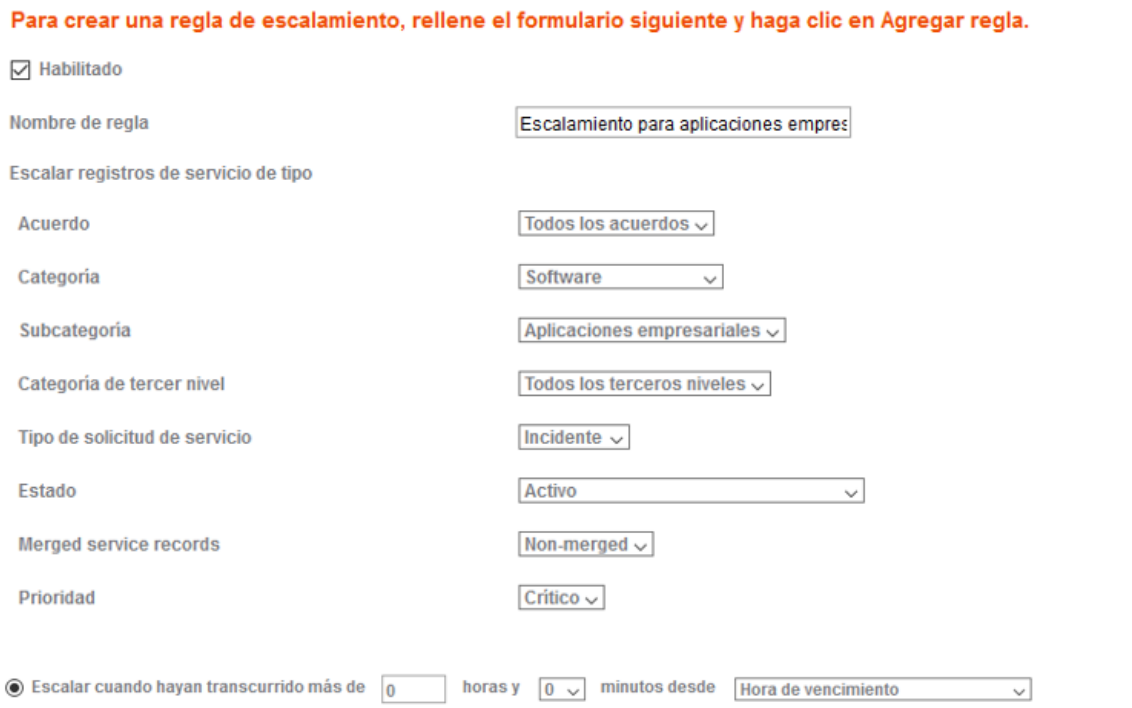
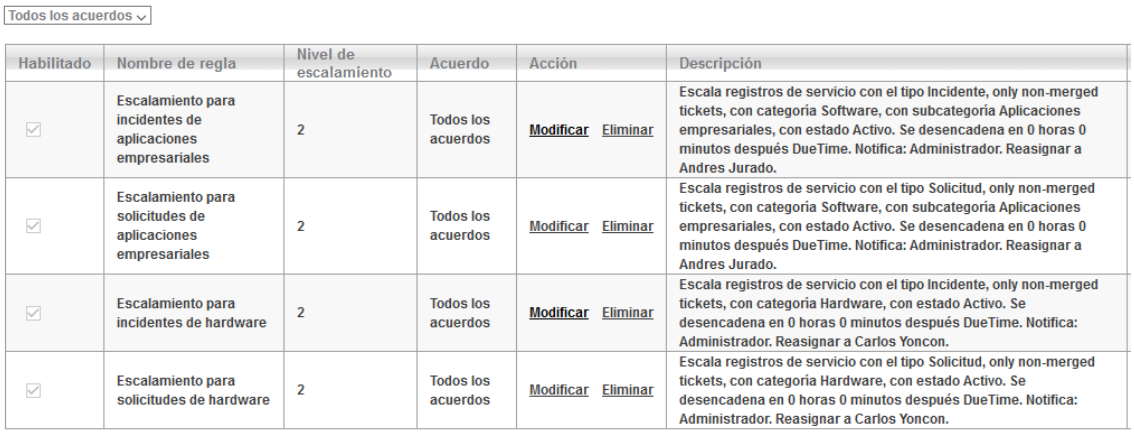


Figura 56. Regla de escalamiento para aplicaciones empresariales con prioridad crítica.



Habilitado	Nombre de regla	Nivel de escalamiento	Acuerdo	Acción	Descripción
☑	Escalamiento para incidentes de aplicaciones empresariales	2	Todos los acuerdos	Modificar Eliminar	Escala registros de servicio con el tipo Incidente, only non-merged tickets, con categoría Software, con subcategoría Aplicaciones empresariales, con estado Activo. Se desencadena en 0 horas 0 minutos después DueTime. Notifica: Administrador. Reasignar a Andres Jurado.
☑	Escalamiento para solicitudes de aplicaciones empresariales	2	Todos los acuerdos	Modificar Eliminar	Escala registros de servicio con el tipo Solicitud, only non-merged tickets, con categoría Software, con subcategoría Aplicaciones empresariales, con estado Activo. Se desencadena en 0 horas 0 minutos después DueTime. Notifica: Administrador. Reasignar a Andres Jurado.
☑	Escalamiento para incidentes de hardware	2	Todos los acuerdos	Modificar Eliminar	Escala registros de servicio con el tipo Incidente, only non-merged tickets, con categoría Hardware, con estado Activo. Se desencadena en 0 horas 0 minutos después DueTime. Notifica: Administrador. Reasignar a Carlos Yoncon.
☑	Escalamiento para solicitudes de hardware	2	Todos los acuerdos	Modificar Eliminar	Escala registros de servicio con el tipo Solicitud, only non-merged tickets, con categoría Hardware, con estado Activo. Se desencadena en 0 horas 0 minutos después DueTime. Notifica: Administrador. Reasignar a Carlos Yoncon.

Figura 57. Listado de reglas de escalamiento.

3.5.10 Modelo de incidentes en SysAid.

Como lo recomienda ITIL v3 debe existir modelos de incidentes que facilitan al usuario final la creación de estos, puesto que siempre existen incidentes repetitivos es útil disponer de una plantilla que, al crear un incidente nuevo todos los campos del incidente se completarán automáticamente tal como aparecen en la plantilla. Como se describió en la sección Modelo de incidente estas plantillas deben tener parámetros como:

- Nombre de la plantilla o modelo
- Título del incidente
- Categoría, subcategoría, tercer nivel de categoría.
- Una descripción
- Urgencia, impacto, prioridad
- Responsable de solución
- Pasos para llegar a la solución

Para configurar modelos de incidentes en SysAid ir a Herramientas > Plantillas > Plantilla de incidente, agregar nueva plantilla. En la figura 58 se configura un modelo para un incidente común. se configuró con los siguientes parámetros:

- Título de la plantilla: Atasco de papel
- Título del incidente: Atasco de papel en la impresora de bodega
- Categoría: hardware
- Subcategoría: impresora
- Categoría de tercer nivel: alimentador de hojas
- Descripción: cuando se manda a imprimir las hojas se atascan
- Urgencia: alto
- Impacto: medio
- Prioridad: medio
- Asignado a: Rubén Clavijo
- Solución: abrir soporte de hojas y retirar hoja atascada

Figura 58. Modelo de incidente para atasco de papel en impresora.

3.5.11 Modelo de problemas en SysAid.

Como se supone que cada problema de un tipo determinado sigue el mismo proceso que todos los demás problemas de ese tipo, los problemas se basan en las plantillas. La lista de plantillas de problemas permite crear y modificar plantillas de problemas.

El proceso para configurar modelos de problemas es muy similar al modelo de incidentes, para acceder a este se dirige a Herramientas > Plantillas > Plantillas de problemas. A continuación, en la figura 59 está un ejemplo para modelos de problemas con el lector de huellas del biométrico.

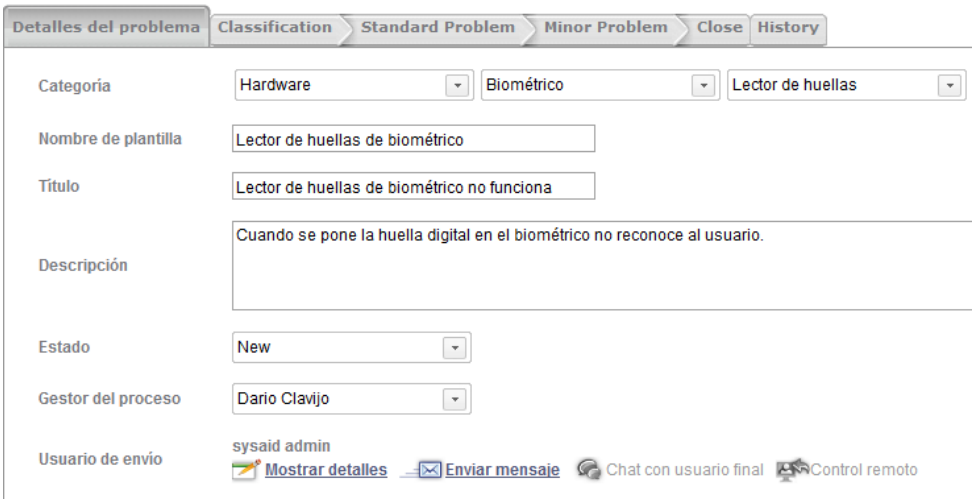


Figura 59. Modelo de problemas para lector de huellas del biométrico.

4. Capítulo IV. Diseño e Implementación del Sistema de Respaldos.

En este capítulo se realizará en primera instancia el diseño de la Política de Respaldos de la empresa en donde se especificará:

- Servidores, aplicaciones, bases de datos y usuarios críticos para la empresa por la información que manejan.

- Se definirá cómo deben darse los respaldos de dicha información de forma local y en un ambiente *cloud*.

- Se establecerá horarios en los que debe darse los respaldos.
- Tipo de respaldo a usarse.
- Definición del personal responsables para realizar y monitorear los respaldos.
- Definirá como es el proceso de restauración de la información tanto para bases de datos, servidores y usuarios.

Después de definir dichos parámetros de la Política de Respaldos se realizará un dimensionamiento a nivel de capacidades de almacenamiento que manejan los servidores, bases de datos y usuarios para determinar cuánto almacenamiento realmente se necesita contratar en la nube.

Se analizará que herramientas existen en el mercado de respaldos en la nube que cumplan los parámetros establecidos, qué servicios ofrecen, se estudiará los valores comerciales manejan cada una y finalmente se hará la elección de la que más convenga para los propósitos de la empresa.

Se implementará la herramienta seleccionada, se configurará de acuerdo con lo parametrizado para en el Capítulo V realizar las respectivas pruebas de funcionamiento.

4.1 Diseño de la Política de Respaldos de la Información de Servidores.

Como se mencionó en el apartado 2.2 Situación actual del Sistema de Respaldos, en la empresa solo se tiene definida una política para respaldar las bases de datos, pero no se toma en cuenta la información de servidores y todo lo que esto implica como lo son:

- Carpetas de configuraciones de aplicaciones.
- Ficheros de información.

Información vital para procesos de restauración de sistemas y aplicaciones puesto que no solo se necesita las bases de datos para levantar dichos servicios, sino que también las configuraciones necesarias para su funcionamiento. Por tal motivo en esta sección se definirá:

1. Servidores y aplicaciones críticos para la operación de la empresa.
2. Cuál es el volumen de datos ocupado en disco duro de todos los servidores de la empresa.
3. Se definirá que se debe respaldar.
4. Se establecerá que tipo de respaldo en la nube se aplicará para dicha información ya sea completo, incremental o diferencial.
5. Se definirá los horarios y frecuencia de cuando realizar los respaldos.

4.1.1 Características de los servidores y aplicaciones de la empresa

En la empresa se cuenta con un total de 18 servidores de los cuales 7 son virtuales y trabajan a través de Hyper-V, en la tabla 32 se encuentra un detalle de cada servidor y la aplicación que trabaja en ellos.

Tabla 30.

Detalle características de los servidores de la empresa.

#	S. O	NOMBRE	APLICACIÓN	MODELO	PROCESADOR	DISCO (Gb)	RAM (Gb)
SERVIDORES FÍSICOS							
1	W. SERVER 2008 X64	HORUS	APLICATIVO GP ECUADOR	HP PROLIANT DL380P GEN 8	INTEL XEON	1000	64
2	W. SERVER 2012 X64	SMDSERVER	ACTIVE DIRECTORY	HP PROLIANT DL160 GEN 9	INTEL XEON	2000	16
3	W. SERVER 2008 X64	MAILSERVER	EXCHANGE 2010	HP PROLIANT ML150 G6	INTEL XEON	1250	10
4	W. SERVER 2012 X64	THANATOS	PRTG	HP PRODESK 400	INTEL CORE I3	500	8
5	W. SERVER 2016 X64	SRVUIOBIO01	BIOMÉTRICOS	HP PRODESK 400	INTEL CORE I7	500	4
6	CENTOS 5	SRVFIREWALL	FIREWALL	PC-SERVER	INTEL CORE I3	1000	16
7	W. SERVER 2012 X64	SRVUIOFILE	FILESERVER	HP PROLIANT MICROSERVER GEN 8	INTEL XEON	1000	4
8	W. SERVER 2016 X64	SRVGYEIMP01	PRINTSERVER GYE	HP PRODESK 400	INTEL CORE I7	500	8
9	W. SERVER 2008 X64	SRVCUEIMP01	PRINTSERVER CUE	HP PRODESK 400	INTEL CORE I7	500	8
11	W. SERVER 2007 X64	ORION	Hyper-V	HP PROLIANT DL380P GEN 8	INTEL XEON	6000	128

4.1.2 Definición de los servidores críticos para la empresa

De acuerdo con el análisis de las funciones que cumplen cada servidor en la empresa se ha definido los siguientes servidores críticos que se considerarán para respaldar su información en la nube. Esta selección se dio en base a los servicios que brindan y el impacto que tiene en la operación de la empresa la falta de continuidad de dichos servicios. En la tabla 33 a continuación se en lista los servidores críticos considerados, la funcionalidad que cumple, qué aplicación empresarial trabaja sobre este, el tamaño en disco que está usado actualmente y el impacto que tiene sobre la operación de la empresa.

Tabla 31.

Tamaño total de almacenamiento ocupado en disco por los servidores críticos de la empresa.

#	NOMBRE	APLICACIÓN	USO DE DISCO ACTUAL (Gb)	IMPACTO
1	HORUS	APLICATIVO GP ECUADOR	438	CRÍTICO
2	OMEGA	APLICATIVO GP PERÚ	18	CRÍTICO
3	OSIRIS	SERVIDOR DE BASE DE DATOS	85	CRÍTICO
4	ICARO	Aplicaciones empresariales: PROGRESS 360 MOVIMIENTO DE EQUIPOS PLANIFIACIÓN INVENTARIO GESTIÓN GENERA	37	CRÍTICO
5	SRVUIOFILE	FILESERVER	500	MEDIO
6	SMDSERVER	ACTIVE DIRECTORY	24	MEDIO
7	MAILSERVER	SERVIDOR DECORREO	1000	ALTO
Tamaño total de almacenamiento ocupado por los servidores críticos			1664	

De los cálculos realizados y considerando una escalabilidad de los datos en el transcurso de los próximos años se puede determinar que la empresa para cubrir sus necesidades de respaldos necesita 2 TB de espacio en la nube.

4.1.3 Definición de directorios a respaldar por servidor.

La restauración de un sistema de acuerdo con su tipo es variada y se tiene distintas formas de realizarla, por lo cual se debe definir que carpetas, archivos, configuraciones son las necesarias para su restauración. Por lo cual se ha clasificado a los servidores críticos de acuerdo con el tipo se sistema y función.

- Servidores donde corre el aplicativo ERP de la empresa.
- Servidor de base de datos
- Servidor donde corren aplicaciones empresariales.
- Servidor de directorio activo.
- Servidor de archivos
- Servidor de correos

4.1.3.1 Información que respaldar de los servidores HORUS y OMEGA para la restauración del aplicativo Microsoft Dynamics GP.

El proceso para restaurar Microsoft Dynamics GP a través de respaldos de datos es el siguiente:

1. Instalar el aplicativo en un servidor.
2. Restaurar las bases de datos del aplicativo.
3. Restaurar los archivos de configuración del aplicativo.

Cómo se puede observar para la restauración de este aplicativo solo se tiene que la base de datos usada y la carpeta de configuraciones.

Las bases de datos de la aplicación se encuentran en el servidor OSIRIS, el mismo que se respalda por separado, con lo cual el único respaldo a realizar en el servidor del aplicativo es de la carpeta configuraciones. En la Figura 60 se puede observar el directorio mencionado el cual se llama “Microsoft Dynamics” y se encuentra en “archivos de programa” dentro del disco C, esta es la carpeta que será respaldada por la solución *cloud*.

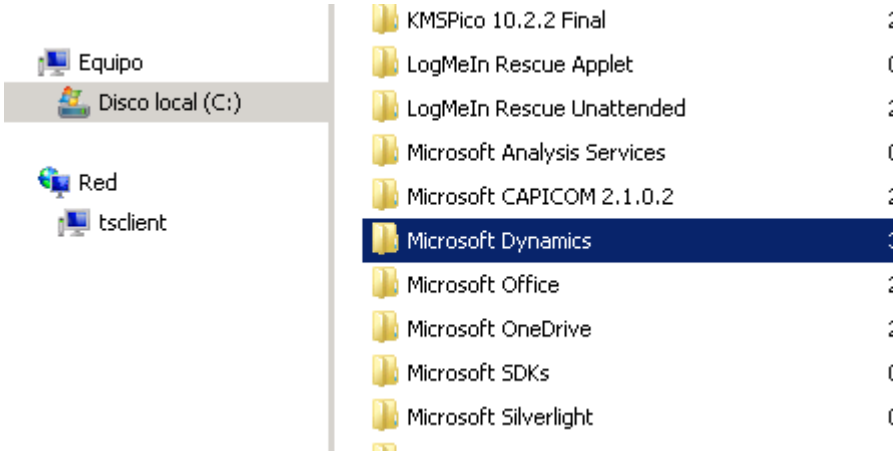


Figura 60. Directorio de configuraciones de GP.

Por lo tanto, no se va a realizar un respaldo de todo el servidor en la nube sino solo de dichas carpetas.

En la tabla 34 a continuación se define el directorio y la ruta de la cual se va a respaldar información en la nube del servidor HORUS y OMEGA.

Tabla 32.

Ruta de la carpeta de configuraciones de GP Ecuador y Perú.

#	NOMBRE SERVIDOR	RUTA CARPETA DE CONFIGURACIONES DEL APLICACTIVO
1	HORUS	C:\Program Files (x86)\Microsoft Dynamics
2	OMEGA	C:\Program Files (x86)\Microsoft Dynamics

De tal forma se establece que estas son las rutas y carpetas por respaldar en la nube de cada servidor.

4.1.3.2 Información que respaldar del servidor ICARO para la restauración de las aplicaciones empresariales.

En este servidor corren aplicaciones web publicadas a través de *Microsoft Internet Information Services,* por lo cual para sus restauraciones se debe realizar el siguiente proceso.

1. Levantar el servicio de *Microsoft Internet Information Services* en un servidor.

2. Restaurar las bases de datos del cada una de las aplicaciones.

3. Restaurar los archivos de configuración de cada una de las aplicaciones.

4. Publicar las aplicaciones en *Microsoft Internet Information Services.*

Por lo cual de igual forma que con los servidores del aplicativo Microsoft Dynamics GP para las restauraciones de estas aplicaciones solo se debe respaldar las carpetas de configuraciones de cada una, puesto que las bases de datos se encuentran en el servidor OSIRIS. En la Figura 61 se puede observar que existe una carpeta que contiene todos los directorios de configuraciones de las aplicaciones llamada “AppSIMED”.

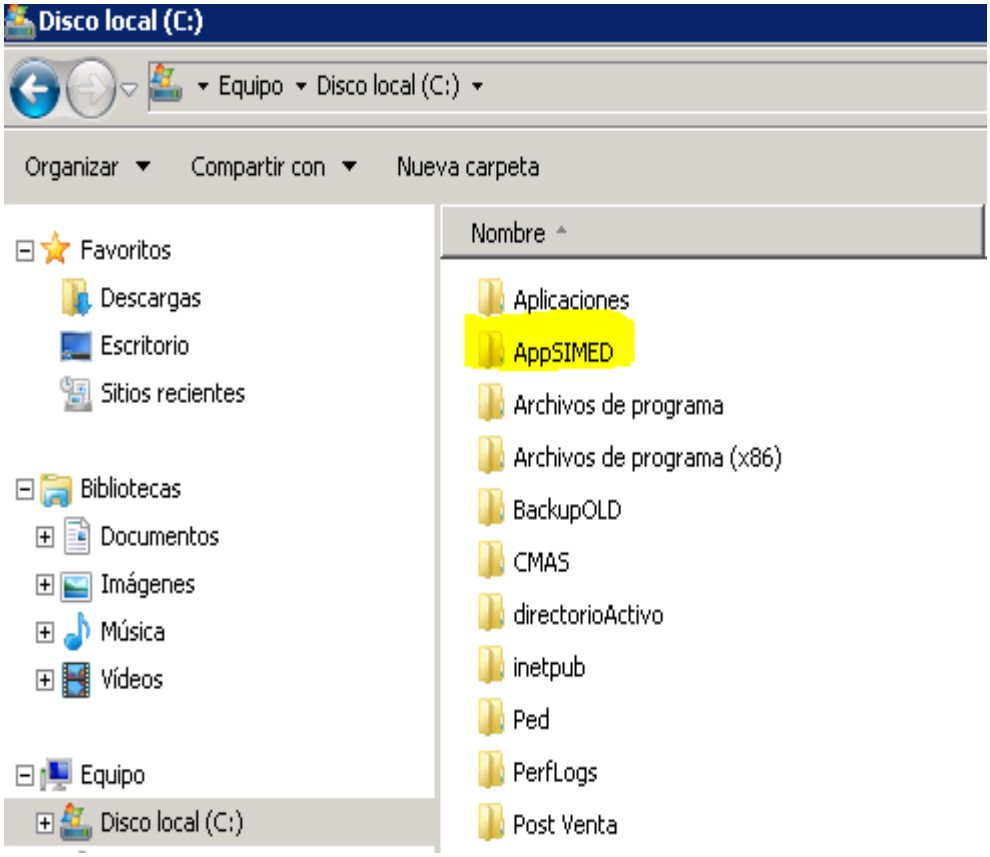


Figura 61. Carpeta donde se guardan todos los directorios de configuraciones de las aplicaciones.

Adentro de esta carpeta se encuentran los directorios mencionados, se lo puede observar en la Figura 62.

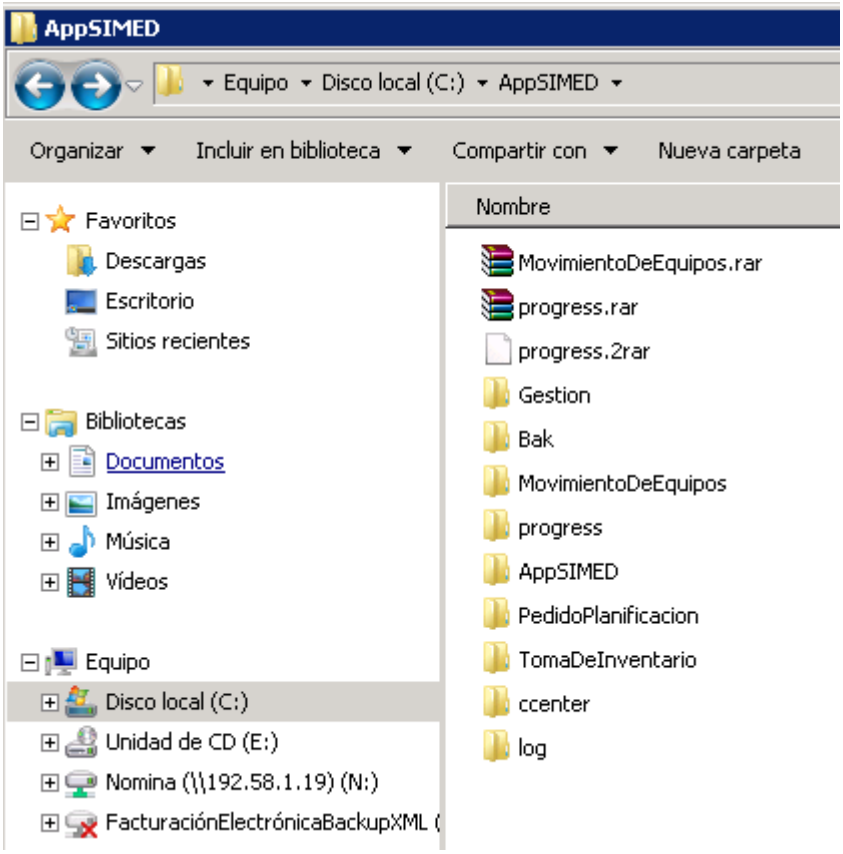


Figura 62. Directorios de configuraciones de las aplicaciones dentro de la carpeta AppSIMED.

En la tabla 35 a continuación se define el directorio y la ruta de la cual se va a respaldar información en la nube del servidor ICARO.

Tabla 33.

Directorio por respaldar en la nube del servidor ICARO.

#	NOMBRE SERVIDOR	RUTA CARPETA DE CONFIGURACIONES DEL APLICACTIVO
1	ICARO	C:\AppSIMED

De tal forma se establece que esta las ruta y carpeta por respaldar en la nube.

4.1.3.3 Información que respaldar del servidor SRVUIOFILE para la restauración de las carpetas compartidas.

En este caso para llegar a la restauración de los archivos compartidos se debe realizar un respaldo de todo el directorio que los contiene.

Todos los archivos compartidos de la empresa que se encuentran en el servidor de archivos se encuentran en una carpeta llamada PUBLICA dentro del disco C. En la Figura 63 se puede observar todas las carpetas de archivos que se encuentran dentro de este directorio.

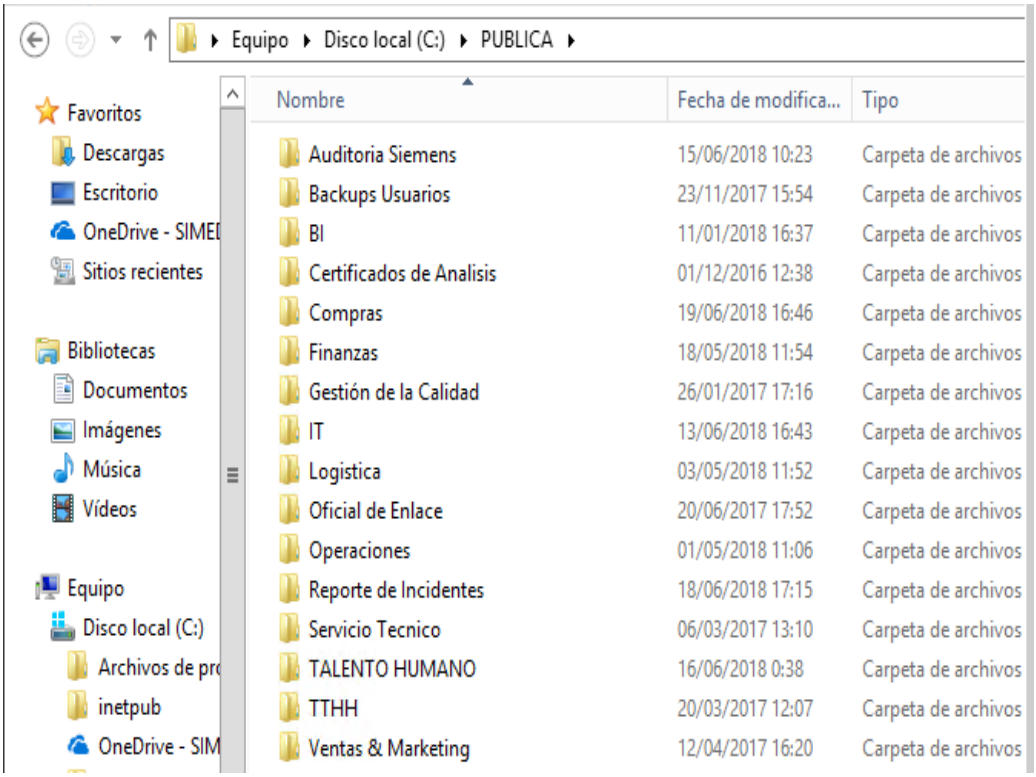


Figura 63. Carpetas de archivos compartidos dentro del directorio PUBLICA.

En la tabla 36 a continuación se define el directorio y la ruta de la cual se va a respaldar información en la nube del servidor SRVUIOFILE. En la tabla 34. Ruta del directorio por respaldar en la nube del servidor SRVUIOFILE.

Tabla 36.

Ruta de los directorios a respaldarse en la nube del servidor SRVUIOFILE.

#	NOMBRE SERVIDOR	RUTA CARPETA DE CONFIGURACIONES DEL APLICACTIVO
1	SRVUIOFILE	C:\PUBLICA

4.1.3.4 Información que respaldar del servidor SMDSERVER para la restauración del Directorio Activo.

Para restaurar un Directorio Activo se puede realizar dos tipos de respaldos:

- Respaldo Estado del Sistema (*System State Backup*): es el respaldo de la configuración actual del equipo (incluyendo el DA y la estructura software del sistema, además del registro).

- Respaldo completa (*Full Backup*): es el respaldo de todo el sistema en general.

Actualmente se tiene configurado un respaldo completo programado a ejecutarse de forma diferencial todos los días a las 23:30, la información del respaldo se guardará en el servidor de archivos SRVUIOFILE en la siguiente ruta: \\192.58.1.58\it\backups\Active Directory, esta dirección se encuentra dentro de la carpeta PUBLICA mencionada en la sección 4.1.3.3. Esta configuración de respaldos se puede observar en la Figura 64.

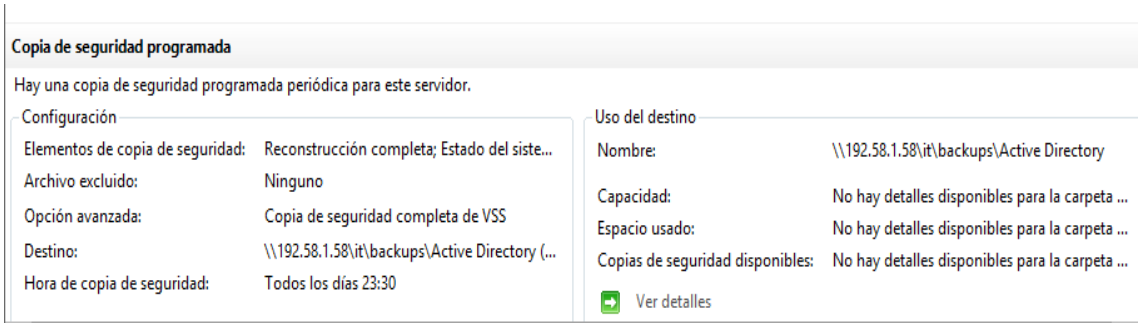


Figura 64. Configuración de las copias de seguridad del Directorio Activo.

Por lo tanto, para una restauración del Directorio Activo no hace falta respaldar información de este servidor en la nube debido a que el respaldo de este ya se guarda en el servidor de archivos SRVUIOFILE donde como ya se definió en la sección 4.1.3.3 se van a realizar los respaldos en la nube de la carpeta PUBLICA, esto ya incluiría información toda la información del Directorio Activo de la empresa.

4.1.3.5 Información que respaldar del servidor MAILSERVER para la restauración de EXCHANGE 2010.

El proceso para la restauración del servicio de Exchange 2010 es el siguiente:

- Instalar el servicio de Exchange en un nuevo servidor.
- Respaldar la carpeta de configuración de Exchange almacenada en la ruta: E:\Exchange
- Respaldar los buzones de correo de todos los usuarios almacenada en la ruta: E:\Program Files\Microsoft\Exchange Server\V14\Mailbox

En la tabla 37 a continuación se define los directorios y las rutas de las cuales se van a respaldar información en la nube del servidor SRVUIOFILE.

Tabla 35.

Ruta de los directorios a respaldarse en la nube del servidor MAILSERVER.

#	NOMBRE SERVIDOR	RUTA CARPETA DE CONFIGURACIONES DEL APLICACTIVO
1	MAILSERVER	E:\Exchange E:\Program Files\Microsoft\Exchange Server\V14\Mailbox

4.1.4 Parametrización de los respaldos a efectuarse por cada servidor.

Una vez definido qué servidores y la información a respaldar de cada uno, es necesario determinar qué tipo de respaldo en la nube se va aplicar, con qué frecuencia se lo va a realizar y cuánto tiempo va estar disponible esta copia de seguridad, esto último debido a que el almacenamiento en la nube tiene costos elevados, por tal motivo no se puede tener la información de forma permanente y la práctica aconsejable recomienda que los respaldos más antiguos tengan un tiempo límite de disponibilidad y se vayan actualizando de forma progresiva.

Cabe recalcar que como se menciona en los marcos de referencia este tipo de respaldo en la nube es una práctica adicional al respaldo de forma local que se debe hacer de forma obligatoria en equipos destinados para esto de la información de los servidores, aplicaciones y bases de datos.

Por tal motivo el único medio donde van a estar de forma permanente el histórico de todos los respaldos va a ser de forma local. Destinando el almacenamiento en la nube par datos actuales de máximo los tres meses de vigencia. En las tablas a continuación se define estos parámetros mencionados.

Tabla 36.

Parámetros de los respaldos para servidores de archivos.

POLÍTICA PARA RESPALDOS DEL SERVIDOR SRVUIOFILE	
PARÁMETRO	VALOR
Tipo de copia de seguridad inicial:	Completo
Tipo de copia de seguridad subsiguiente:	Diferencial
Horario de copias diferenciales:	01:00 AM
Duración de las copias diferenciales:	5 horas
Días a repetirse la copia diferencial:	Martes y sábados
Ancho de banda a ocuparse en copias diferenciales:	20 Mbps
Horarios y parámetros para copias de seguridad completas:	Cada 4 semanas desde las 07:00 PM los sábados hasta que termine, con ancho de banda de 1 Mbps.
Tiempo de duración en la nube de cada versión del respaldo	15 días

Tabla 37.

Parámetros de los respaldos para servidores del aplicativo GP.

POLÍTICA PARA RESPALDOS DE LOS SERVIDORES HORUS Y OMEGA	
PARÁMETRO	VALOR
Tipo de copia de seguridad inicial:	Completo
Tipo de copia de seguridad subsiguiente:	Incremental
Horario de copias diferenciales:	01:00 AM
Duración de las copias diferenciales:	7 horas
Días a repetirse la copia diferencial:	Domingo, martes, jueves, viernes
Ancho de banda a ocuparse en copias diferenciales:	15 Mbps
Horarios y parámetros para copias de seguridad completas:	Solo se trabajará con incrementales a partir de la copia completa inicial
Tiempo de duración en la nube de cada versión del respaldo	60 días

Tabla 38.

Parámetros de los respaldos para el servidor de aplicaciones.

POLÍTICA PARA RESPALDOS DEL SERVIDOR ICARO	
PARÁMETRO	VALOR
Tipo de copia de seguridad inicial:	Completo
Tipo de copia de seguridad subsiguiente:	Incremental
Horario de copias diferenciales:	01:00 AM
Duración de las copias diferenciales:	7 horas
Días a repetirse la copia diferencial:	Domingo, martes, jueves, sábado
Ancho de banda a ocuparse en copias diferenciales:	15 Mbps
Horarios y parámetros para copias de seguridad completas:	Cada 3 semanas los sábados desde las 02:00 AM por 4 horas, con ancho de banda de 20 Mbps.
Tiempo de duración en la nube de cada versión del respaldo	60 días

4.2 Diseño de la Política de Respaldos de la Información de Bases de Datos.

El respaldo de las bases de datos se debe tratar por separado a los respaldos de información tanto de servidores como de usuarios, como en la sección 2.2 Situación actual del sistema de respaldos se analizó la Política actual de respaldos de las bases de datos y cuál es el procedimiento de realizar estos de forma local, en esta sección se mejorará dicha política analizada y se describirá el proceso para respaldar las bases de datos en la nube, por cual se tomarán en cuenta los siguientes puntos para la implementación y configuración de la herramienta de sistemas de respaldos de la información.

- Instancias de motores de bases de datos implementados en la empresa.
- Tamaño en disco ocupado por todas las bases de datos de la empresa.
- Proceso para respaldar las bases de datos en la nube.
- Parametrización de los respaldos en la nube.

4.2.1 Descripción detallada de las bases de datos de la empresa.

A continuación, se describe características importantes como que motor de base de datos se está usando, cuantas instancias de motor de base de datos se tiene implementado, cuantas bases de datos hay por cada instancia y qué tamaño en disco usa cada instancia. Lo descrito se lo puede observar en la Tabla 41.

Tabla 39.

Descripción del motor de bases de datos.

Motor de base de datos	**SQL SERVER**	
Instancias instaladas	OSIRIS	OSIRIS\Perú
Número de bases de datos	83	8
Tamaño en disco de la instancia	49,2 GB	8.14 GB

4.2.2 Proceso para realizar respaldos de las bases de datos en la nube.

Para implementar redundancia en los respaldos de las bases de datos se va a considerar realizar dos tipos de respaldos:

- Respaldo de las bases de datos de forma local en el servidor OSIRIS por medio del JOB ejecutado en SQL SERVER de forma diaria a las 02:00 AM.
- Copia de seguridad del respaldo obtenido de las bases de datos hacia el servidor ANUBIS de forma diaria a través de la herramienta Cobian Backup.
- Respaldo en la nube de todas las instancias del servidor OSIRIS.

De lo definido se puede determinar que la herramienta a implementarse debe ser capaz de realizar al menos dos tipos de respaldos de la información:

1. Respaldo de ficheros: para realizar los respaldos de archivos mencionados en la sección 4.1.3 de los servidores críticos.

2. Respaldo de instancias de bases de datos: para la restauración de las bases de datos de los sistemas.

4.2.3 Parametrización de los respaldos a efectuarse para las bases de datos.

Como se mencionó en la sección 4.1.4 es necesario determinar qué tipo de respaldo en la nube se va a aplicar, con qué frecuencia se lo va a realizar y cuánto tiempo va a estar disponible esta copia de seguridad. Por lo tanto, en la tabla 42 se define estos parámetros que deben configurarse en la herramienta.

Se puede observar cómo se configuraron los tiempos y días para la copia diferencial o incremental.

Tabla 40.

Políticas para respaldos de información de las bases de datos.

POLÍTICA PARA RESPALDOS DE LAS INSTANCIAS DE BASE DE DATOS	
PARÁMETRO	VALOR
Tipo de copia de seguridad inicial:	Completo
Tipo de copia de seguridad subsiguiente:	Diferencial
Horario de copias diferenciales:	03:00 AM
Duración de las copias diferenciales:	4 horas
Días a repetirse la copia diferencial:	Lunes, martes, miércoles, jueves, viernes
Ancho de banda a ocuparse en copias diferenciales:	15 Mbps
Horarios de copias de seguridad completas:	01:00 AM
Duración de las copias completas:	15 horas
Días a repetirse la copia completa:	miércoles

4.3 Diseño de la Política de Respaldos de la Información de usuarios.

De lo analizado en la sección 2.2.1 se encontró que los respaldos de información de usuarios el área de TI solo lo realiza discos duros externos cuando se renueva o se formatea la computadora al colaborador.

Dando como resultado que no se tiene un respaldo diario de la información algo grave puesto que los datos de los usuarios cambiar de forma exponencial y solo disponer de respaldos de varios meses de antigüedad es poco productivo.

Por lo cual en esta sección se definirá lo siguiente:

- Jerarquización de criticidad de la información de usuarios por el cargo.
- Plan de implementación de respaldos para usuarios normales.
- Plan de implementación de respaldos para usuarios críticos.

4.3.1 Jerarquización de criticidad de la información de usuarios por el cargo.

La idea de realizar la jerarquización de usuarios de acuerdo con su cargo para establecer la criticidad de información que manejan es porque en la empresa se cuenta con un servicio de Office365 con cuentas Premium y Essentials para todos sus colaboradores que en la actualidad solo es usado para el servicio de ofimática dejando de lado servicios muy buenos que Microsoft Office proporciona como lo es OneDrive con un almacenamiento de 1TB por usuario en la nube.

Para el uso de esta herramienta el usuario debe iniciar sesión en su computadora con su correo corporativo y proceder a copiar los archivos que desea respaldar en el directorio de OneDrive. Por lo tanto, el usuario es el responsable de realizar esta gestión para resguardar sus datos.

De lo mencionado se puede esperar que por falta de costumbre algunos usuarios harán caso omiso de este proceso y la implementación de esta herramienta no

tendrá el efecto deseado para los objetivos de la empresa, por lo tanto debido a este y para cumplir las políticas de seguridad de la empresa se desea que ciertos usuarios que se consideran críticos para la operación de la empresa siempre se esté respaldando su información independientemente si ellos realizan o no el proceso de OneDrive, por lo cual se desea además de implementar OneDrive disponer de otro programa para realizar copias de seguridad de toda la máquina de en la nube de los usuarios considerados como críticos.

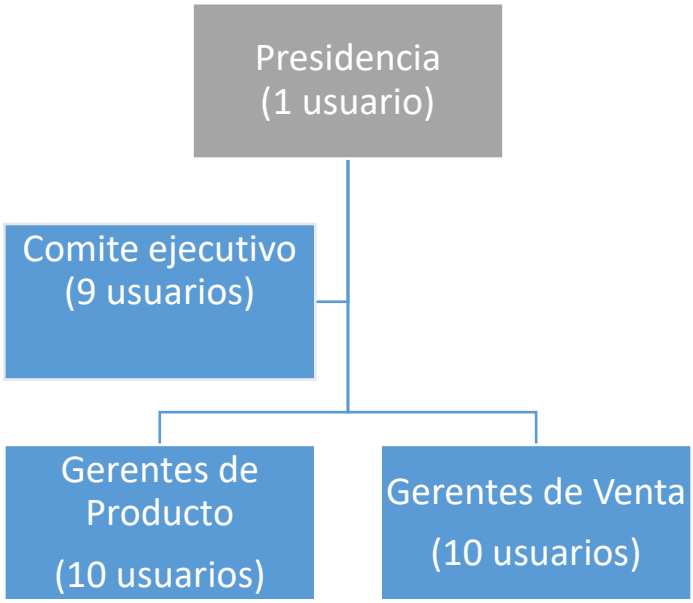


Figura 65. Áreas críticas de la empresa.

De la Figura 65 se puede observar que se necita respaldar la información de un total de 30 usuarios en la nube con una herramienta diferente a OneDrive.

4.3.2 Plan de implementación de respaldos para usuarios normales.

Son considerados usuarios normales todos los usuarios de la empresa que no pertenezcan a las áreas de presidencia, comité ejecutivo, gerentes de producto y gerentes de ventas.

El total de usuarios de la empresa que no pertenecen a las áreas mencionadas es de 183 personas. Como se puede observar en la figura 66 a continuación se

encuentran el total de licencias Premium y Essentials con la que cuenta la empresa.

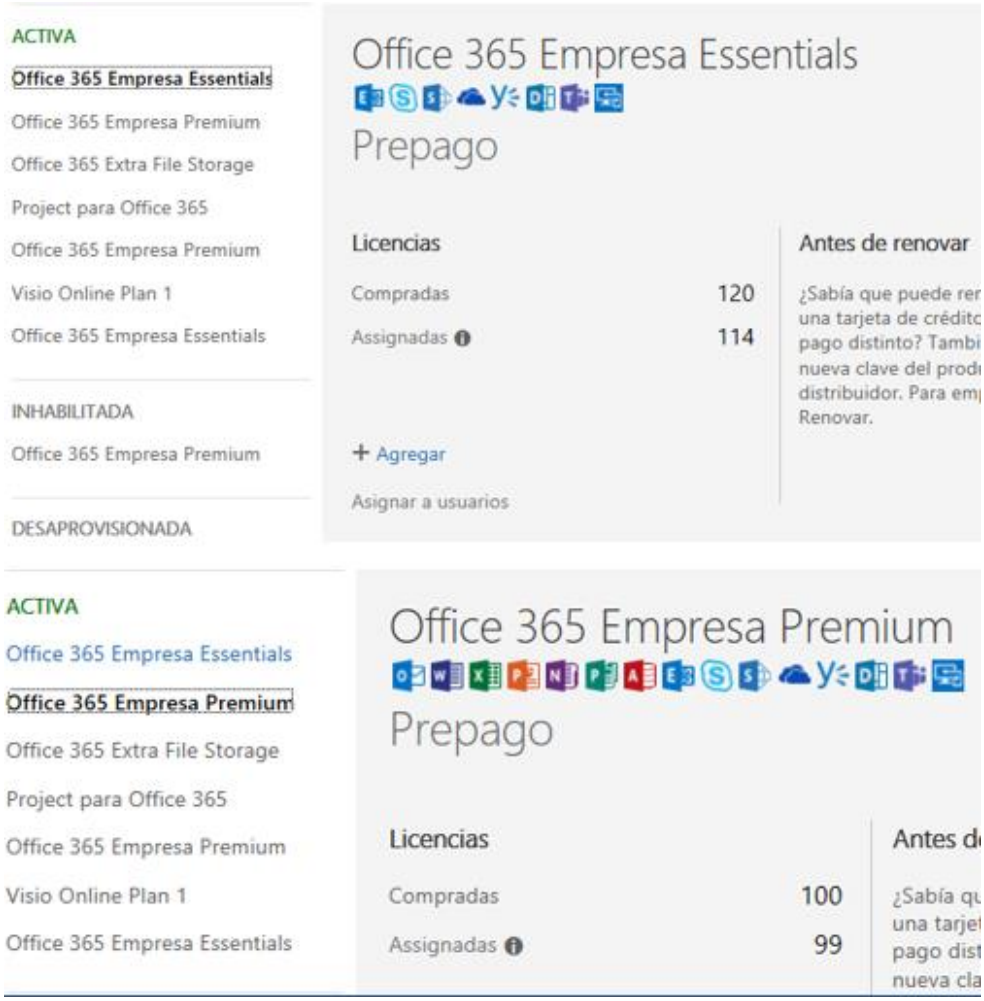


Figura 66. Licencias Microsoft Office Premium y Essentials de la empresa.

El proceso por realizarse para la implementación de respaldos de información para usuarios normales de la empresa es el siguiente:

1. Difusión de la nueva política de respaldos de información por medio de OneDrive a los usuarios implicados, dando a las ventajas que se tiene y las normativas de uso de la herramienta.

2. Habilitación de la herramienta OneDrive ya incluida en todas las estaciones de trabajo de los usuarios como característica nativa de

Windows 10, la habilitación se da por medio del correo electrónico de cada colaborador.

3. Capacitación a los usuarios de cómo se respalda la información por medio de OneDrive y como es el proceso para recuperar su información.

4.4 Análisis de herramientas de respaldos de información en la nube.

En esta sección de acuerdo con el diseño planteado para el respaldo de información de servidores, bases de datos, usuarios y en contraste con el presupuesto de la empresa. Se realizará un análisis de los servicios actuales que se ofrecen en el mercado de sistema de respaldo en la nube. Posterior elección de uno para su implementación, configuración y pruebas de funcionamiento.

4.4.1 Herramientas de respaldos en la nube consideradas para analizar

Las soluciones en la nube analizadas fueron escogidas de acuerdo con el cuadrante Gartner acerca de las mejores herramientas para respaldos online 2018 donde se menciona a:

- ✓ iDrive
- ✓ Backblaze
- ✓ Carbonite.
- ✓ Druva Phoenix
- ✓ Acronis

4.4.2 Comparativa de características de herramientas seleccionadas

A continuación, en la Tabla 43 se analizan las características de cada una de las herramientas mencionadas.

Tabla 41.
Comparativa entre herramientas de respaldos en la nube.

	IDrive	BLACKBLAZE	DRUVA	ACRONIS
RESPALDO				
Respaldo de MS-SQL	No	No	Sí	No
Respaldo de Hyper-V	No	Sí	Sí	Sí
Respaldo de VMware	Si	No	Si	No
Programador de respaldo	Sí	Sí	Sí	Sí
Copia de seguridad continua	Sí	Sí	Sí	Sí
Respaldo incremental	Sí	Sí	Sí	Sí
Copia de seguridad basada en imágenes	Sí	No	No	Sí
Copia de seguridad externa	Sí	Sí	Sí	Sí
Respaldo NAS	Sí	No	No	Sí
Respaldo de servidor	No	No	Sí	No
Copia de seguridad híbrida	Sí	No	Sí	Sí
Respaldo de dispositivo móvil	Sí	No	No	Sí
Copia de seguridad ilimitada	No	Sí	Sí	No
Dispositivos Ilimitados	Sí	No	No	No

	IDrive	BLACKBLAZE	DRUVA	ACRONIS
Velocidad de aceleración	Sí	Sí	Sí	Sí
Copia de archivos a nivel de bloque	Sí	Sí	Sí	Sí
Copia de seguridad multiproceso	No	Sí	No	No
RESTAURACIÓN				
Servicio de recuperación de mensajería	Sí	Sí	Sí	No
Acceso al navegador	Sí	Sí	Sí	Sí
Acceso a aplicaciones móviles	Sí	Sí	Sí	Sí
Versiones	Sí	Sí	Sí	Sí
Retención de archivos eliminados	Sí	Sí	Sí	Sí
SEGURIDAD				
Encriptación privada	Sí	Semi-privada	Sí	Sí
Cifrado de tránsito	Sí	Sí	Sí	Sí
Protocolo de cifrado	AES 256	AES 128	AES 256	AES 128
Autenticación de dos factores	No	Sí	Sí	No
Centro de datos endurecido	Sí	Sí	Sí	Sí
Configuración del servidor proxy	Sí	No	Sí	No
Compatible con HIPPA	No	No	Sí	No
APOYO				
Apoyo 24/7	Sí	Sí	Sí	Sí
Soporte de chat en vivo	Sí	Sí	No	Sí
Soporte telefónico	Sí	No	Sí	Sí

	IDrive	BLACKBLAZE	DRUVA	ACRONIS
Soporte de correo electrónico	Sí	Sí	Sí	Sí
Foro de usuarios	Sí	No	No	Sí
Base de conocimientos	Sí	Sí	Sí	Sí
OTROS				
Compartición de archivos	Sí	Sí	Sí	No
Prueba gratis	Ilimitada	15	15	30

4.4.3 Comparativa de precios de herramientas seleccionadas

En las siguientes tablas se describen los precios comerciales manejados de acuerdo con los diferentes planes que ofrecen cada herramienta.

Tabla 42.

Precios comerciales de IDrive.

Plan	Gratis	Personal 2tb	Personal 5tb	Business 250gb	Business 1.25tb
Precio del plan	Gratis por mes	$ 52 ANUAL	$ 74 ANUAL	$ 74 ANUAL	$ 374 ANUAL
		$ 104 2 AÑOS	$ 149 2 AÑOS	$ 149 2 AÑOS	$ 749 2 AÑOS
Storage	5 GB	2000 GB	5000 GB	250 GB	1250 GB

Tabla 43.

Precios comerciales BACKBLAZE.

PLAN	PERSONAL 2TB
PRECIO DEL PLAN	$ 5 MENSUAL
	$ 50 ANUAL
	$ 95 2 AÑOS
DETALLES	PLAN ES PARA UNA COMPUTADORA

Tabla 44.

Precios comerciales DRUVA PHOENIX PARA SERVIDORES.

PLAN	DRUVA PHOENIX PARA SERVIDORES
PRECIO DEL PLAN	$ 83 MENSUAL
	$ 500 ANUAL
	$ 950 2 AÑOS
STORAGE	5 TB
DETALLES	NÚMERO DE SERVIDORES ILIMITADOS HASTA CUMPLIR CUOTA

Tabla 45.

Precios comerciales DRUVA INSYNC ENTREPRISE para usuarios.

PLAN	DRUVA INSYNC ENTERPRISE PARA USUARIOS
PRECIO DEL PLAN	$ 105 ANUAL
STORAGE	ILIMITADO
DETALLES	PLA ES PARA UN USUARIO

Tabla 46.

Precios comerciales de ACRONIS.

PLAN	ADVANCED 250GB	ADVANCED 500GB	PREMIUM 1TB	PREMIUM 2TB
PRECIO DEL PLAN	$ 49 ANUAL (1 PC)	$69 ANUAL (1 PC)	$ 99 ANUAL (1 PC)	$ 139 ANUAL (1 PC)
	$ 79 ANUAL (3 PC)	$ 99 ANUAL (3 PC)	$ 149 ANUAL (3 PC)	$ 189 ANUAL (3 PC)

4.4.4 Elección de una herramienta de respaldos de información en la nube

De acuerdo con el análisis realizado sobre las características y precios de las herramientas evaluadas se llegó a la elección del sistema de respaldos de información con el servicio de DRUVA. A continuación, las principales razones de su elección:

1. Es la única herramienta de las analizadas que realizada respaldos de MS-SQL. Esto permitirá respaldar en su totalidad a las instancias
2. Permite realizar respaldos de Hyper-V, tecnología usada en la empresa.
3. Emplea respaldos incrementales.
4. Cuenta con un programador de respaldos que permitirá configurar los parámetros de frecuencia establecidos anteriormente.
5. Maneja tecnología de deduplicación de datos que permitirá optimizar al espacio de almacenamiento en la nube.
6. Dispone de variadas formas para la recuperación de la información.
7. Cuenta con un gran nivel de soporte 24/7.
8. No se debe implementar nada de forma local, no tiene requisitos de infraestructura para su funcionamiento, es totalmente un servicio *cloud*.
9. Maneja altos niveles de seguridad, al implementar encriptación AES256.
10. Ofrece dos servicios; Druva Phoenix y Druva inSync. Con el primero se gestionarán los respaldos de servidores y bases de datos. Con el segundo se implementará el servicio de respaldos de información para los usuarios críticos de la empresa.
11. Los precios comerciales de Druva Phoenix están a acorde al almacenamiento que ofrece de 5TB por el valor de $ 500 anuales. Este tamaño de almacenamiento se ajusta perfectamente a los valores en la

nube que necesita la empresa, puesto que de los cálculos realizados se plantea que para el respaldo inicial se necesita 2TB de almacenamiento y se debe considerar que al aplicarse copias incrementales por versiones el tamaño de los datos almacenados llega incrementa al doble, es decir realmente se necesita un espacio de almacenamiento en la nube de mínimo 4TB.

12. El mismo proveedor ofrece el servicio de Druva INSYNC ENTERPRISE el cual permite realizar respaldos de la información de usuarios un almacenamiento ilimitado pagando por usuario un valor de $ 105 anual. Se adquirirá 30 licencias, con el fin de cubrir el número de usuarios críticos de la empresa.

4.5 Implementación del Sistema de Respaldos de la Información para servidores y bases de datos con DRUVA PHOENIX.

En esta sección se analizará los siguientes puntos:

- ✓ **Matriz de soporte:**

- ✓ **Configuración de los servidores y las máquinas virtuales para la copia de seguridad:**
  Pasos rápidos para realizar una copia de seguridad de servidores y máquinas virtuales.

- ✓ **Configurar organizaciones:**
  Instrucciones sobre cómo crear, administrar y ver organizaciones en Phoenix

- ✓ **Configuración de Phoenix para copia de seguridad y restauración:**
  Esta categoría proporciona instrucciones para implementar y configurar Servidor de archivos y Microsoft SQL. También proporciona información sobre la realización de copias de seguridad de los servidores.

- ✓ **Monitor de PHOENIX:**

  Se dará a conocer los paneles de la organización, alertas generadas por Phoenix Cloud, detalles del espacio de almacenamiento, trabajos que monitorean Phoenix, informes que describen las actividades de Phoenix y el estado de Phoenix Cloud.

4.5.1 Matriz de soporte de PHOENIX

En esta sección se dará a conocer información sobre niveles de soporte, licencias, requisitos de software, requisitos de hardware, soporte de navegador, requisitos de red y consideraciones de seguridad.

4.5.1.1 Navegadores soportados

En la tabla 49 a continuación enumera los navegadores admitidos para acceder a la Consola de Administración de Phoenix.

Tabla 47.

Navegadores soportados para ingresar a la Consola de Administración de Phoenix.

Navegador	Requerimiento mínimo
Navegador web	• Internet Explorer (IE) 11 and Edge • Mozilla Firefox (Firefox) 33 • Google Chrome (Chrome) 35

4.5.1.2 Sistemas operativos para copias de seguridad de archivos y carpetas

Las plataformas certificadas y compatibles en las que Phoenix puede realizar copias de seguridad y restaurar archivos y carpetas se enumeran en la tabla 50 a continuación.

Tabla 48.

Sistemas operativos soportados por Phoenix.

Sistema operativo	Sistema de archivos	Ediciones
Windows **(Versiones Estándar y Empresa)**	✓ NTFS	• Windows Server 2016 (x86-64) • Windows Server 2012 R2 (x86-64) • Windows Server 2012 (x86-64) • Windows Server 2008 R2 (x86-64) • Windows Server 2008 (x86-64) • Windows Small Business Server (SBS) 2011 (x86-64)
Linux	• EXT • XFS	• CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1 and 7.2 (x86-64) • Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1 and 7.2 (x86-64)
Ubuntu	✓ EXT	• Ubuntu 14.04 (x86-64) • Ubuntu 16.04 (x86-64)

4.5.1.3 Puertos y protocolos de comunicación para Phoenix

Phoenix se comunica con sus recursos NAS para realizar una copia de seguridad y restaurar los datos. Esto ocurre a través de puertos y protocolos que son seguros para la comunicación y la transición de datos.

Phoenix usa el protocolo Transport Layer Security (TLS) para establecer una conexión e iniciar la comunicación entre los componentes Phoenix y su dispositivo NAS.

En la figura 67 a continuación se muestra los puertos y protocolos de comunicación que utiliza Phoenix para la conexión segura y la comunicación durante las operaciones de copia de seguridad y restauración.

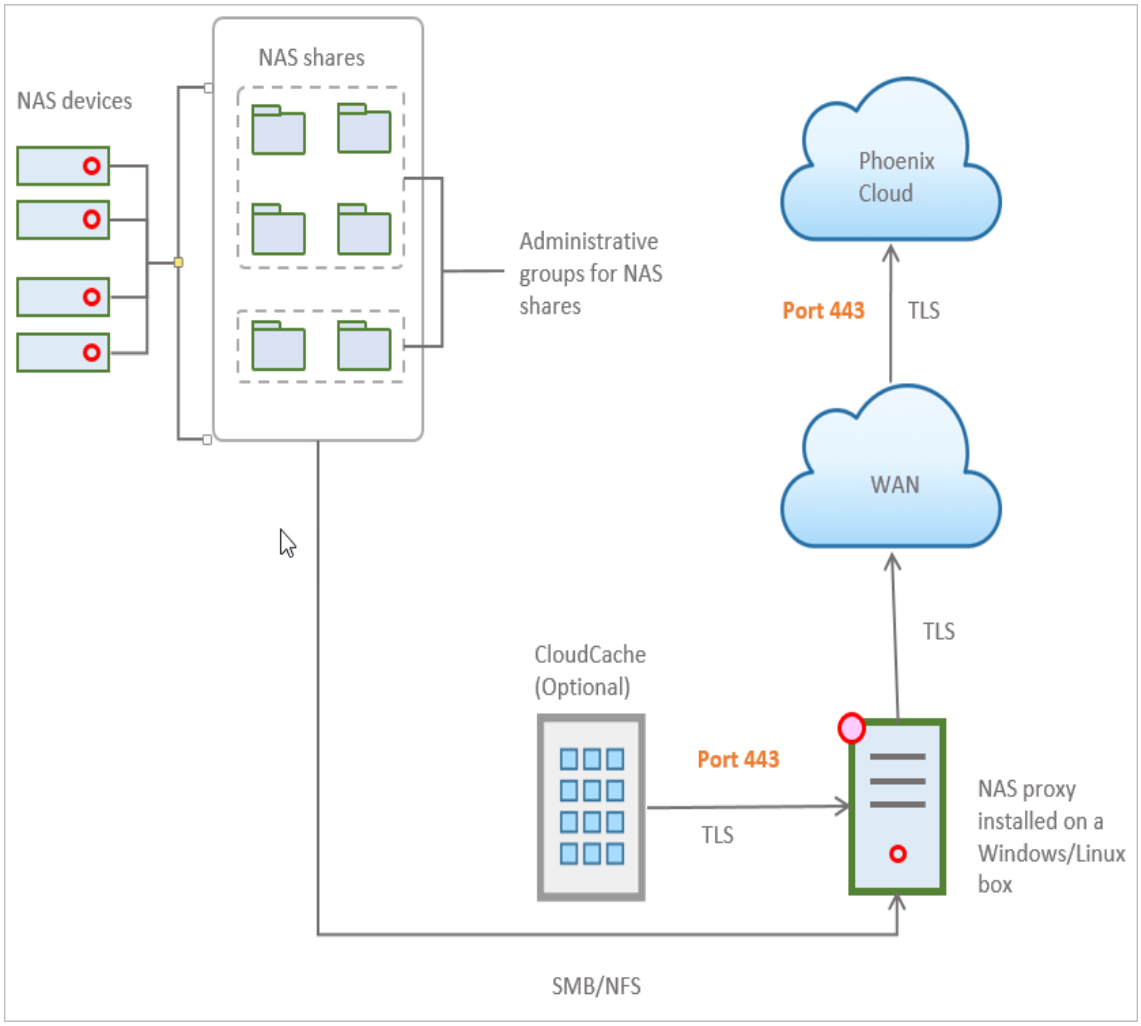


Figura 67. Diagrama de puertos y protocolos usados por Phoenix.

4.5.1.4 Versiones de SQL Server soportadas por PHOENIX

Druva certifica las siguientes ediciones:

- ✓ Sistemas operativos Windows Server (64 bits) Standard y Windows Server (64 bits) Enterprise Edition.

- ✓ Edición de SQL Server Enterprise

En la tabla 51 a continuación se enlistan las versiones de SQL SERVER soportadas por Phoenix.

Tabla 49.

Versiones de SQL SERVER soportadas por Phoenix.

Windows Server (64-bit)	SQL Server Edition
Windows Server 2016 (x86-64)	• SQL Server 2016 SP1 • SQL Server 2014
Microsoft Windows Server 2012 R2	• SQL Server 2016 SP1 • SQL Server 2014 • SQL Server 2012 Service Pack (SP) 2 • SQL Server 2008 Service Pack (SP) 4 • SQL Server 2008 R2 SP 3
Microsoft Windows Server 2012	• SQL Server 2016 SP1 • SQL Server 2012 SP 2 • SQL Server 2008 R2 SP 3 • SQL Server 2008 RTM
Microsoft Windows Server 2008 R2	• SQL Server 2008 R2 SP 3 • SQL Server 2008 RTM
Microsoft Windows Server 2008 SP 2	• SQL Server 2012 SP 2 • SQL Server 2008 R2 SP 3 • SQL Server 2008 RTM
Microsoft Windows Server 2008	• SQL Server 2008 SP 4 • SQL Server 2008 RTM

4.5.1.5 Requisitos previos de hardware para instalar el agente de Phoenix

En la tabla 52 a continuación se enlista los requerimientos mínimos para la instalación del agente de Phoenix en un servidor, así como también se da a conocer cuál es la ruta por defecto en donde se guardará la información del agente.

Tabla 50.

Requerimientos mínimos para la instalación del agente de Phoenix.

Hardware	Requerimiento Mínimo
CPU	2 GHz dual-Core (Intel Core series) 2.4 GHz (AMD) o equivalente
RAM	4 GB
Espacio libre	• En servidores Windows y Linux, 2% del total de los datos es utilizado por la aplicación Phoenix. La información de la aplicación es almacenada en: ○ **Windows 2012 Server** C:\ProgramData\Phoenix ○ **Windows 2008 Server** C:\ProgramData\Phoenix

4.5.2 Pasos para configurar Phoenix para respaldar archivos y carpetas

En esta sección se configurará e implementará Phoenix para el respaldo de los servidores críticos analizados en la sección 4.1.2.

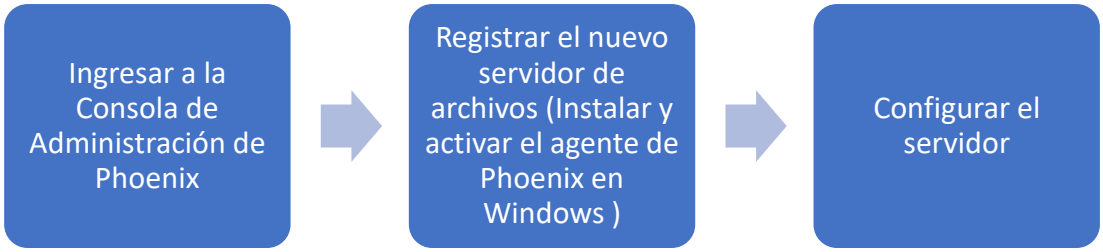


Figura 68. Pasos para implementar Phoenix en los servidores de archivos.

1. INGRESAR A LA CONSOLA DE ADMINISTRACIÓN DE PHOENIX

Se recibe un correo con la URL y los datos para ingresar como administrador. (usuario y clave).

Figura 69. Pantalla de ingreso a la Consola de Administración de Phoenix.

2. GENERAR TOKEN DE ACTIVACIÓN Y DESCARGAR EL AGENTE

A. En la barra de menú, hacer clic en Todas las organizaciones y seleccione la organización requerida de la lista desplegable. En este caso se selecciona la organización SIMED.

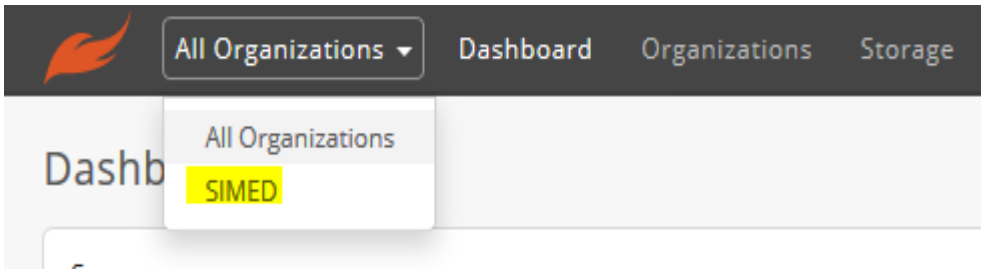


Figura 70. Selección de la organización.

B. En la barra de menú, se hace clic en Proteger> Servidores de Windows / Linux.

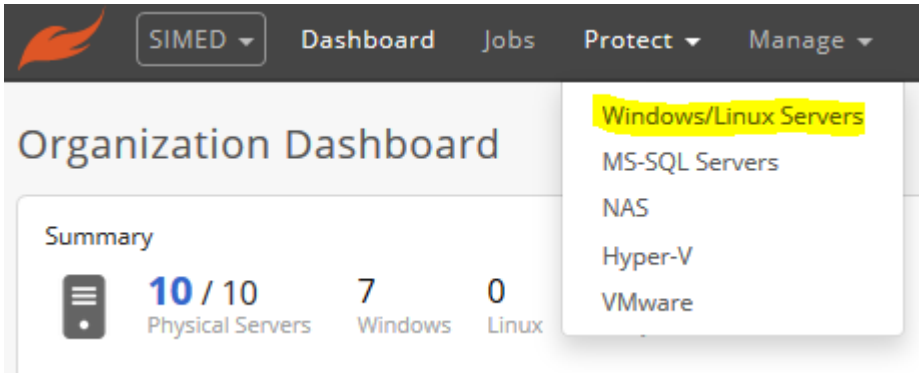


Figura 71. Acceso para registrar un nuevo servidor de archivos Windows.

C. Se hace clic en Registrar nuevo servidor.
D. En la página de Registro de Servidor antes de dar clic en Next se debe descargar el agente de Phoenix dando clic en el link para descargas.

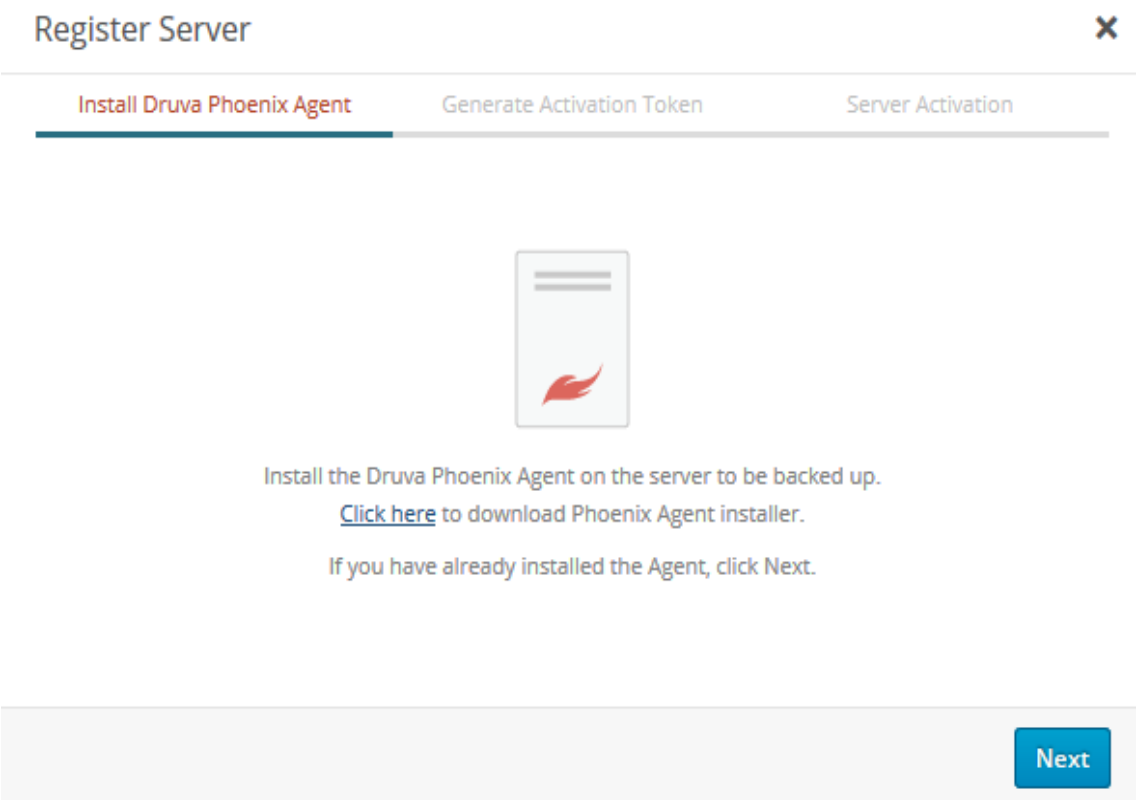


Figura 72. Registro de un nuevo servidor paso 1.

E. Al dar clic en el link se abrirá la página donde se debe descargar el agente, en este caso a ser los servidores donde se va a instalar Windows, se descarga el agente para dicho sistema operativo.

Figura 73. Descargar el agente de instalación de Phoenix para Windows Server.

F. En la pestaña de generación de Token se debe colocar una descripción para dicho token.

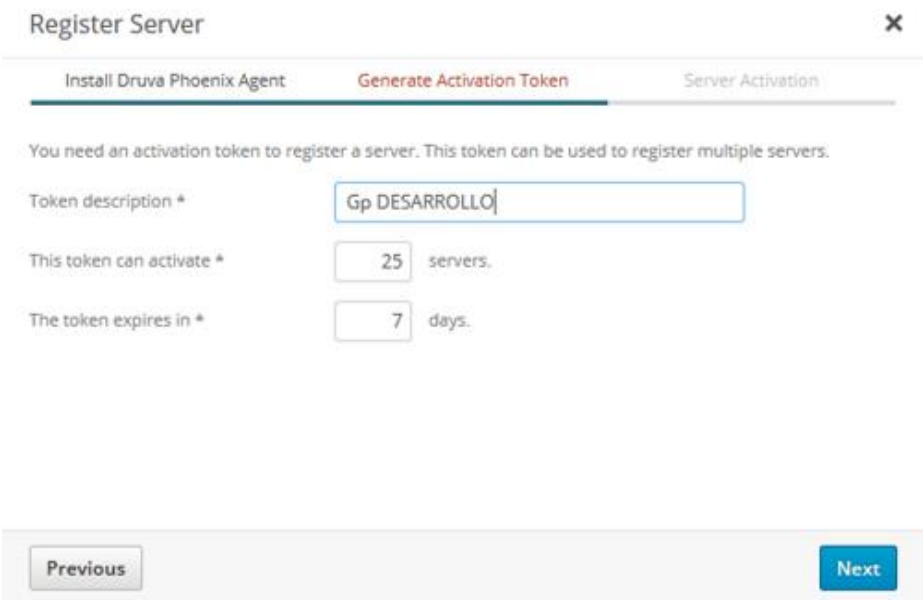


Figura 74. Descripción del Token.

G. En la pestaña de Activación de Servidor dar clic en guardar y copiar Token. Después de copiar dar clic en Finalizar.

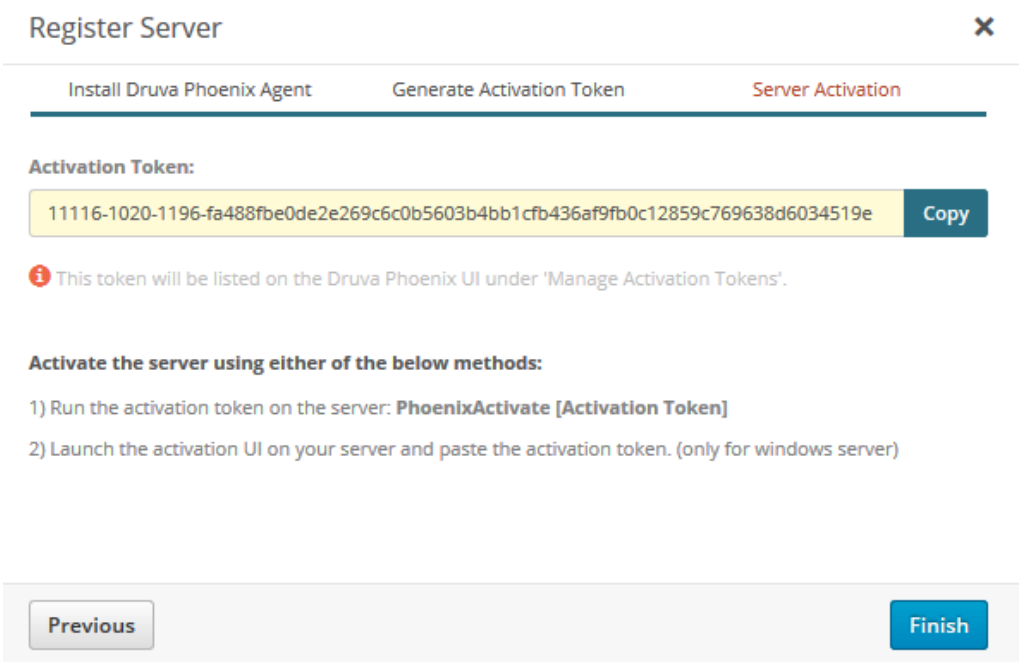


Figura 75. Token generado para el registro del nuevo servidor.

3. INSTALAR AGENTE EN EL SERVDIOR

A. Entrar al servidor donde se va a instalar el agente, para esta primera implementación se realizará el respaldo del servidor HORUS donde se encuentra el aplicativo de Microsoft Dynamics GP Ecuador.

B. Ir a la ubicación donde descargó el instalador del Agente Phoenix.

C. Hacer doble clic en el instalador de Phoenix.

D. Hacer clic en Siguiente.

E. En el cuadro Ubicación de instalación, escriba o seleccione la ruta completa al directorio de inicio de la instalación.

F. Hacer clic en Instalar.

G. Una vez completada la instalación, se hace clic en Finalizar.

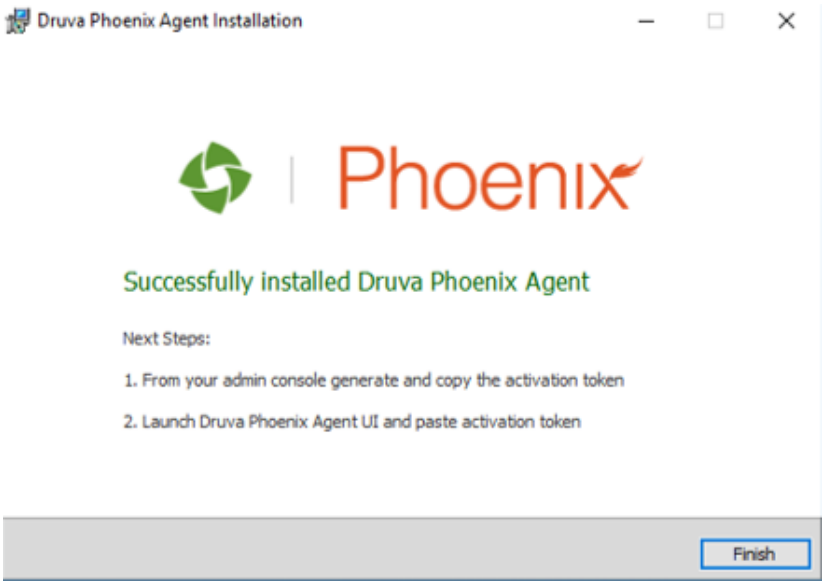


Figura 76. Finalización de la instalación del Agente de Phoenix.

H. Abrir el ícono de acceso rápido creado en el escritorio.

I. Copia el token de activación que Phoenix generó.

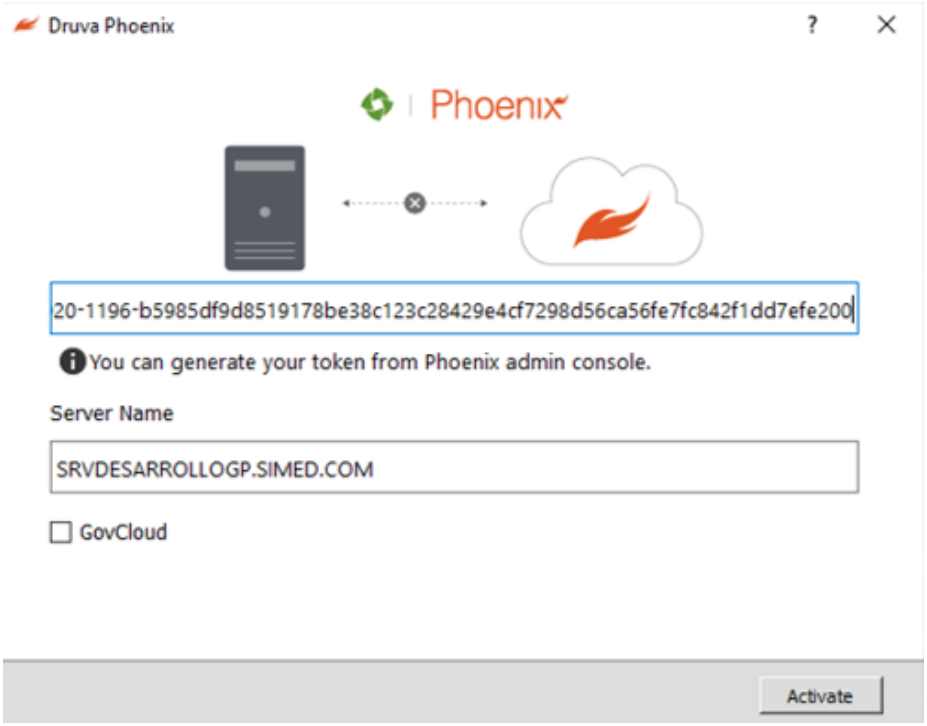


Figura 77. Copiar el token generado por Phoenix en el agente instalado en el servidor HORUS.

4. CREAR GRUPOS ADMINISTRATIVOS

Con el fin de tener una estructura de administración de los servidores que se están respaldando en Phoenix se deben crear grupos administrativos en donde se puedan agregar los servidores que tengan las mismas funciones o características. Con esto se gana disponer de una administración centralizada.

Para crear grupos administrativos ir a Administración >Grupos administrativos > Crear nuevo grupo. En la pantalla desplegada se debe establecer el nombre del grupo y una descripción. Para este caso se creará el grupo administrativo ServerHORUS, el mismo que se le asignará al servidor HORUS registrado en los pasos anteriores.

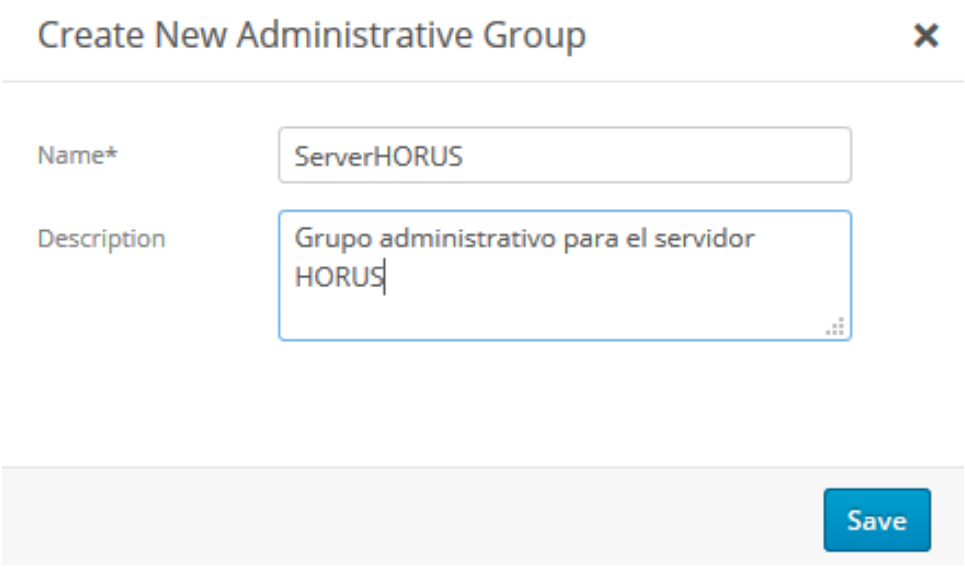


Figura 78. Creación del grupo administrativo para el servidor HORUS.

5. CREAR REGLAS DE CONTENIDO

Phoenix tiene la opción de crear reglas de contenido a respaldar, se puede respaldar todas las carpetas o rutas específicas. Para la configuración de este respaldo se creará la regla de contenido para el servidor HORUS, como se determinó en la sección 4.1.3.1 en la tabla 34 el directorio del cual se debe respaldar la información para este servidor es “C:\Program Files (x86)\Microsoft Dynamics”.

Para la creación de esta regla ir a Administración > Reglas de contenido > Crear nueva regla de contenido. En la pantalla desplegada se debe colocar el nombre de la regla y el tipo.

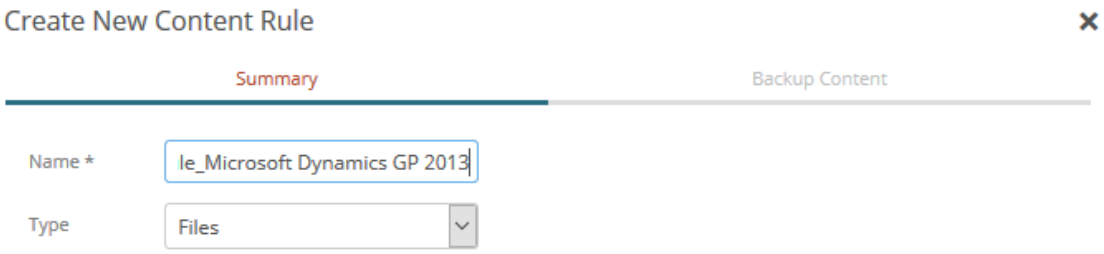


Figura 79. Definición de nombre de regla de contenido.

A continuación, se debe definir la ruta de la carpeta a respaldar, en esta sección se coloca la ruta anteriormente mencionada. También se debe especificar qué tipo de archivos excluir.

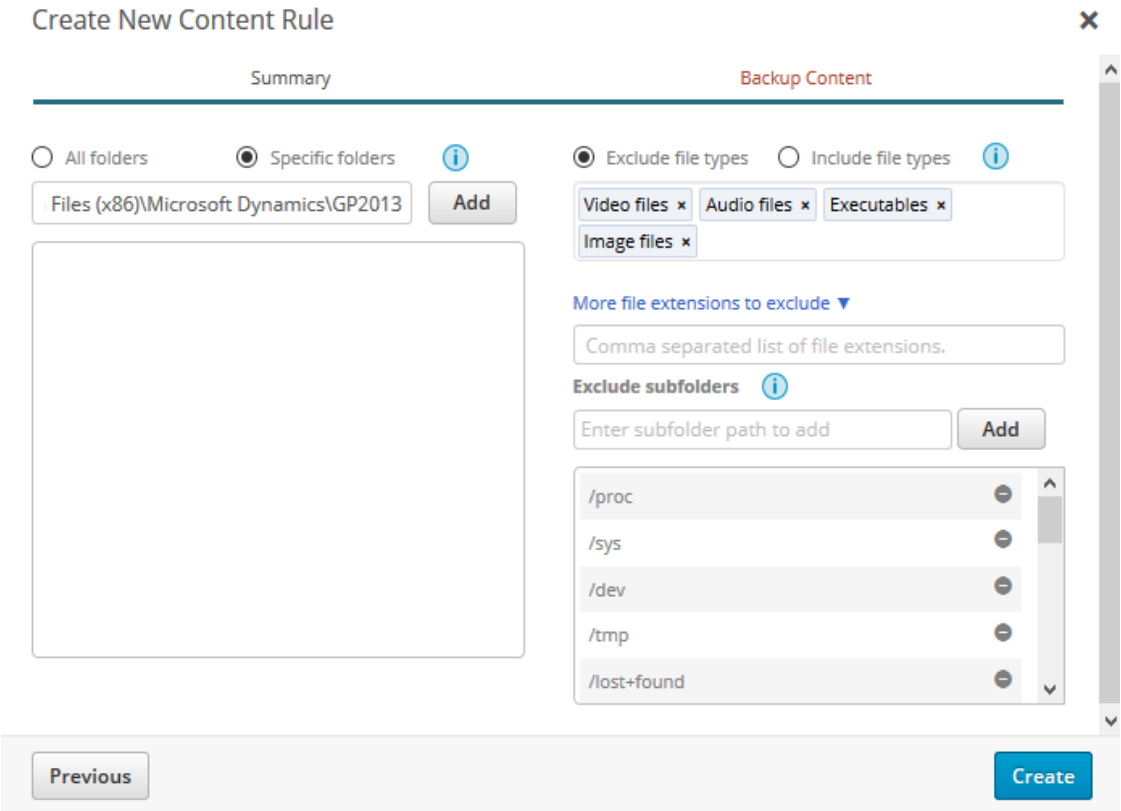


Figura 80. Configuración de ruta para regla de contenido.

6. CREAR POLÍTICAS DE RESPALDO

Como se definió en la sección 4.1.4 acerca de la parametrización de los respaldos a efectuarse por cada servidor en Phoenix se debe crear políticas de respaldo donde se especificará los horarios de respaldo, los días a efectuarse, la duración de estos, el ancho de banda que empleará, la duración de las versiones de respaldos en mantenerse disponibles en la nube. Para realizar la configuración de lo descrito se debe ir a Administración > Políticas de respaldos > Crear nueva política de respaldos. En la pantalla desplegada se coloca un nombre, descripción y se configura la política de respaldos.

Para continuar con la implementación de respaldos para el servidor HORUS que se está realizando se creará en esta sección una política de respaldos para dicho servidor. En este caso la política se llamará FilesHORUS_Default Retention Policy y se configuran los valores definidos en la sección 4.1.4 en la tabla 39 para dicho servidor.

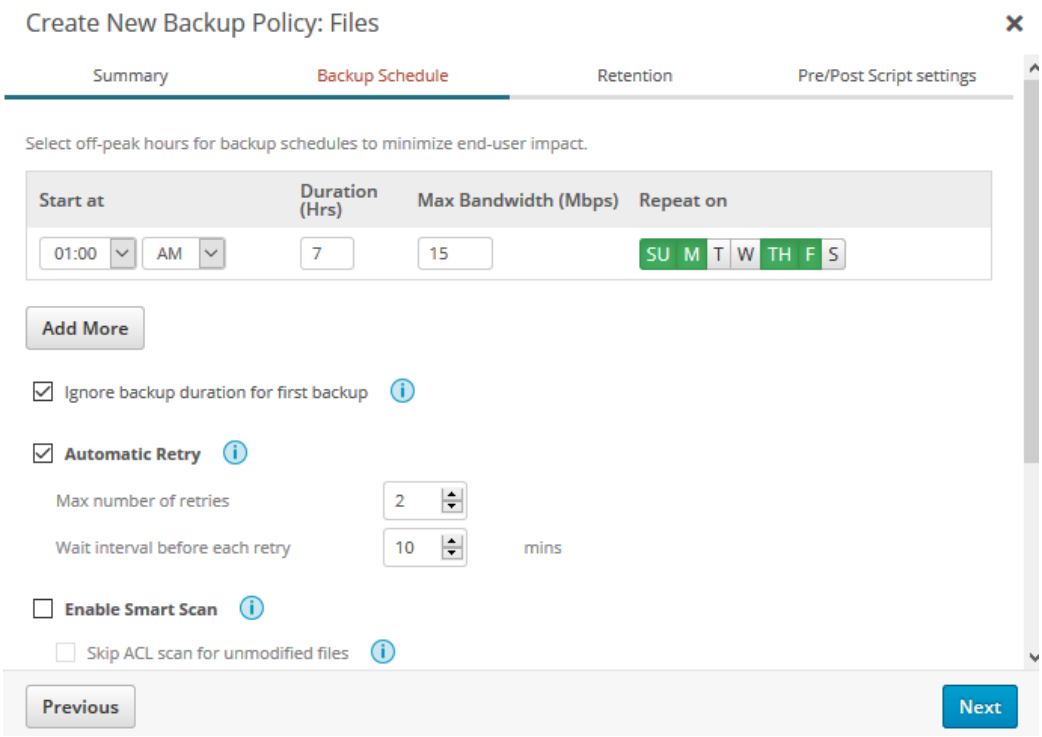


Figura 81. Configuración de los horarios y frecuencias para los respaldos del servidor HORUS.

7. CONFIGURACIÓN DEL SERVIDOR HORUS EN LA COSNOLA DE ADMISTRACIÓN DE PHOENIX

Después de haber instalado el agente en servidor y de haberlo activado este será visible desde la consola de administración de Phoenix de donde se lo podrá configurar ya sea como respaldos de bases de datos o respaldos de archivos. Como se ha mencionado este servidor corresponde a respaldos de archivos para realizar dicha configuración se realizar los siguientes pasos:

1. Ir a Protección > Windows/Linux Servidores >
2. Seleccionar el servidor a configurar, en este caso selecciona el servidor de HORUS.
3. Se da clic en Crear un conjunto de copias de seguridad de archivos.
4. Se elige el almacenamiento a usar, en este caso es Simed Corp_sa-east-1
5. Se elige la regla de contenido, para este caso la regla de contenido definida anteriormente Rule_Microsoft_Dynamics_GP2013.

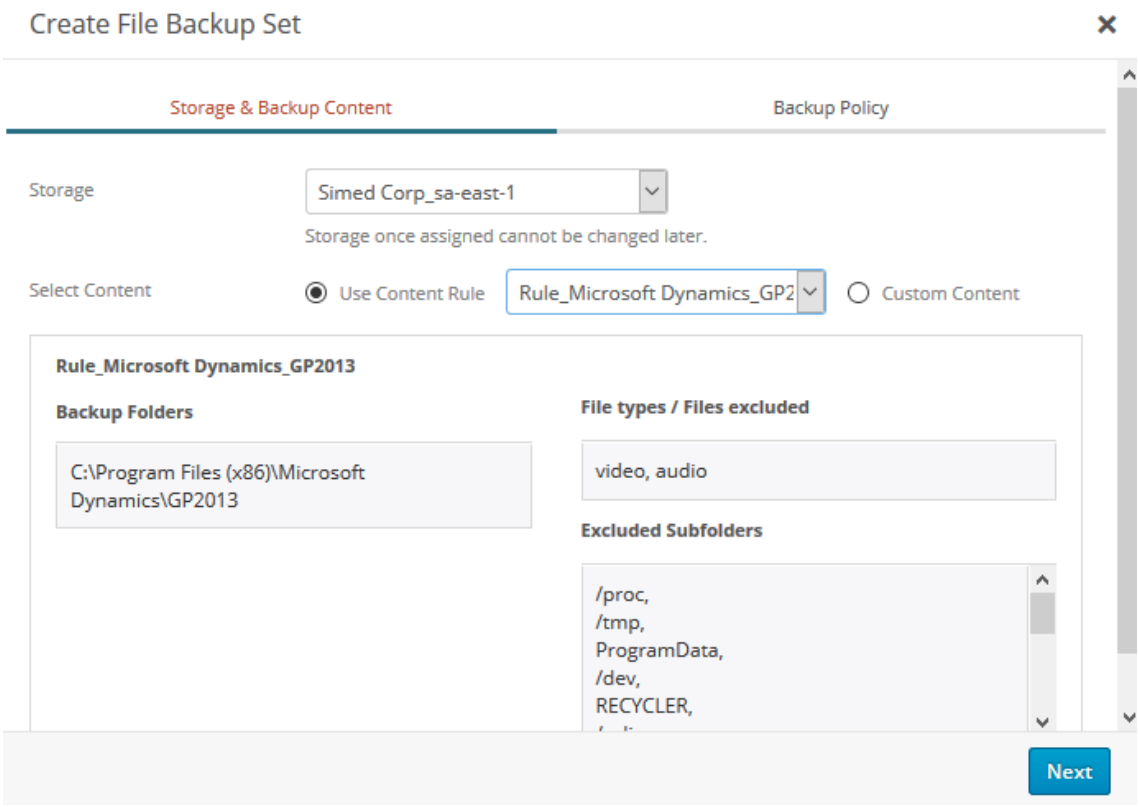


Figura 82. Selección de la regla de contenido para el servidor HORUS.

6. Se selecciona la política de respaldo definida en los pasos anteriores.

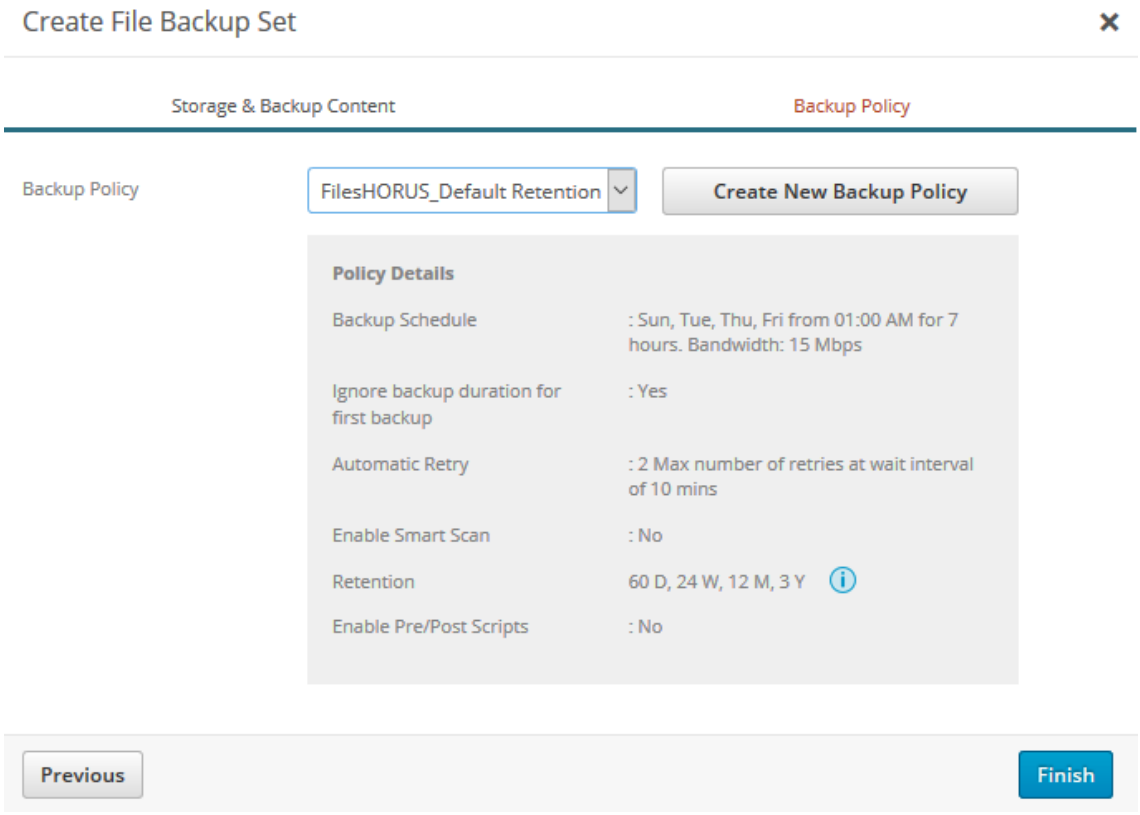


Figura 83. Selección de la política de respaldos para el servidor HORUS.

4.5.3 Pasos para configurar Phoenix para respaldar bases de datos.

En esta sección se explicará cómo es el proceso para respaldar el servidor de bases de datos OSIRIS. El proceso para configurar respaldos de bases de datos es casi igual al proceso realizado anteriormente para respaldos de archivos, resumiendo los pasos explicados en la sección 4.5.2 se tiene:

1. Crear Token en la consola de administración de Phoenix.
2. Instalación del agente Phoenix en el servidor OSIRIS.
3. Activación del servidor con el Token creado por Phoenix.
4. Creación de un grupo administrativo para este servidor, para este caso se creó el grupo administrativo llamado GroupBD.

5. A diferencia de los respaldos para servidores de archivos en los servidores de bases de datos no se trabaja con reglas de contenido puesto que se va a hacer un respaldo de las instancias instaladas.
6. Creación de la política de respaldos para el servidor HORUS, a diferencia de los servidores de archivos en este se puede programar tanto respaldos incrementales como respaldos completos. En esta regla se configurará de acuerdo con lo definido en la sección 4.2.3 en la tabla 42.

Policy Type	Backup Schedule	Retention
MS-SQL	***Full Backup:*** - Wed from 01:00 AM for 6 hours. Bandwidth: 15 Mbps ***Differential Backup:*** - Mon, Tue, Wed, Thu, Fri from 03:00 AM for 4 hours. Bandwidth: 15 Mbps	60D, 24W, 12M, 3Y

Figura 84. Política de respaldos para servidores de bases de datos.

7. Ir a Protección > MS-SQL SERVER
8. Seleccionar el servidor activado, para este caso OSIRIS.
9. Se da clic en Crear un conjunto de copias de SQL.
10. Se selecciona el almacenamiento.

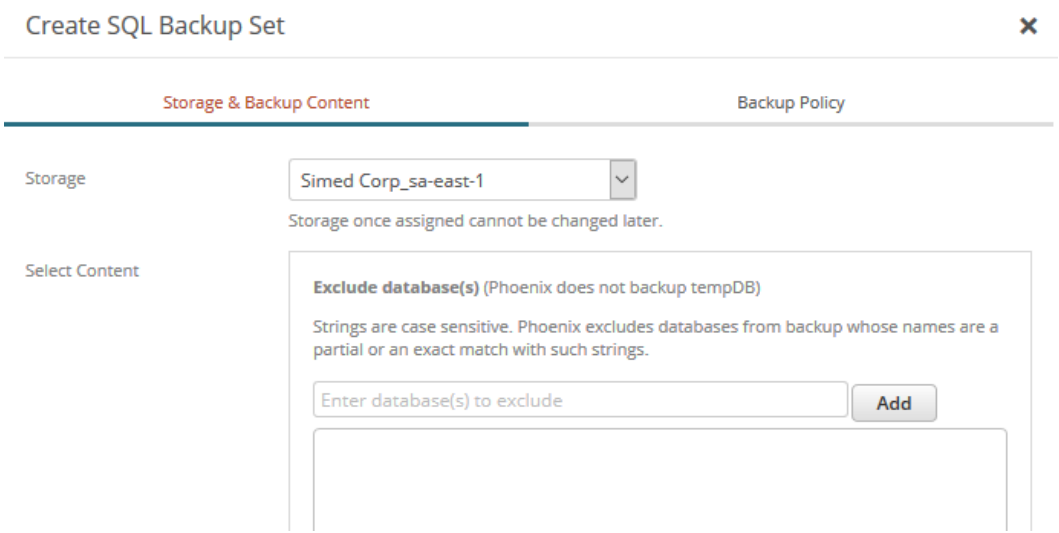


Figura 85. Selección del almacenamiento para los respaldos del servidor OSIRIS.

11. Se selecciona la política de respaldos a aplicarse para el servidor OSIRIS, en este caso es Backup Base de Datos_Default Retention.

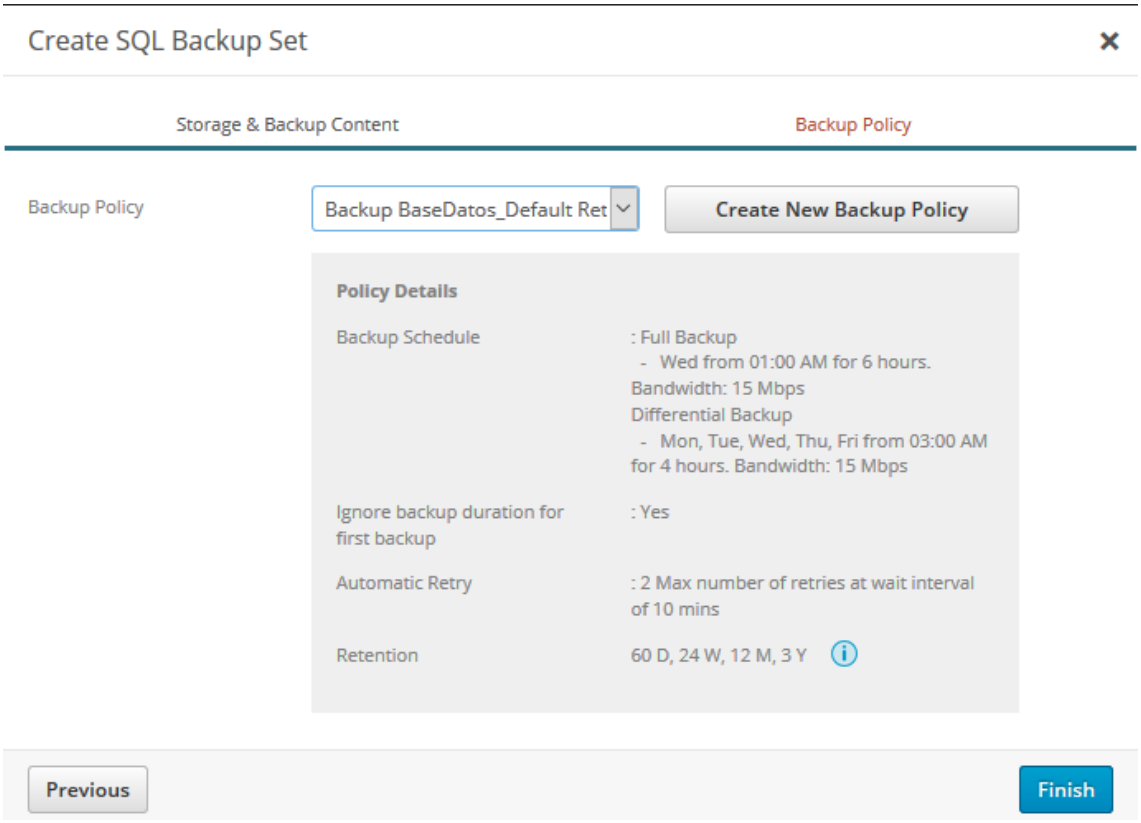


Figura 86. Selección de política de respaldos para servidor OSIRIS.

4.6 Implementación del Sistema de Respaldos de la Información para usuarios críticos con DRUVA inSync.

Druva inSync proporciona un único panel de control para proteger, preservar y descubrir información en dispositivos finales y aplicaciones en la nube, lo que ayuda a los clientes a aumentar drásticamente la disponibilidad y visibilidad de los datos críticos para la empresa a la vez que reduce costos, riesgos y complejidad.

1. **Protección de datos de dispositivos finales:**
   Copia de seguridad de alto rendimiento, borrado remoto y ubicación geográfica de computadoras portátiles y dispositivos inteligente.

2. **Copia de seguridad y archivo de la aplicación en la nube:** Protección y gobierno para Microsoft Office 365, G Suite, Box y Salesforce

3. **Monitoreo de cumplimiento de datos:**
   Identificación y remediación de riesgos de datos confidenciales en reposo (PHI, PII, PCI).

4. **Búsqueda Federada:**
   Ubicación rápida de archivos en puntos finales y aplicaciones en la nube.

5. **Migración del SO y actualización del dispositivo:**
   Gestión centralizada para migraciones a gran escala y actualizaciones de autoservicio

4.6.1 Pasos para configurar DRUVA inSync para respaldar información de usuarios.

En esta sección se definirá como es el proceso para respaldar información de usuarios a través de DRUVA inSync.
Los pasos por seguirse son los siguientes:

1. Ingresar a la Consola de Administración de DRUVA inSync, con el usuario y contraseña proporcionados después de la compra de la herramienta.

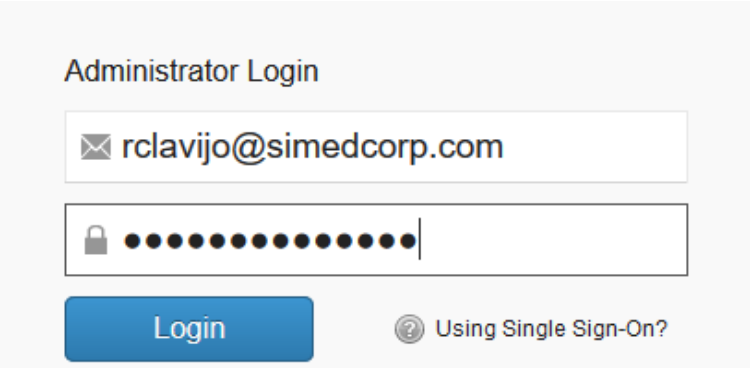


Figura 87. Ingreso al sistema de DRUVA InSync.

2. Dirigirse a la pestaña usuarios.

3. Dar clic en crear nuevo usuario.

4. Colocar el correo del usuario.

5. Colocar el nombre del usuario.

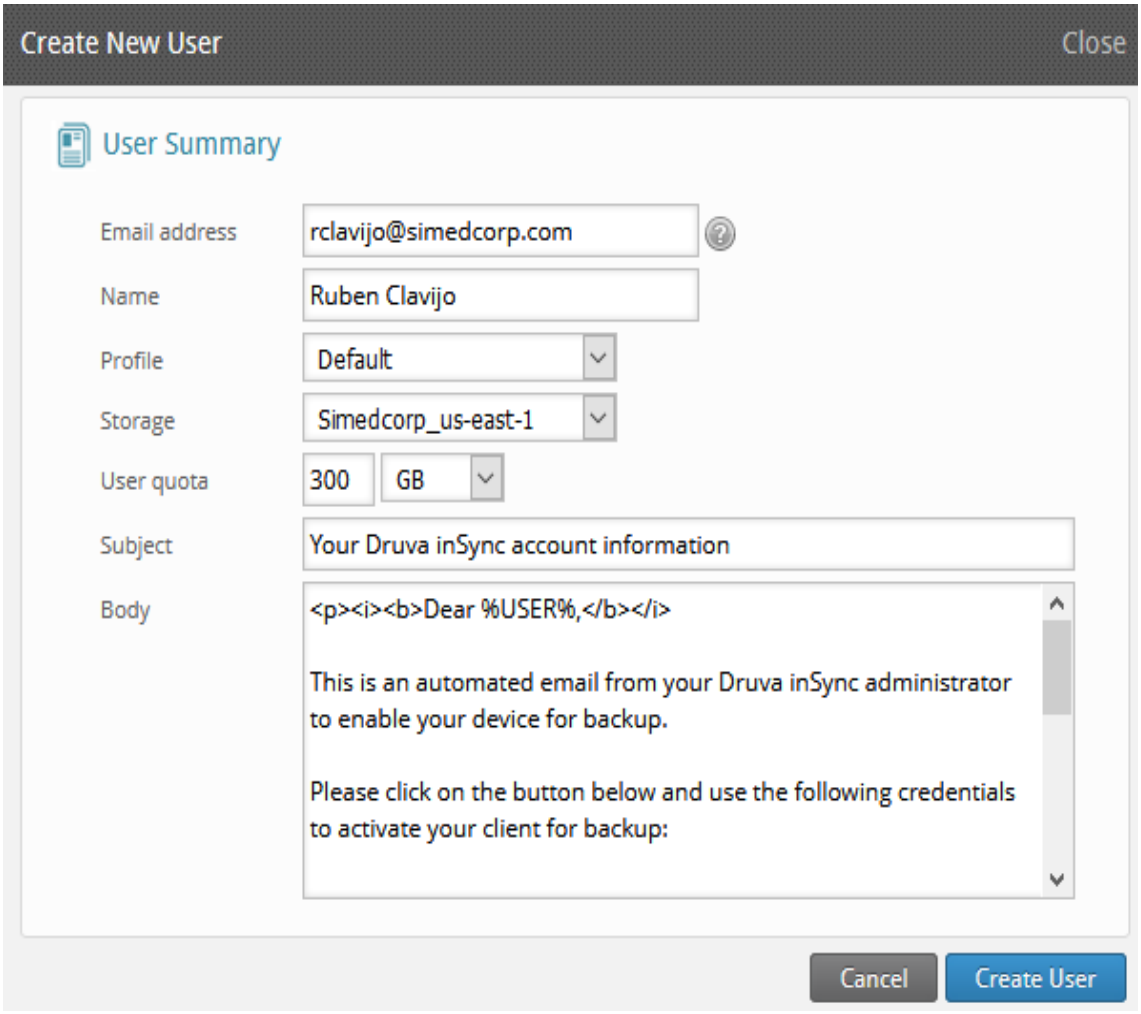


Figura 88. Creación de un nuevo usuario en Druva inSync.

6. Druva InSync enviará un correo con el usuario y contraseña temporal para la activación de dicha cuenta en computadora del usuario.

7. Se instala el agente de DRUVA InSync en la computadora del usuario.

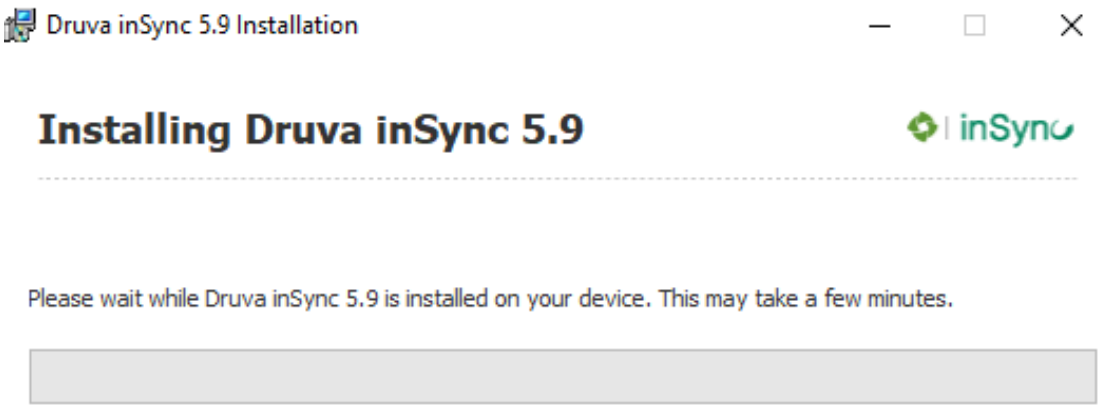


Figura 89. Instalación del agente de DRUVA InSync.

8. Al finalizar la instalación se despliega una ventana donde se debe ingresar el usuario y la contraseña enviadas al correo.

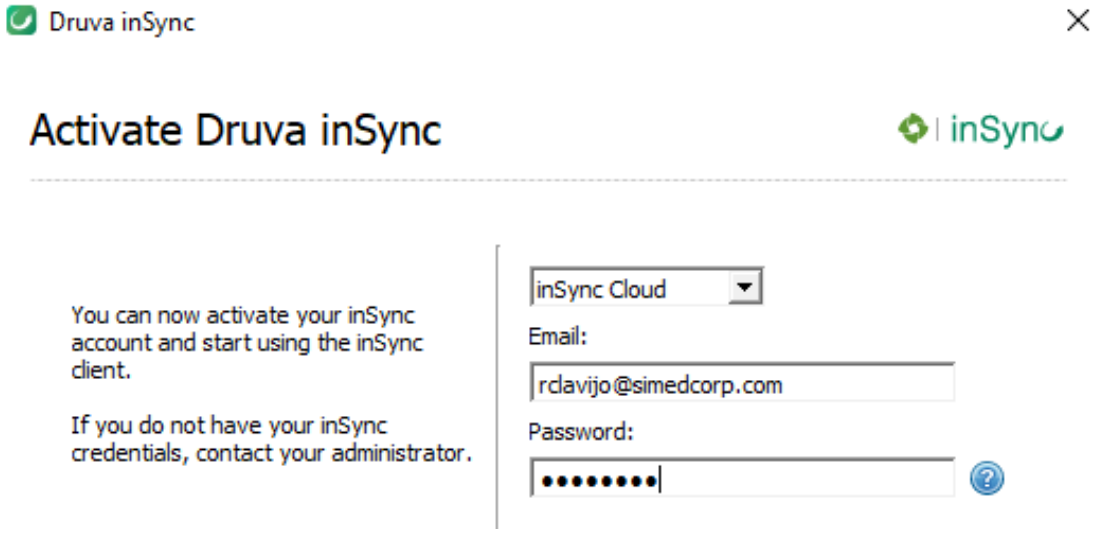


Figura 90. Iniciar el servicio de DRUVA InSync.

9. Comenzará el proceso de respaldo de la información. El respaldo que realiza DRUVA inSync es de toda la máquina.

5. Capítulo V. Pruebas de funcionamiento.

En este capítulo se realizará las pruebas de funcionamiento de la herramienta implementada en la empresa para la mesa de servicios *cloud* llamada SysAid, en donde se demostrará las funcionalidades de todos los parámetros anteriormente configurados. La otra sección de este capítulo de igual forma son las pruebas de funcionamiento en cuanto a la herramienta de sistema de respaldos *cloud* DRUVA, donde se verificarán pruebas de recuperación, se medirán los tiempos empleados en estas recuperaciones y el grado de recuperación de los datos obtenidos.

5.1 Pruebas de funcionamiento de la Mesa de Servicios SysAid.

Las pruebas de funcionamiento a realizarse en cuanto a SysAid son las siguientes:

- Prueba de funcionamiento del descubrimiento remoto a través del RDS implementado.

- Pruebas de funcionamiento para la creación de usuarios a través de la integración del servicio LDAP.

- Pruebas de funcionamiento de la integridad con correo electrónico Exchange Online.

- Pruebas de funcionamiento de la integración de Office365 con el calendario de SysAid.

- Pruebas de funcionamiento del despliegue del agente de SysAid a través del paquete de implementación MSI por medio de políticas de grupo.

- Pruebas de funcionamiento de la visibilidad en el portal del usuario final de la categorización de servicios configurada.

- Pruebas de funcionamiento de enrutamiento de incidentes y solicitudes al técnico responsable del servicio.

- Pruebas de funcionamiento de la asignación automática de una prioridad a un registro de servicio de acuerdo con la matriz de prioridades configurada.

- Pruebas de funcionamiento de las fechas de vencimiento para un registro de servicio.

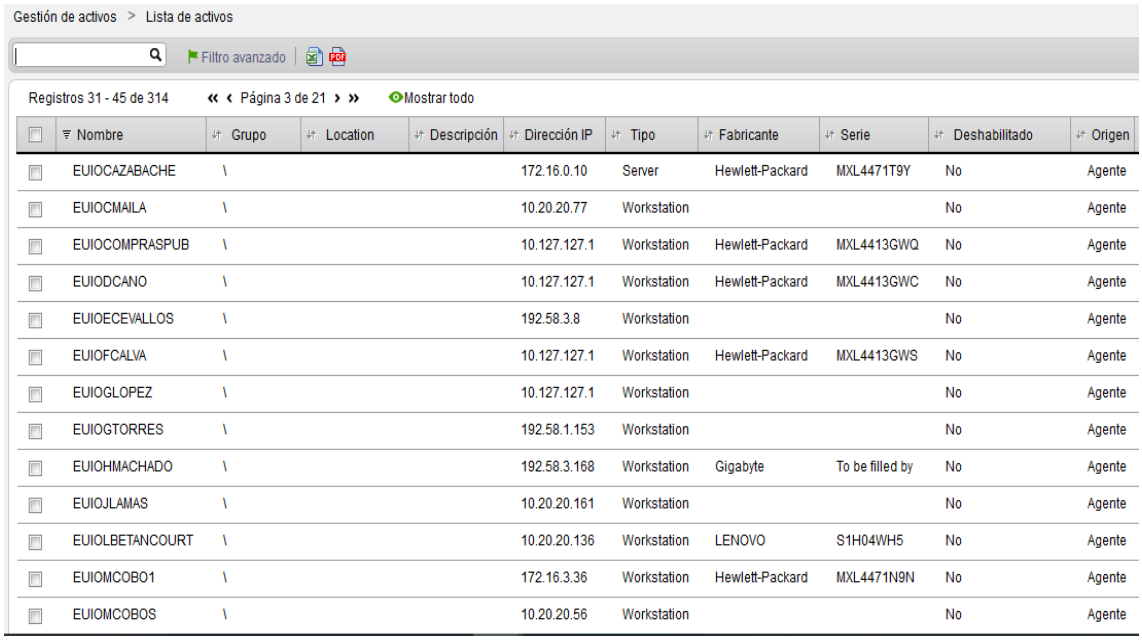
- Pruebas de funcionamiento de las reglas de escalamiento implementadas.

- Pruebas de funcionamiento de las plantillas de incidentes y problemas creados.

5.1.1 Prueba de funcionamiento del descubrimiento remoto a través del RDS implementado.

Como se indicó en la sección 3.5.3 Configuración del Servicio de Descubrimiento Remoto de SysAid por medió de *Remote Discovery Service* (RDS), se puede gestionar los activos de la empresa ya que al realizar un descubrimiento de los equipos que se encuentran en la red, trae los datos de todos estos al portal web de SysAid.

Para acceder a esta información se debe ir a Activos > Lista de activos. Después de haber implementado este servicio de descubrimiento remoto a través del RDS se obtuvo los datos de todos los activos que se encuentran en la red de la empresa tanto de servidores como de estaciones de trabajo de los usuarios. A continuación, en la figura 91 se puede observar la prueba del descubrimiento y gestión de estos activos.



Nombre	Grupo	Location	Descripción	Dirección IP	Tipo	Fabricante	Serie	Deshabilitado	Origen
EUIOCAZABACHE	\			172.16.0.10	Server	Hewlett-Packard	MXL4471T9Y	No	Agente
EUIOCMAILA	\			10.20.20.77	Workstation			No	Agente
EUIOCOMPRASPUB	\			10.127.127.1	Workstation	Hewlett-Packard	MXL4413GWQ	No	Agente
EUIODCANO	\			10.127.127.1	Workstation	Hewlett-Packard	MXL4413GWC	No	Agente
EUIOECEVALLOS	\			192.58.3.8	Workstation			No	Agente
EUIOFCALVA	\			10.127.127.1	Workstation	Hewlett-Packard	MXL4413GWS	No	Agente
EUIOGLOPEZ	\			10.127.127.1	Workstation			No	Agente
EUIOGTORRES	\			192.58.1.153	Workstation			No	Agente
EUIOHMACHADO	\			192.58.3.168	Workstation	Gigabyte	To be filled by	No	Agente
EUIOJLAMAS	\			10.20.20.161	Workstation			No	Agente
EUIOLBETANCOURT	\			10.20.20.136	Workstation	LENOVO	S1H04WH5	No	Agente
EUIOMCOBO1	\			172.16.3.36	Workstation	Hewlett-Packard	MXL4471N9N	No	Agente
EUIOMCOBOS	\			10.20.20.56	Workstation			No	Agente

Figura 91. Lista de activos de la empresa.

Como se puede observar en este listado cuenta con 314 activos de la empresa en donde se obtiene:

- Nombre de la máquina
- Dirección IP.
- Tipo
- Fabricante
- Número de serie

Una información valiosa a la hora de gestionar activos, pero se puede precisar aún más con SysAid debido a que tiene la opción de abrir el detalle de cada activo, donde se mostrará información más completa. Se obtiene parámetros adicionales como: sistema operativo, CPU, memoria, pantalla, almacenamiento, red, entre otros.

En la Figura 92 se puede observar información en detalle de un activo, indica nombre de la máquina (EUIOGLOPEZ), sistema operativo (Windows 8.1 Pro), CPU (Intel Core i3), memoria RAM (3996 Mb), pantalla (Intel HD), almacenamiento (466 Gb) y red (Adaptador TAP Windows).

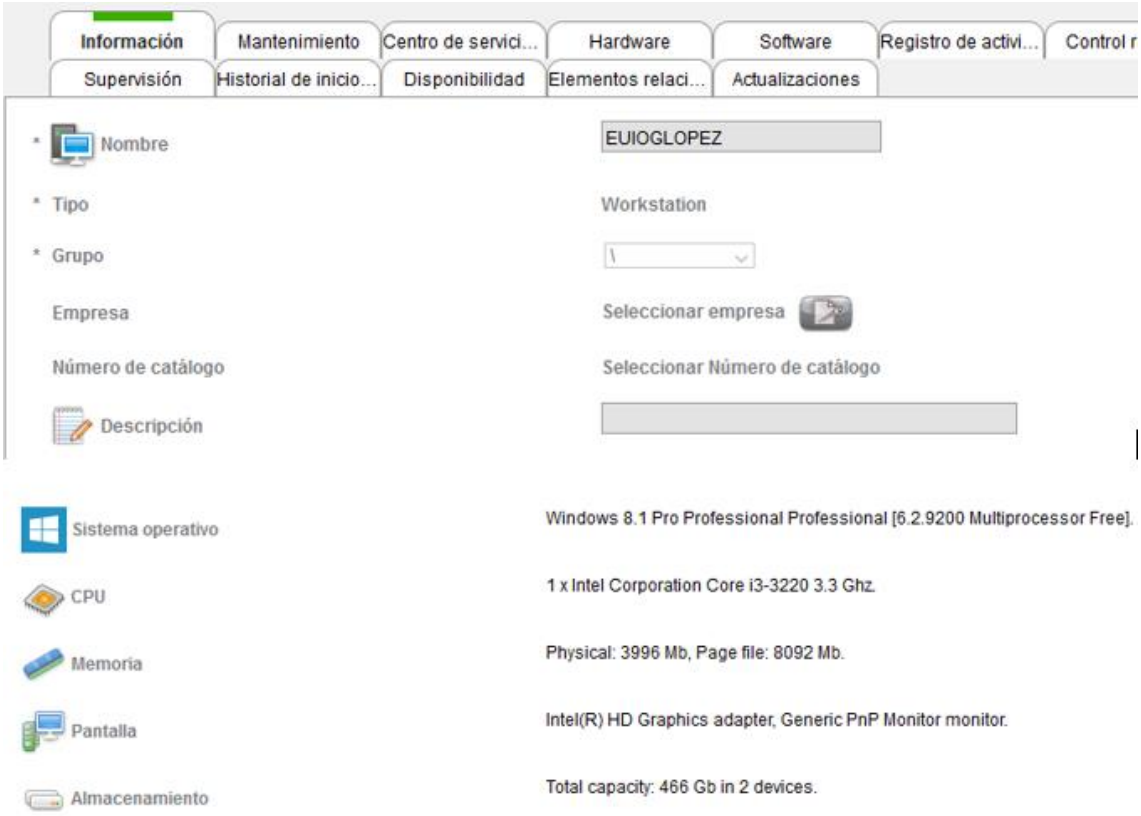


Figura 92. Detalle de un activo descubierto por RDS en SysAid.

5.1.2 Pruebas de funcionamiento para la creación de usuarios a través de la integración del servicio LDAP

Después de haber realizado la integración con LDAP se puede observar que es exitosa, ya que la misma trae toda la estructura de usuarios del directorio activo a SysAid, en la figura 93 a continuación se puede observar las unidades organizativas cargadas en SysAid después de la correcta integración LDAP.

En esta sección se puede quitar a las unidades organizativas que no sean necesarias para SysAid con el fin de registrar en el sistema solo los usuarios que verdaderamente vayan a usar el servicio de mesa de ayuda.

Por ejemplo, en las empresas cuando sale un usuario este no se lo borra si no que deshabilita por lo cual LDAP también traerá desde el AD a estos usuarios.

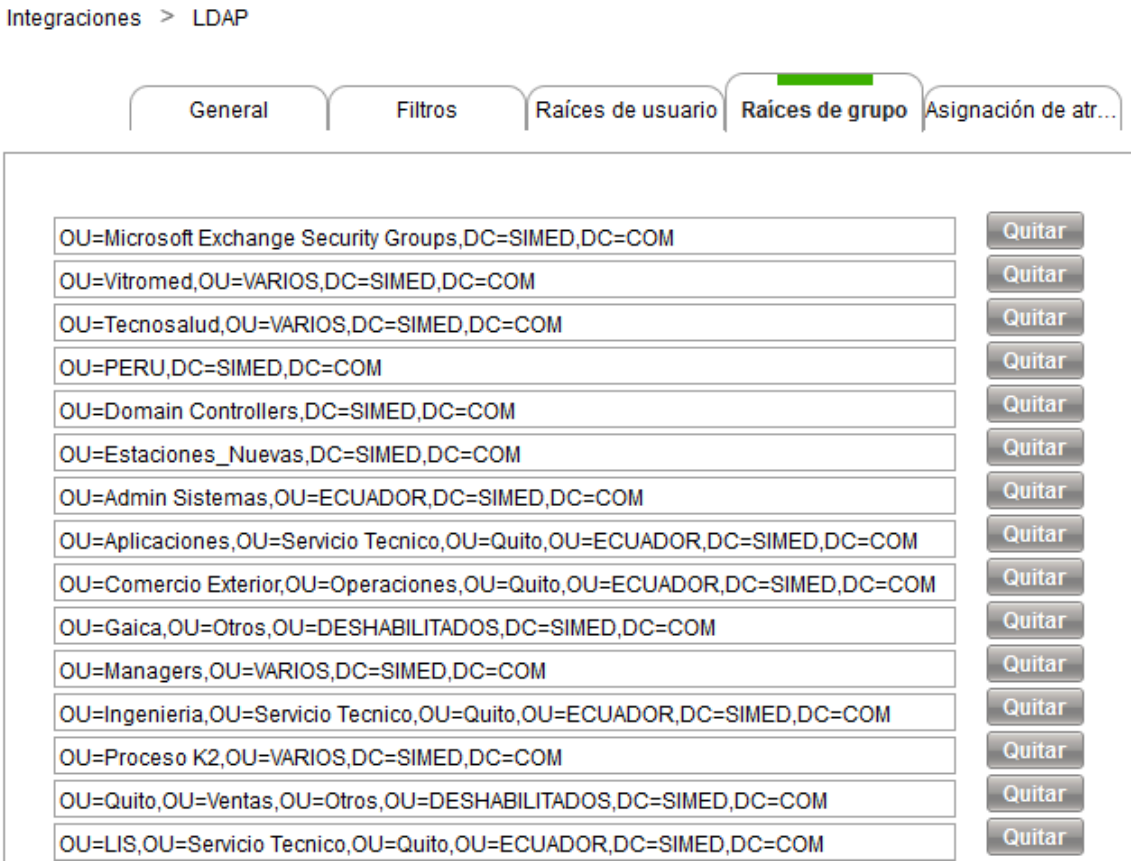


Figura 93. Unidades organizativas del directorio activos después de la integración con LDAP.

Otra prueba del correcto funcionamiento de la integración con LDAP es el ingreso al portal web de SysAid con los usuarios del directorio activo.

5.1.3 Pruebas de funcionamiento de la integridad con correo electrónico Exchange Online

De la configuración de integridad con correo electrónico como se mencionó en la sección anterior esto permite que SysAid envíen diversas notificaciones por medio de la cuenta de correo electrónico establecida.
Dentro de dichas notificaciones enviadas por SysAid se tiene:

- Crear nuevos incidentes a partir de correos electrónicos entrantes.}
- Registrando toda la correspondencia por correo electrónico relacionada con un registro de servicio específico.

- Envío de notificaciones automatizadas a usuarios finales y administradores.

Para la prueba de funcionamiento a continuación se puede observar en la figura 94 el envío de una notificación por correo electrónico al grupo de administradores de la mesa de ayuda cuando un usuario final crea un nuevo incidente.

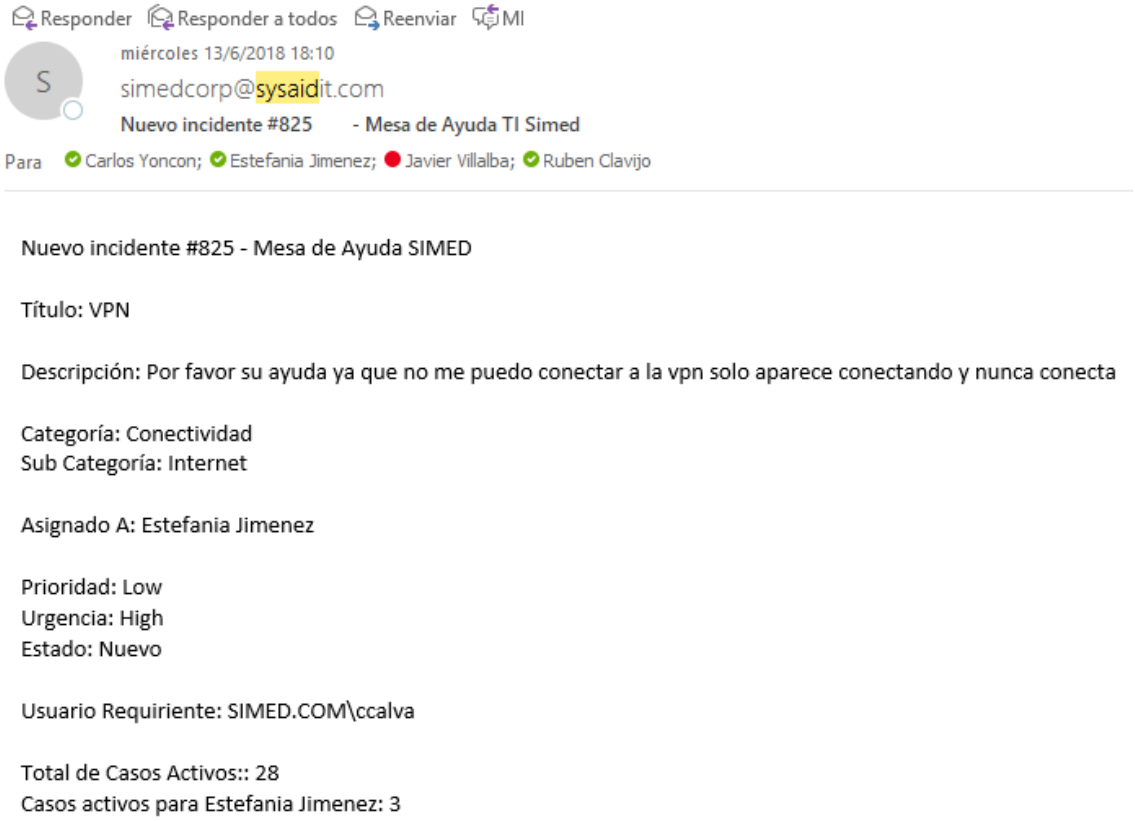


Figura 94. envío de notificación de nuevo incidente por correo hacia el grupo de administradores del sistema.

5.1.4 Pruebas de funcionamiento de la integración del calendario de Office365 con el calendario de SysAid

Para el escenario de esta prueba de funcionamiento un administrador de la mesa de servicio Rubén Clavijo entra al portal de SysAid, se dirigirá a la sección de Herramientas > Mi calendario, y procederá a crear un evento para el lunes 11 de junio con el título de “Actualizaciones de servidor de bases de datos”.

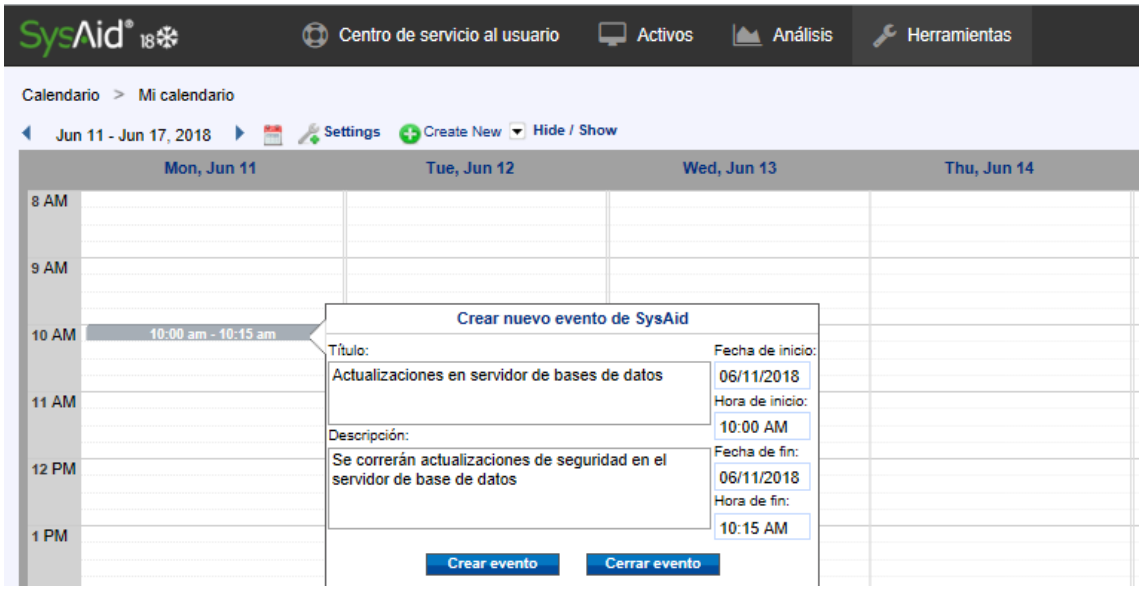


Figura 95. Creación de evento el calendario SysAid del administrador Rubén Clavijo.

Este evento creado en el calendario de SysAid se replicará automáticamente el calendario de Outlook del administrador, esto se pude observar en la Figura 96 más adelante.

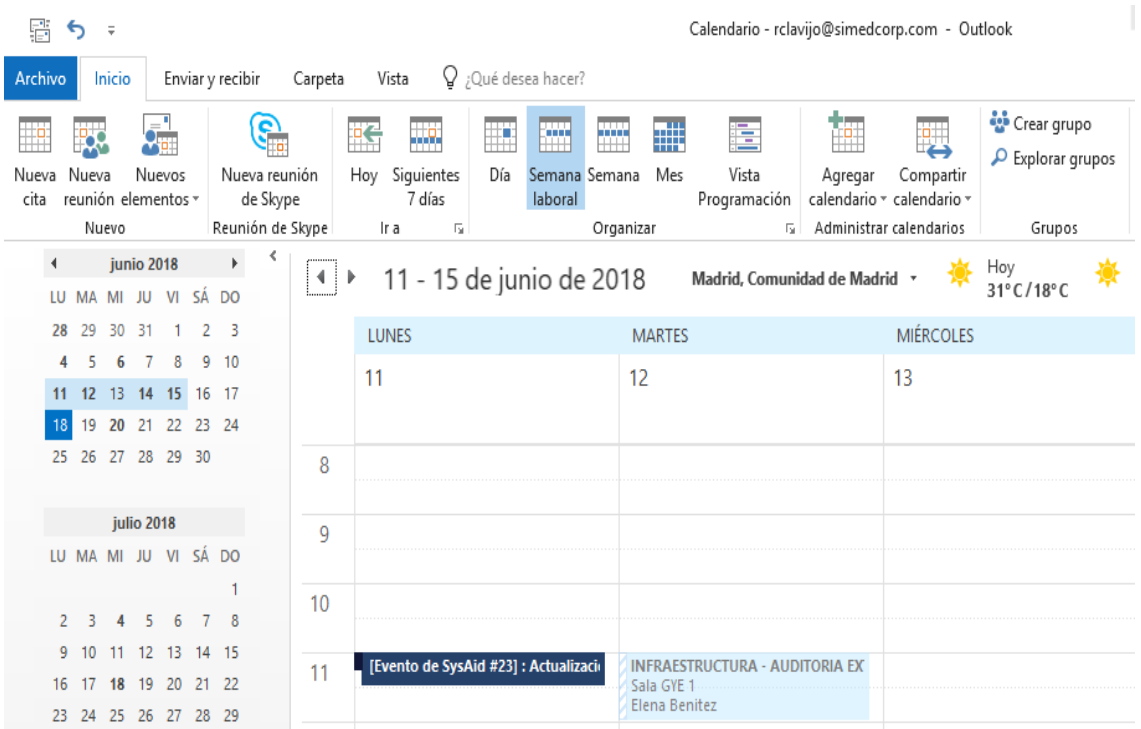


Figura 96. Replicación de calendario SysAid en Outlook.

5.1.5 Pruebas de funcionamiento del despliegue del agente de SysAid a través del paquete de implementación MSI por medio de políticas de grupo.

Después de haber creado el instalador del agente, este se lo despliega a través de políticas de grupo para que se cargue en todas las estaciones de trabajo del dominio. En la figura 97 está aplicada la política a nivel de toda la organización.

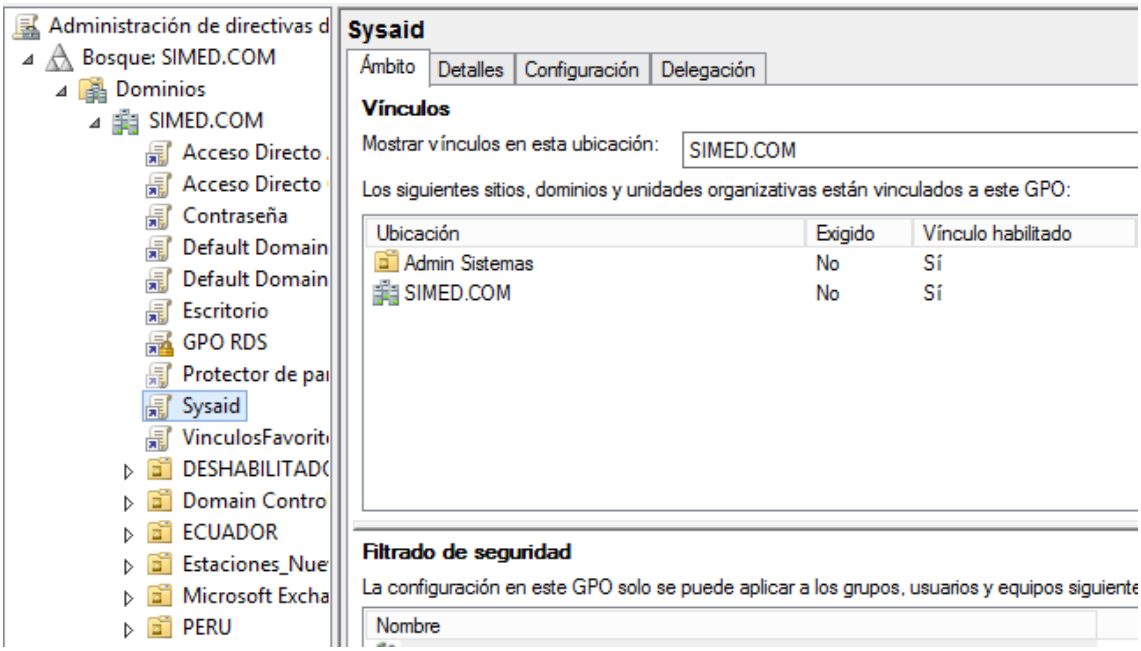


Figura 97. Aplicación de GPO para instalar agente de SysAid aplicada a todo el dominio.

Si la aplicación de la GPO es correcta cuando cualquier usuario de la red inicie sesión de nuevo el agente de SysAid procederá a instalarse y se creará un ícono de acceso directo hacia el portal de usuario final de SysAid. Además, una vez instalado el agente en la estación de trabajo se habilita la opción de control remoto sobre ese activo para una gestión remotas de los administradores de la mesa de ayuda con los usuarios finales.

Por otro lado, también se dispone de la opción de abrir el portal web con la tecla de acceso rápido F11, cuando se abre el sistema de esta forma al crear un incidente o solicitud nuevo por defecto se adjuntará una captura de pantalla del

momento cuando se presionó la tecla F11. En la figura 98 se observa el ícono de acceso directo cargado en una estación de trabajo para el acceso a SysAid.

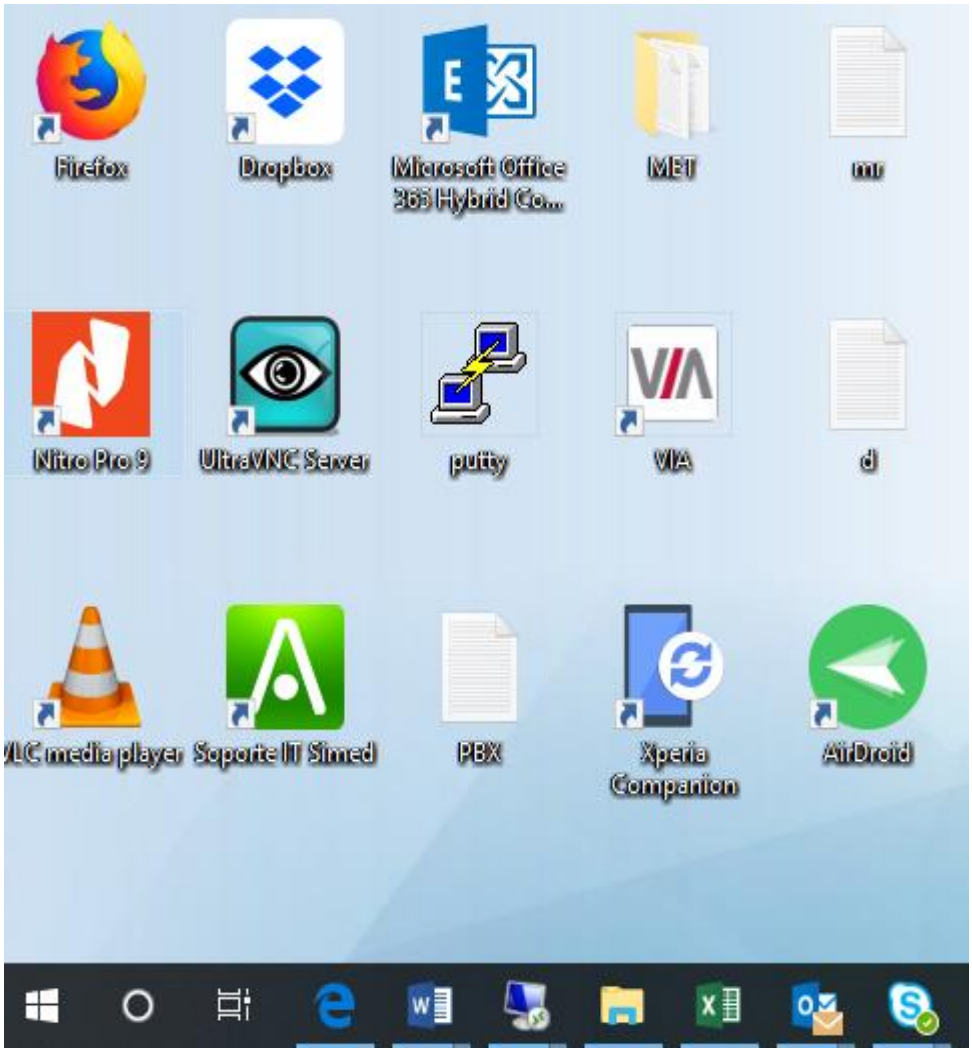


Figura 98. Acceso directo al sistema de SysAid cargado en escritorio por GPO.

5.1.6 Pruebas de funcionamiento de la visibilidad de la clasificación de los servicios de TI por categorías en el portal de creación de incidentes y solicitudes del usuario final.

Cuando un usuario final va a crear una solicitud o incidente de servició en la plantilla de ingreso tendrá la opción de escoger una categoría, subcategoría, y tercer nivel de acuerdo con la estructura de categorización anteriormente establecida. En la Figura 72 se puede observar cómo se presentan las categorías para el usuario final.

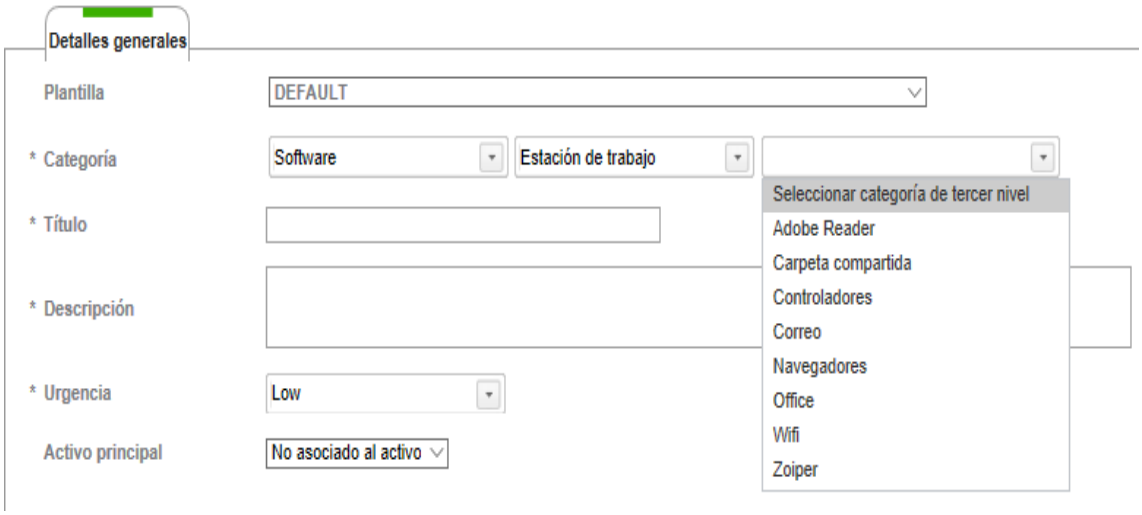


Figura 99. Categorías, subcategorías y tercer nivel de servicios.

En este caso se puede observar que está elegido la categoría “Software”, la subcategoría “Estación de trabajo” y se encuentra desplegado el listado de categorías de tercer nivel.

5.1.7 Pruebas de funcionamiento de reglas de enrutamiento, prioridades, fechas de vencimiento y reglas de escalamiento.

Para la realización de pruebas de todas estas configuraciones mencionadas se va a crear un escenario completo desde la creación de un incidente por parte del usuario final, la asignación de este registro de servicio a un administrador de nivel 1 de la mesa de servicios, el seguimiento de dicho servicio por parte del administrador asignado desde el portal para administradores de SysAid, se verificará que el cálculo de prioridad se realiza automáticamente en base a la matriz de prioridades configurada, se verificará que se establece una fecha de vencimiento del registro de servicio automáticamente, para realizar la prueba de escalamiento se dejará que el registro llegue a su fecha de vencimiento para analizar el escalamiento del mismo. Por último, el administrador de nivel 2 al que se le reasignó el caso lo gestionará desde su portal de administración.

Todo este proceso va de acuerdo con las configuraciones que se han venido realizando en la etapa del diseño del modelo de respaldos.

1. Ingresa al sistema el usuario final Antonio Llorente

2. Una vez ingresado el usuario tiene las siguientes opciones

    - Enviar un incidente
    - Enviar una solicitud
    - Ver solicitudes de servicio
    - Entrar a la Base de Datos de Conocimiento.
    - Ingresar al Calendario de SysAid
    - Configurar Acciones de flujo de trabajo.

Figura 100. Portal de usuarios finales de SysAid.

3. Para esta prueba se enviará un incidente.

4. El usuario final debe llenar los siguientes campos:

    - Seleccionar una categoría del servicio: software.
    - Seleccionar una subcategoría del servicio: aplicaciones empresariales.
    - Seleccionar una categoría de tercer nivel: Microsoft Dynamics GP
    - Ingresar un título: Fallo en el módulo de ventas
    - Ingresar una descripción: No se pueden ingresar nuevas ventas

- Seleccionar que tipo de urgencia: crítica
- Tiene la opción de adjuntar algún documento referente al incidente.

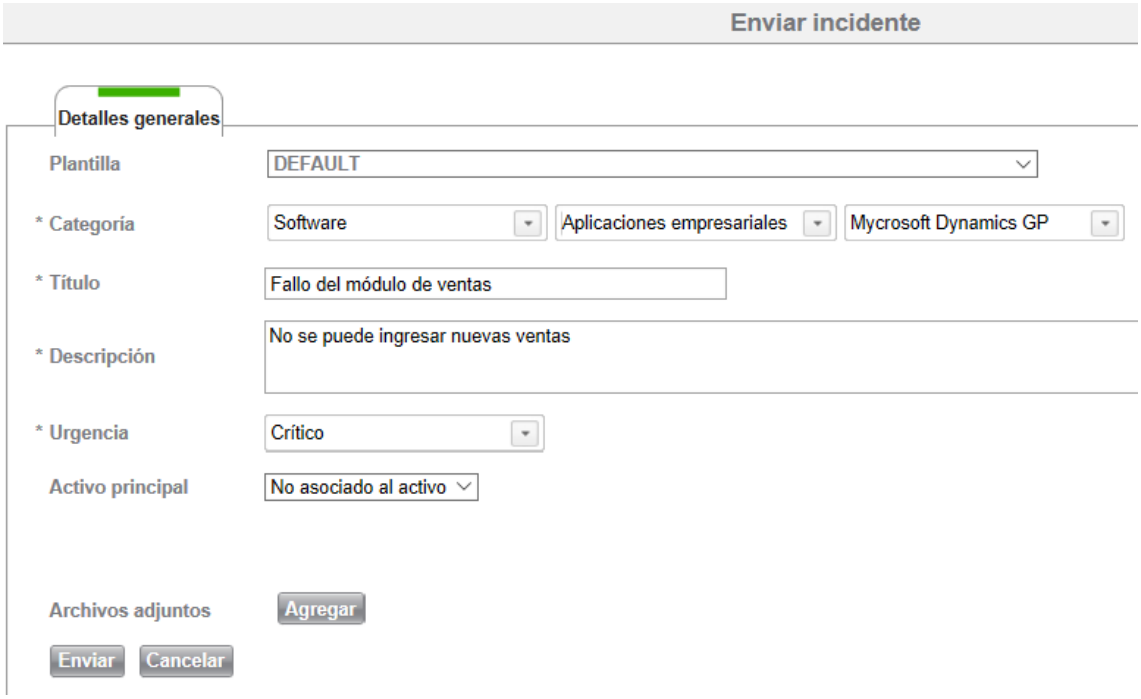


Figura 101. Creación de un nuevo incidente.

5. Se aplica la regla de enrutamiento. Según lo configurado al ser un incidente de la subcategoría “aplicaciones empresariales” debe asignarse al administrador Javier Villalba.

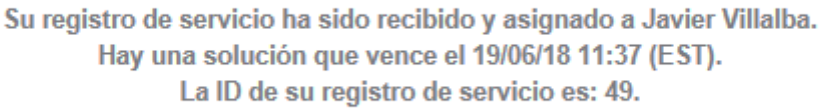


Figura 102. Se aplica regla de enrutamiento.

6. El administrador asignado ingresa al portal de administración para atender el registro de servicio. En la sección de incidentes ya puede observar este nuevo registro de servicio asignado. Del servicio asignado se tiene los siguientes datos:

- **ID de registro:** 49
- **Alerta:** círculo de color rojo al tratarse de una prioridad crítica
- **Categoría, subcategoría, título**
- **Estado:** nuevo
- **Usuario de solicitud:** Antonio Llorente
- **Asignado a:** Javier Villalba
- **Prioridad:** crítico, esta prioridad se asignó automáticamente de acuerdo con la matriz de prioridades, debido a que el usuario Antonio Llorente estableció una urgencia crítica y esta categoría tiene un impacto crítico por lo tanto se obtiene una prioridad crítica.
- **Hora de solicitud:** 06/18/2018 06:37:21 PM

Figura 103. Datos del incidente 49.

7. El administrador debe abrir el incidente asignado donde encontrará se tiene datos y opciones adicionales como:

- **Notas**
- **Fecha de vencimiento:** para este caso al tratarse de una prioridad crítica se tiene configurado 60 minutos para el vencimiento. Se puede observar en la siguiente figura que la fecha de vencimiento se estableció para el 06/18/2018 07:37:21 PM, 60 minutos más tarde de la hora de solicitud.

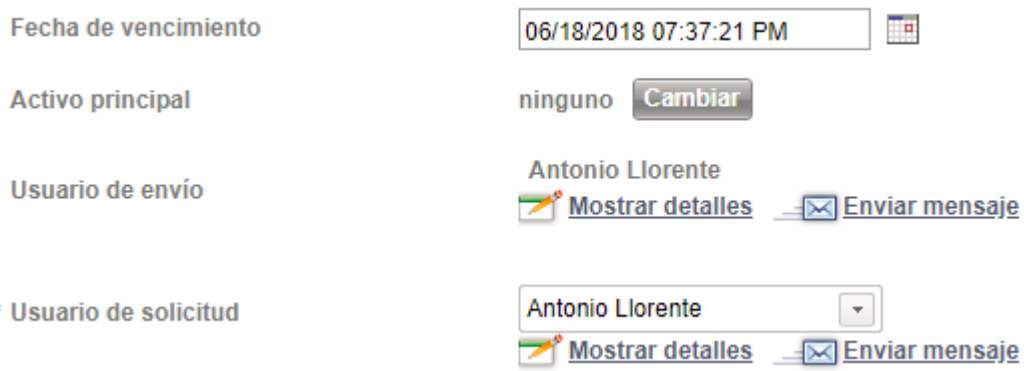


Figura 104. Fecha de vencimiento del incidente.

- **Chat y control remoto con usuario final:** se tiene la opción de iniciar un chat con el usuario que solicitó el servicio y también la opción del control remoto.

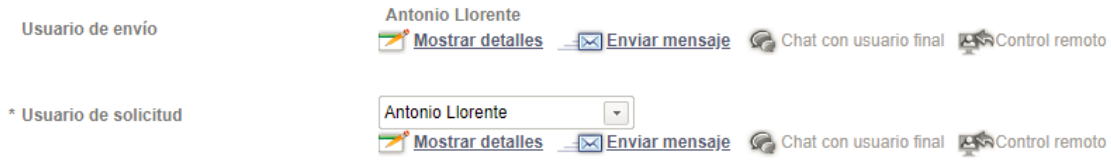


Figura 105. Chat y control remoto con usuario final.

.

- **Chat y control remoto con usuario final:** se tiene la opción de iniciar un chat con el usuario que solicitó el servicio y también la opción del control remoto.
- **Buscar en la base de datos de conocimiento:** el administrador tiene la opción de buscar si existe un incidente, solicitud o problema parecido o el mismo en la KDB.

8 El administrador en esta pantalla es donde debe solucionar y cerrar los registros de servicio, pero para la demostración de las reglas de escalamiento no se cerrará el registro de este ejemplo. Por lo tanto, se aplicará las reglas de escalamiento establecidas en la implementación. La regla que aplica en este registro es la reasignación del caso después de llegar a la fecha límite que (60 min) y no obtener una solución, se

escala al administrador de la mesa de ayuda de nivel 2 Andrés Jurado debido a qué está dentro de la categoría “Aplicaciones empresariales”. Cuando se produce el escalamiento en la pantalla de listas de registros se puede notar algunos cambios:

- La alerta cambia a signo de registro escalado.
- En la sección asignado a: ya se encuentra el nuevo administrador responsable.

Figura 106. Incidente escalado.

8. El administrador de nivel 2 al que se le reasignó el caso puede ver este desde su portal de administración y proceder a solucionarlo. Cuando un técnico ya llega a la solución de un caso debe cerrar para lo cual debe cambiar el estado del registro a cerrado. En la figura 107 se puede observar cómo se cambia de estado a un registro.

Figura 107. Cambio de un registro a cerrado.

9. El administrador después de cambiar el estado de un registro a cerrado debe colocar que hizo para solucionar, cuando guarda esto SysAid pregunta si desea guardar dicha información en la base de datos de conocimiento, donde es decisión del técnico dependiendo de la relevancia de la información.

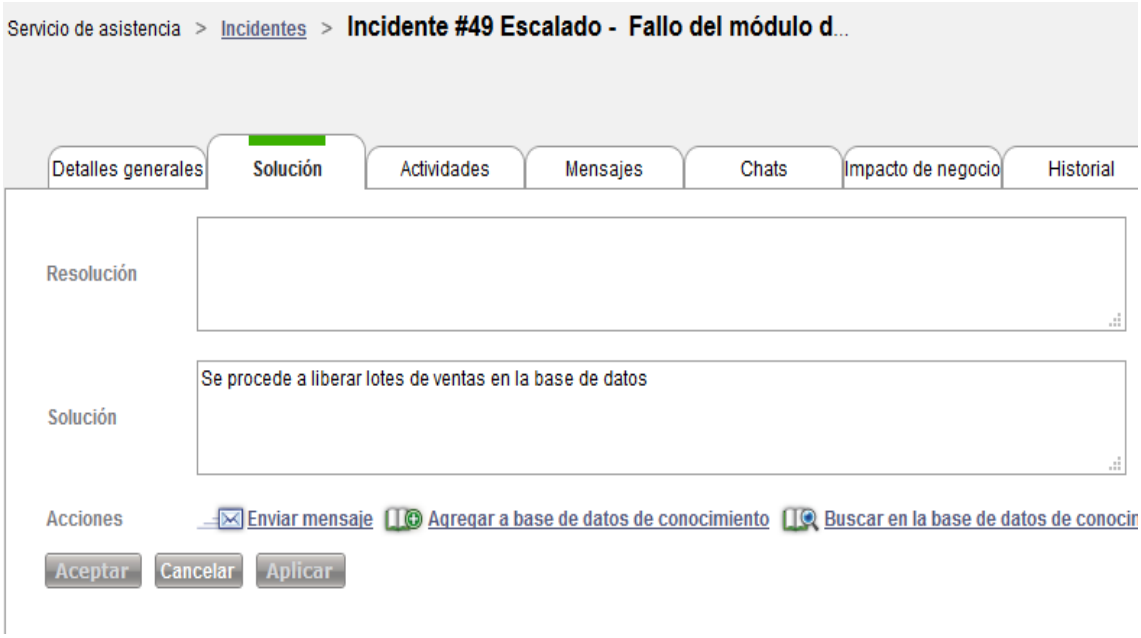


Figura 108. Solución de un registro.

5.1.8 Pruebas de funcionamiento de la gestión de problemas.

Como se mencionó en la sección Diseño de la Gestión de Problemas en la herramienta debe tener la opción de:

- Detección de problemas
- Registrar problemas
- Categorizar problemas
- Priorizar problemas
- Resolver problemas
- Cerrar problemas

En el portal de SysAid dirigirse a Centro de servicio al usuario > Problemas > Agregar nuevo problema.

En esta sección se puede configurar todo lo propuesto en el diseño, para este caso se resolverá un problema hallado en la fase de análisis de la situación actual de la mesa de servicios. El problema es con las videollamadas a través

del sistema POLYCOM. Para lo cual en la ventana abierta se llenaron los siguientes campos:

- Categoría: Software
- Subcategoría: POLYCOM
- Categoría de tercer nivel: No realiza la llamada
- Estado: Nuevo
- Gestor del proceso: Carlos Yoncón
- Solicitud: Carlos Yoncón
- Impacto: Medio
- Urgencia: Medio
- Prioridad: Medio

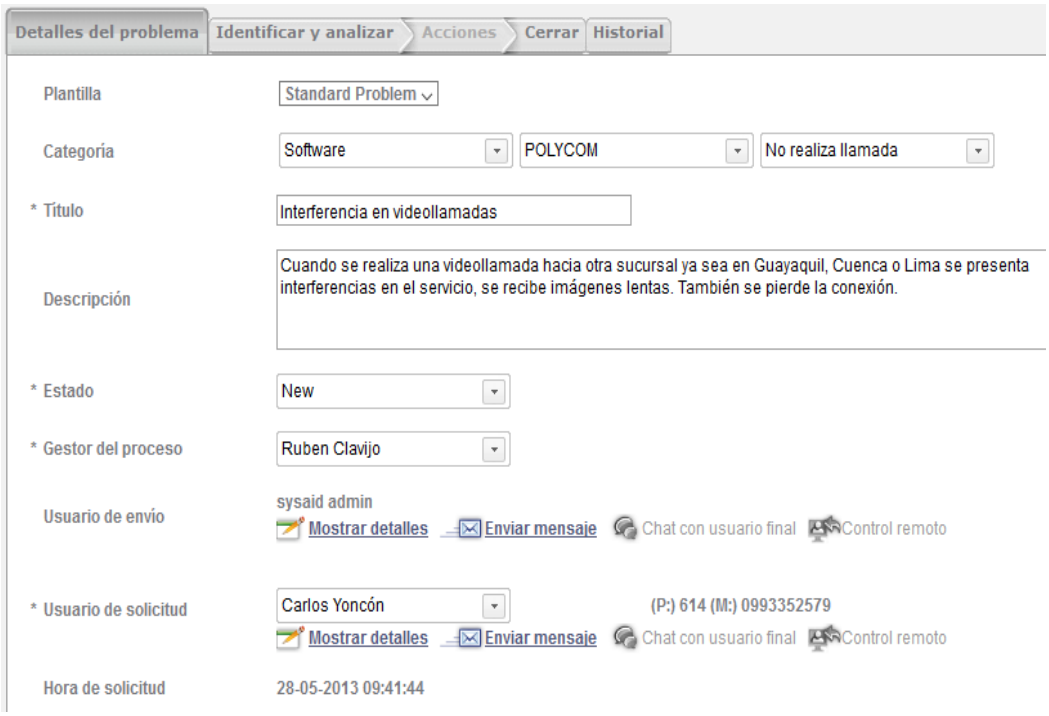


Figura 109. Registro de un problema.

Para cerrar el problema se debe colocar cuál fue el procedimiento para solventarlo, cambiar el estado ha cerrado.

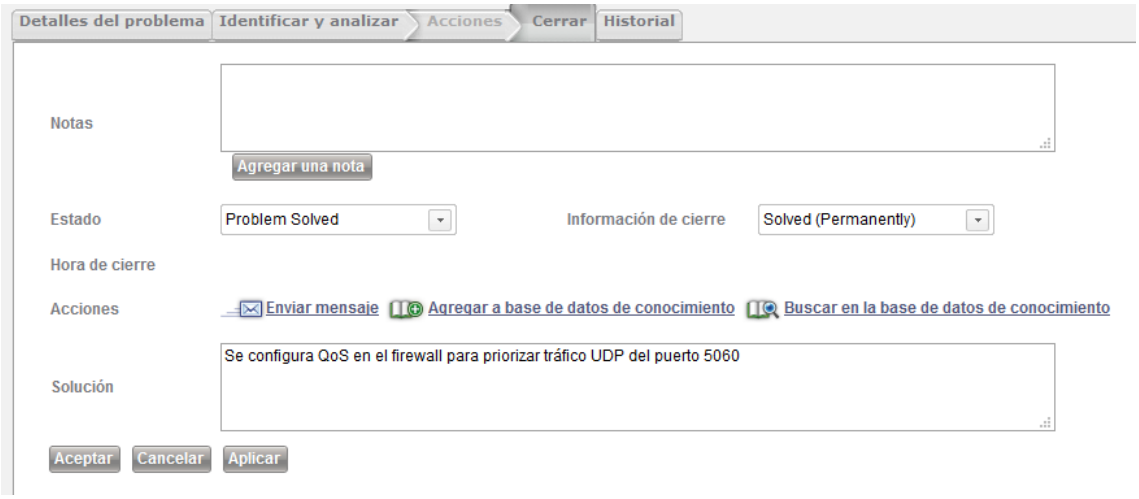


Figura 110.Cerrar un problema.

5.1.9 Pruebas de funcionamiento de la gestión de eventos.

Como se mencionó en la sección de Gestión de Eventos la herramienta debe tener opciones de trabajar con monitoreos de equipo, alertas y avisos a usuarios de cuando se vaya a realizar algún mantenimiento que vaya a producir una para a algún servicio.

5.1.9.1 Monitoreo de servidores.

En la Figura 111 se puede observar cómo se encuentra configurado el monitoreo de un servidor en el cual se maneja un umbral para el uso del CPU.

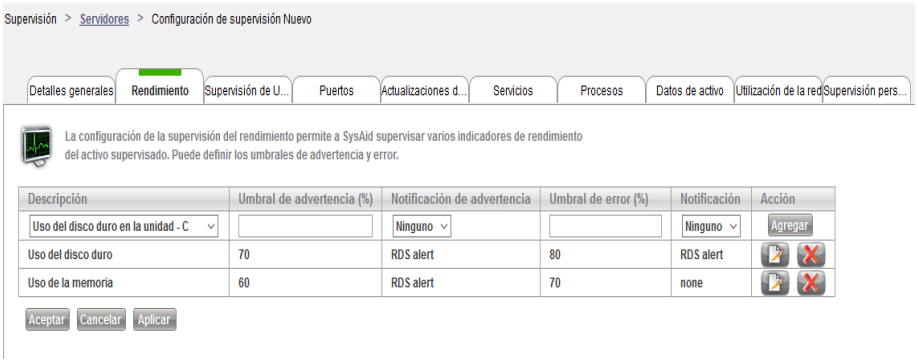


Figura 111. Monitoreo y alertas de activos.

5.1.9.2 Creación de eventos mostrados en los calendarios de los usuarios finales.

De acuerdo con lo planteado debe poder notificarse a los usuarios cuando un servicio vaya a entrar en mantenimiento. Para esto en el calendario de SysAid se crea eventos con las indicaciones respectivas, los cuales aparecerán en los calendarios de los usuarios finales.

Con esto un colaborador va a conocer de ante mano cuando no estará disponible algún servicio, por ejemplo, si se va a realizar el mantenimiento de las impresoras se creará un evento previamente el cual se programará para la fecha correspondiente y será visible por todos los usuarios, con lo cual sabrán que día se dará dicho mantenimiento.

En la Figura 112 se puede observar la creación de un evento en cual se programa para la fecha martes 12 de junio a las 9:00 AM hasta las 10:00 AM en donde se indica que se realizará el mantenimiento a las impresoras de la empresa. Este evento se sincronizará en todos los calendarios de los usuarios finales.

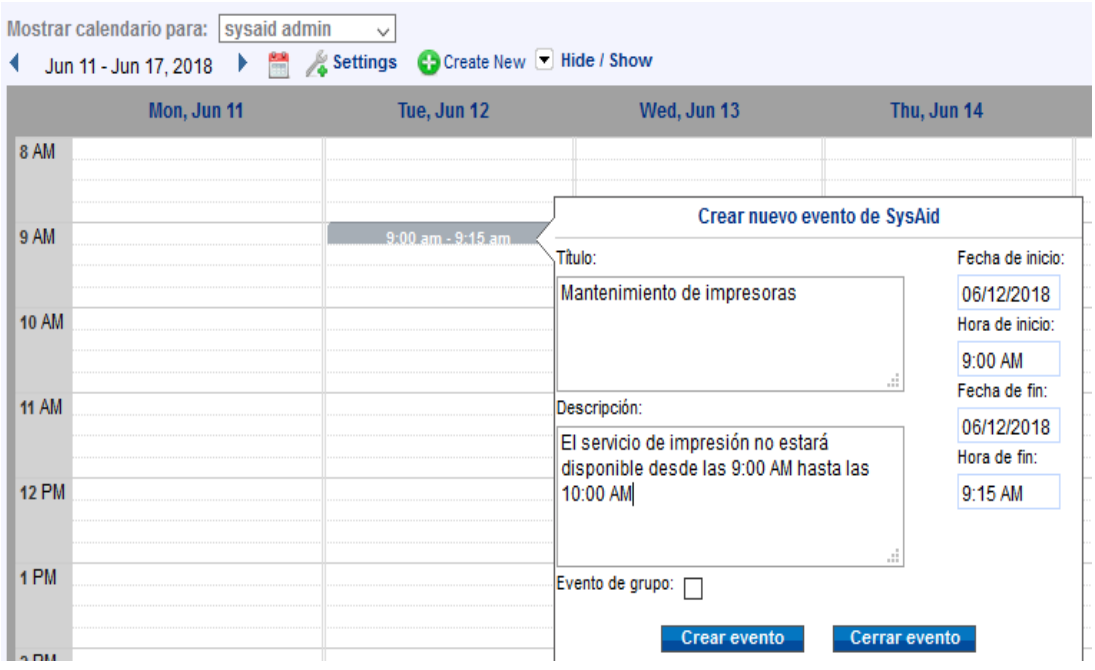


Figura 112. Creación de un evento.

5.1.10 Pruebas de funcionamiento de la base de datos del conocimiento.

En SysAid se configuró varias entradas a la KDB de acuerdo con varias categorías, con los pasos para solucionar incidentes, solicitudes, problemas entre otros.

Esto es un eje fundamental cuando se trabaja con mesas de ayuda debido a que optimiza los tiempo de resolución de solicitudes, incidentes y problemas, al tener información del paso a paso de como se resuelven, llegando a obtener tiempos de respuesta muchos más rapidos en la reolución de este tipo de casos que son comúmnes para una organización.

Por tal motivo es importante parametrizar y tener identificado los procesos específicos. En la Figura 113 se puede observar diversas entradas en la KDB de la empresa.

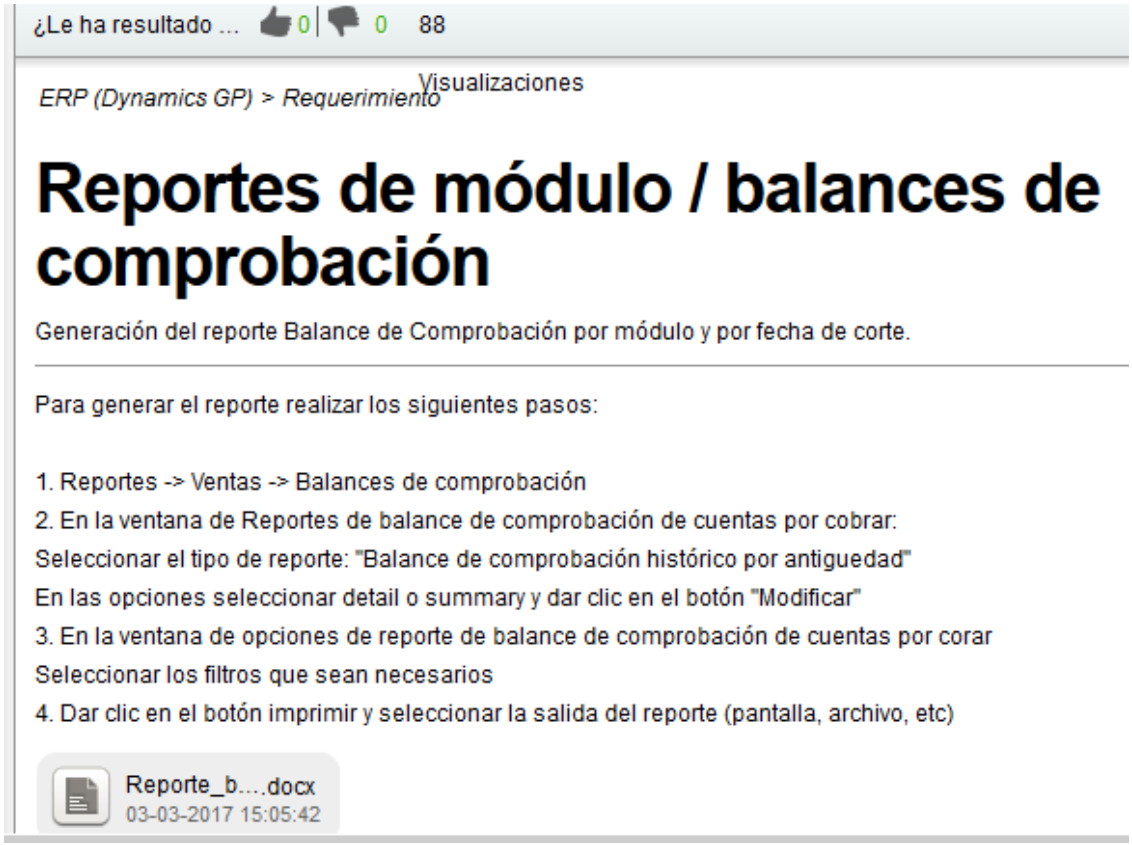


Figura 113. Entradas de la KDB.

5.2 Pruebas de funcionamiento de Sistema de Respaldos DRUVA PHOENIX.

Las pruebas de funcionamiento a realizarse en cuanto Phoenix son las siguientes:

- Prueba de funcionamiento del respaldo realizado del servidor HORUS.
- Pruebas de funcionamiento del respaldo realizado del servidor OSIRIS
- Pruebas de funcionamiento del sistema de reportes de Phoenix.

5.2.1 Prueba de funcionamiento del respaldo de información del servidor del aplicativo Microsoft Dynamics GP HORUS

En esta sección se realizará la prueba de funcionamiento del respaldo implementado al servidor HORUS, en la figura 114 a continuación se puede observar datos como:

- Tamaño de la fuente actual: 663.08 GB
- Tamaño de la fuente + cambios: 2.42 TB
- Número de instantáneas: 133
- Qué almacenamiento se está usando
- Nombre de la regla de contenido
- Nombre de la política de respaldos.
- Nombre del grupo administrativo.

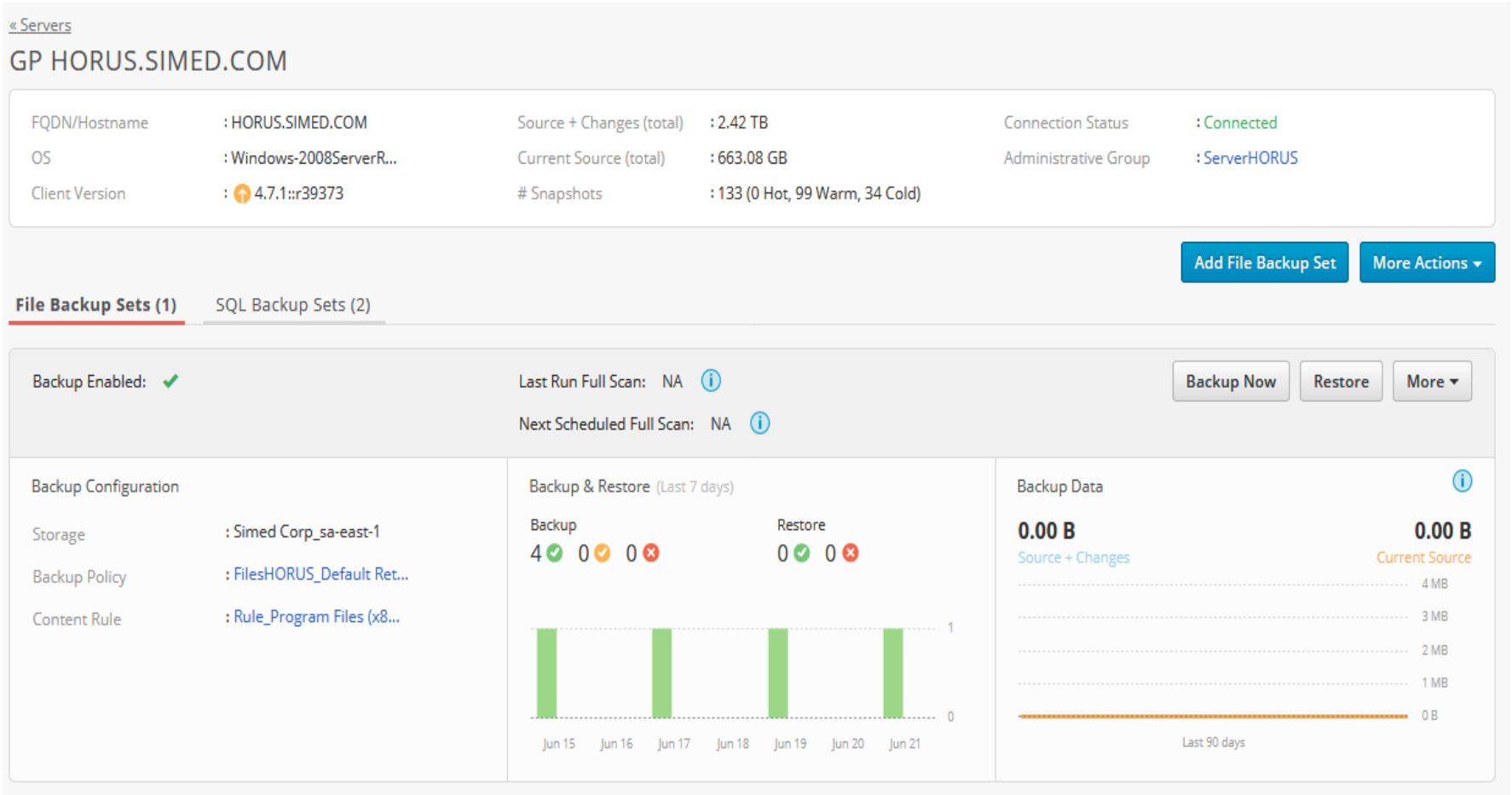


Figura 114. Pantalla de administración de los respaldos del servidor HORUS.

5.2.2 Prueba de funcionamiento de recuperación de los respaldos de información del servidor del aplicativo Microsoft Dynamics GP HORUS

A continuación se indica el proceso para restaurar la información de los respaldos del servidor HORUS, para lo cual en la ventana de administración del servidor se debe seleccionar Restaurar.

A continuación se seleciona el la fecha de la que se requiere el respaldo, se marca el directorio donde está la información y se da clic en restaurar.

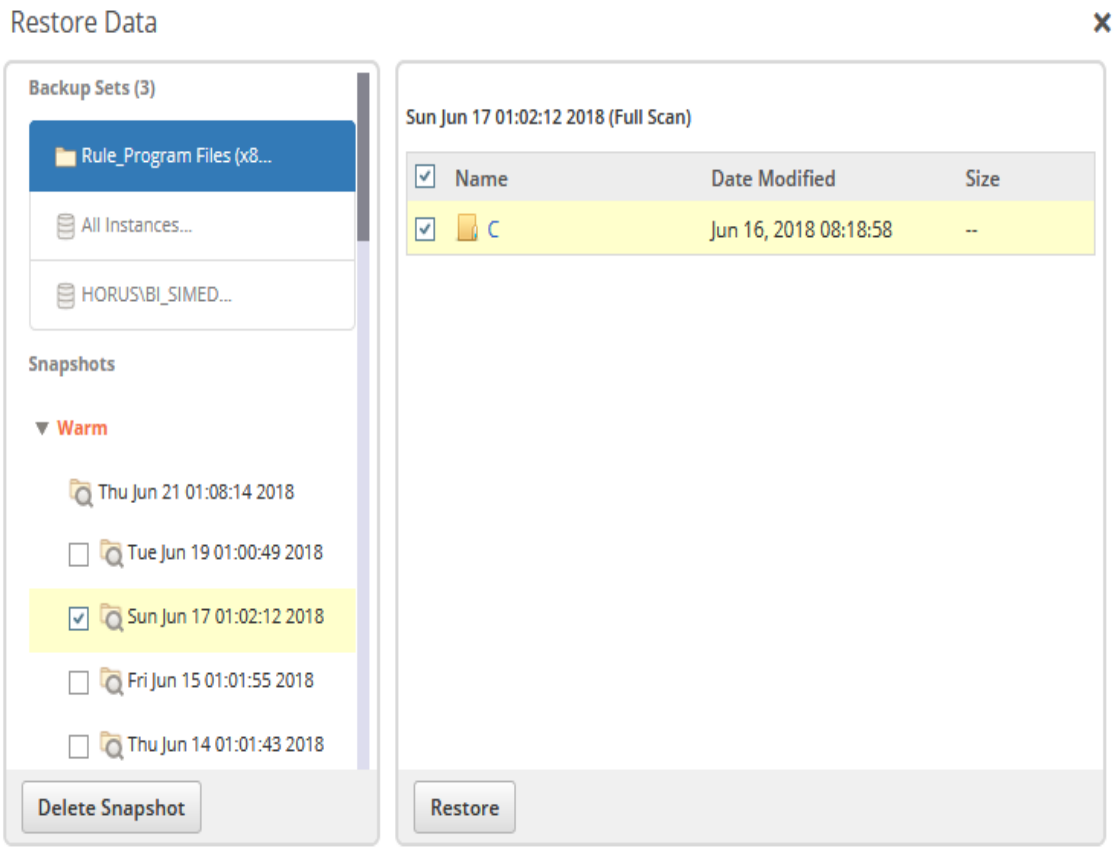


Figura 115. Selección de la fecha que se desea restaurar y la selección del fichero.

A continuación se selecniona donde se desea respaldar, esto puede ser en la misma ruta donde esta la información, una ruta diferente dentro del mismo servidor o en otro servidor diferente.

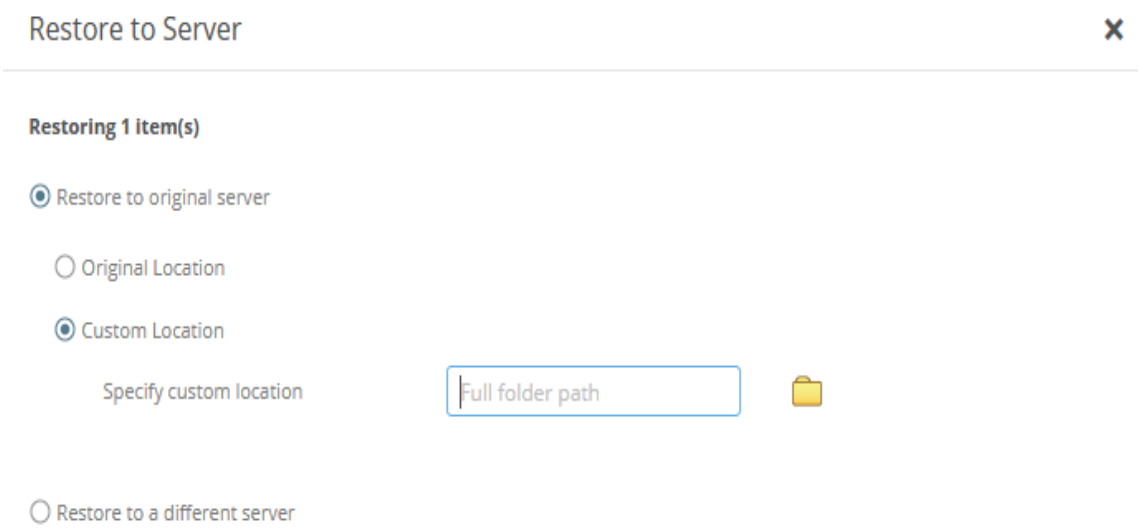


Figura 116. Selección de donde se va a guardar la restauración de datos.

Por último esta restauración se guardará en la ruta seleccionada y podrá ser usada para los fines necesarios. Como buena práctica se recomienda estar realizando pruebas a los respaldos obtenidos

5.2.3 Prueba de funcionamiento del respaldo de información del de bases de datos OSIRIS.

En esta sección se realizará la prueba de funcionamiento del respaldo implementado al servidor OSIRIS, en la figura 117 a continuación se puede observar datos como:

- Tamaño de la fuente actual: 165.13 GB
- Tamaño de la fuente + cambios: 1.15 TB
- Número de instantáneas: 143
- Qué almacenamiento se está usando
- Nombre de la regla de contenido

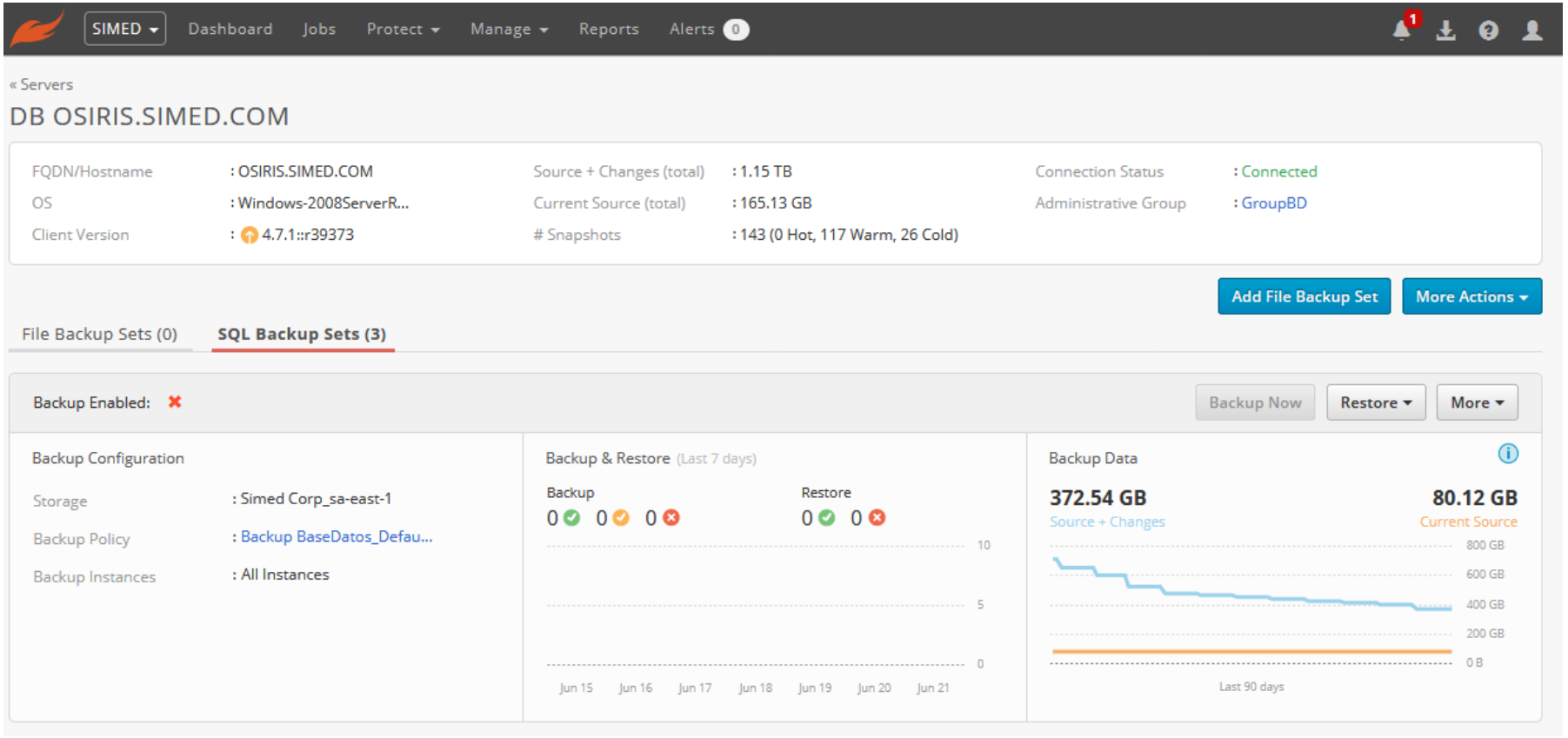


Figura 117. Pantalla de administración de los respaldos del servidor de bases de datos OSIRIS.

5.2.4 Prueba de funcionamiento de recuperación de los respaldos de información del servidor de bases de datos OSIRIS

Como se demostró en la restauración de los respaldos del servidor HORUS, para el servidor de bases de datos es similar a diferencia que en la pantalla de restauración de datos no se tiene para elegir un directorio a restaurar, sino que se elige una instancia de la base de datos.

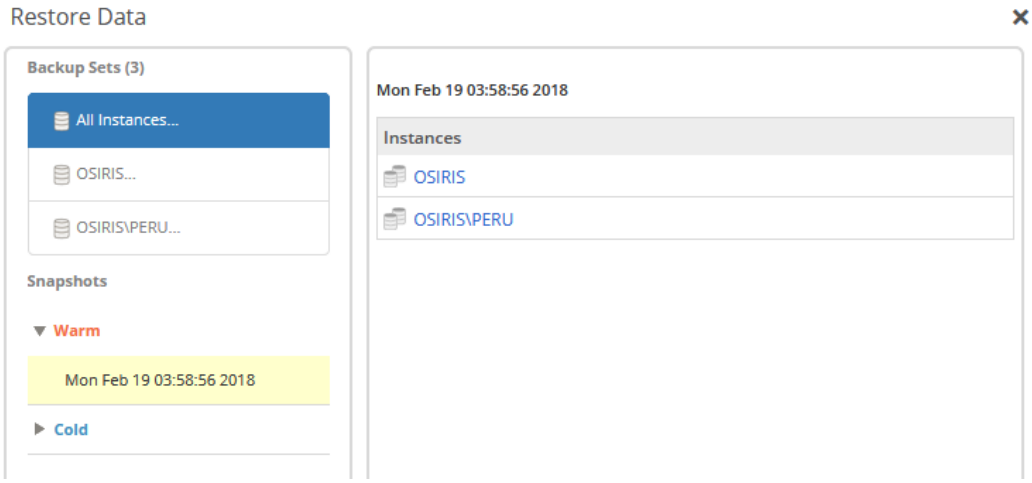


Figura 118. Selección de instancia a restaurar.

Al seleccionar la instancia se debe elegir qué base de datos se desea restaurar.

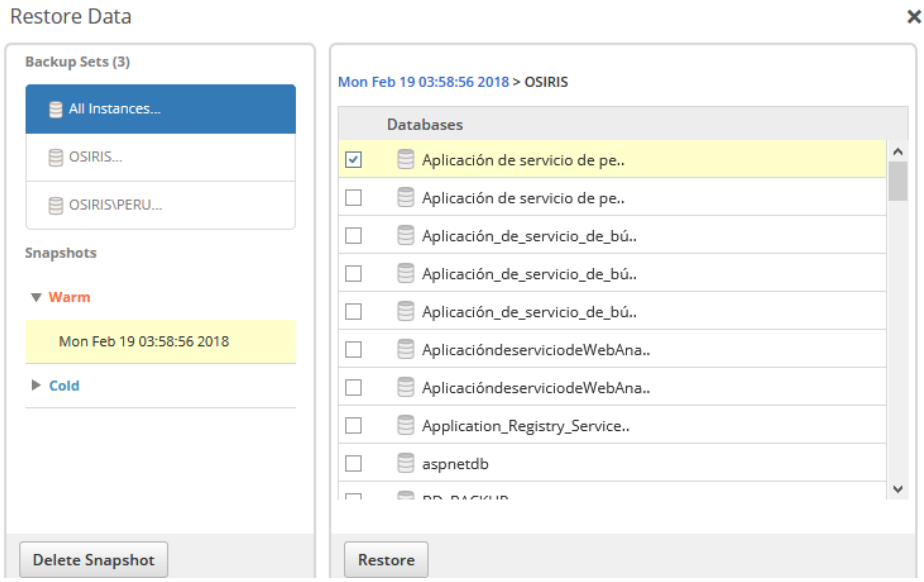


Figura 119. Selección de una base de datos determinada a restaurar.

5.2.5 Servidores instalados el agente de Phoenix para respaldar su información.

A continuación, en la figura 120 se observa todos los servidores montados para la obtención de sus respaldos:

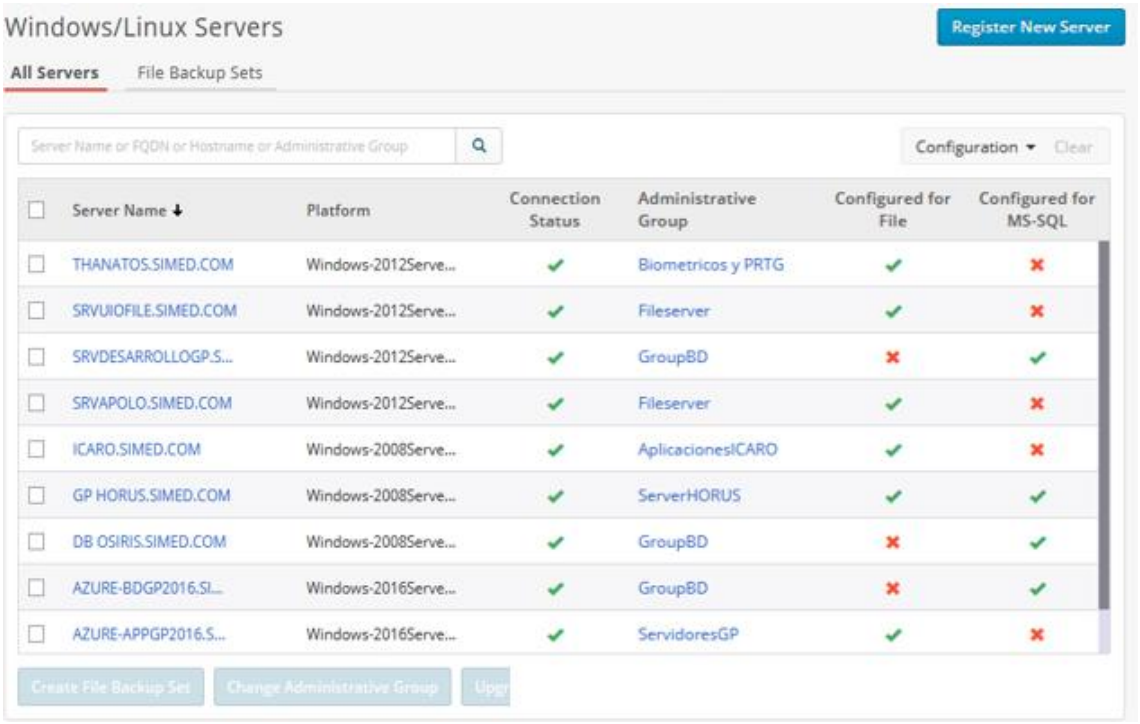


Figura 120. Servidores respaldados por Phoenix.

5.2.6 Prueba de funcionamiento de restauración de los respaldos de información de los usuarios.

En esta sección se realizará la prueba de funcionamiento del respaldo de información de los usuarios configurados con DRUVA InSync. El proceso para restaurar es muy parecido al de Phoenix por tratarse servicios de la misma empresa.

1. Ingresar al portal.
2. Dirigirse a la pestaña usuarios
3. Dar clic en el nombre del usuario del cual se desea obtener una restauración.

4. Seleccionar la versión de la fecha de respaldo que se desea restaurar.
5. Seleccionar que carpeta se desea restaurar.

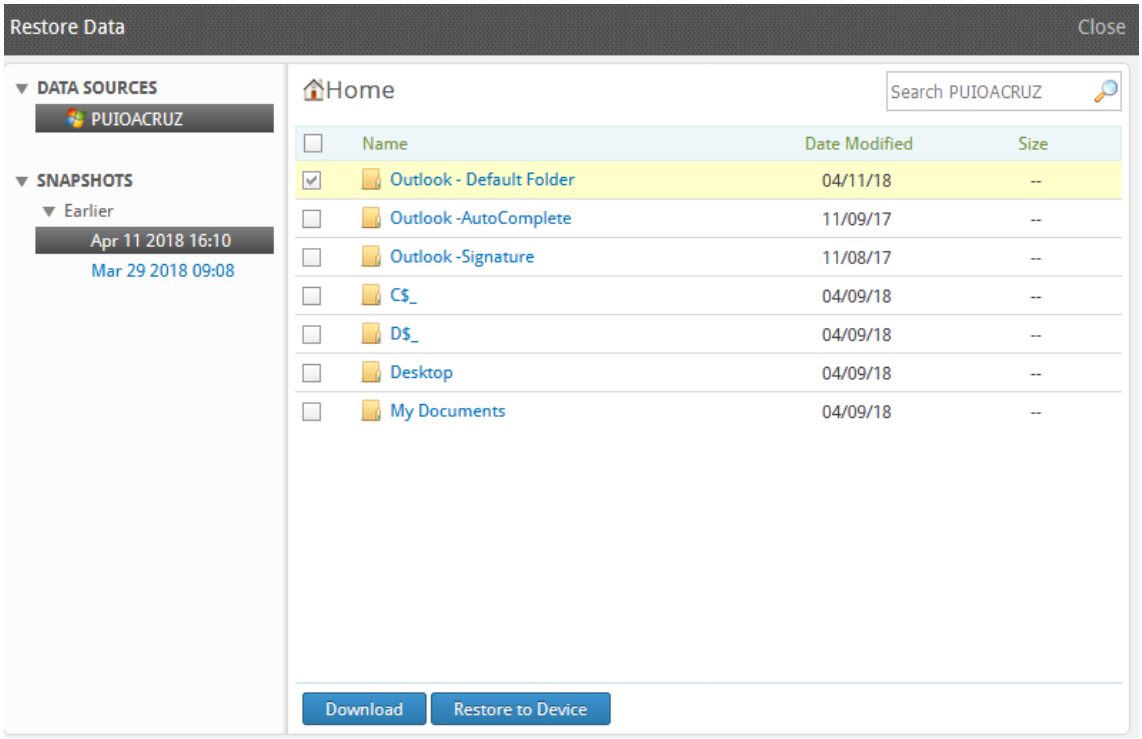


Figura 121. Selección de la versión de respaldo para un sumario mediante DRUVA InSync.

6. Finalmente se da clic en descargar.

6. Conclusiones y recomendaciones.

6.1 Conclusiones

La implementación de servicios como mesa de ayuda y sistemas de respaldos en cualquier organización permite garantizar la entrega de servicios de calidad a los clientes de la empresa generando un valor agregado a sus productos.

ITIL V3 fue fundamental para el desarrollo de la estructura, procesos y funciones de los servicios de TI que brindará la mesa de ayuda implementada, gracias a las buenas prácticas recomendadas por este marco de referencia que pueden ser adaptadas a la necesidad y los medios disponibles de cada organización.

Con la implementación de una mesa de ayuda basada en tecnología *cloud* en la empresa se generó un valor agregado en la entrega de servicios de TI, optimizó procesos y disminuyó tiempos de respuestas, ayudando en gran medida a dar un servicio de calidad a los usuarios internos de en la organización.

La definición de los servicios de TI que brindará la empresa fue un punto vital puesto que a partir de esto se pudo definir todas las demás configuraciones en cuanto a la fase de operación del servicio.

Para establecer los tiempos de respuesta con los que trabaja la mesa de ayuda implementada se tuvo en primera instancia definir cuáles son los impactos de los servicios de TI en reuniones con los responsables de cada área de la empresa con lo cual se consiguió definir correctos Acuerdos de Niveles de Servicio.

El uso de la funcionalidad de LDAP que proporciona SysAid fue de gran utilidad en la gestión de la mesa de ayuda puesto que facilitó la configuración de usuarios y contraseñas de ingreso a la herramienta al disponer de una misma base central de datos obtenida del directorio activo de la empresa.

Con el despliegue de la herramienta SysAid en las estaciones de trabajo de los colaboradores de la empresa mediante políticas de uso configuradas en el

directorio activo permitió una fácil instalación del agente en las máquinas de la red.

Con el uso del enrutamiento de los registros de servicios creados por los usuarios se optimizó el proceso de atención de los casos puesto que automatizó la asignación de estos hacia el técnico responsable.

Con la implementación de la integridad del calendario de SysAid con el calendario de Outlook se proporcionó una gestión de eventos más centralizada para la empresa y se consiguió un medio de comunicación con el usuario final de las acciones que se vayan a realizar en los servicios de TI que puedan llegar a parar su funcionamiento.

Haber realizado el modelo de respaldos siguiendo buenas prácticas recomendadas por marcos de referencia fue una fase vital previa a la implementación del sistema de respaldos, puesto que definió los parámetros a configurarse y los procesos a realizarse ante cualquier escenario donde existiera pérdida de la información.

Con la implementación del sistema de respaldos en la nube se garantizó la protección de la información en la empresa ante cualquier escenario donde pudiera existir pérdida de información a nivel local. Punto vital que considerar hoy en día donde la información es el activo más importante de las empresas.

La definición de los servidores críticos para la empresa y la información principal de cada uno de ellos fue de suma importancia, puesto que permitió definir cuanto espacio en la nube era necesario realmente.

Al usar políticas de respaldos en Phoenix permitió definir tipos de respaldos, frecuencias, duración entre otros parámetros que tuvieron que ser aplicados a ciertos tipos de respaldos.

6.2 Recomendaciones

Se recomienda que en los presupuestos anuales de las empresas sea un punto fundamental la inversión en tecnologías de información innovadoras que permitan el incremento de seguridad informática, productividad del personal de TI, entre otras que conjuntamente tienen como fin aportar al crecimiento de la organización.

Se recomienda capacitar al personal de TI de las empresas en el uso de marcos de referencia como lo son ITIL v3, COBIT, Normas ISO/IEC 20000, Normas ISO/IEC 17799, INEI que permitirán que cada colaborador este en la facultad de crear, implementar y hacer cumplir buenas prácticas para la entrega de servicios de TI.

Se recomienda no solo para el despliegue de la herramienta SysAid si no para el despliegue de cualquier otra herramienta de forma masiva en las estaciones de trabajo de los usuarios el empleo de políticas de uso que facilita esta labor en gran medida.

Se recomienda en función de las tareas que cumple cada miembro del personal de TI definir qué casos debería atender cada uno de acuerdo a sus conocimientos y habilidades, con lo cual se puede realizar una correcta configuración de los enrutamientos de los registros de servicios en la herramienta SysAid.

Se recomienda utilizar la configuración de métricas en SysAid para poder evaluar el desempeño en general de la mesa de ayuda y el desempeño individual de cada técnico.

Se recomienda realizar capacitaciones constantes a los usuarios sobre el uso de la herramienta, con el din de ir disminuyendo progresivamente el uso de correos y llamadas telefónicas para la creación de incidentes, solicitudes, problemas.

Se recomienda la configuración de grupos administrativos en Phoenix para disponer de una gestión más organizada de servidores clasificándolos de acuerdo con sus características y funciones que cumplen.

Se recomienda la configuración de notificación por correo electrónico de respaldos fallidos, con el fin de que el personal responsable este siempre en conocimiento del estado de los respaldos y pueda tomar medidas correctivas, además realizar pruebas constantes de recuperación de información tanto de los respaldos de DRUVA como de los respaldos de PHOENIX con el fin de evaluar la integridad de dichos datos.

Referencias.

Arqueros, M. (2013). El valor de los servicios. Recuperado el 10 de enero de 2018 de https://www.securityartwork.es/2013/03/26/el-valor-de-los-servicios/

Faquinones. (s.f.). Gestión de Niveles de Servicio. Recuperado el 12 de febrero de 2018 de http://faquinones.com/gestiondeserviciosit/itilv3/diseno_servicios_TI/gestion_nivel_servicio/introduccion_objetivos.php

Fellows, R. (2008). Copia de seguridad completa, incremental o diferencial: cómo elegir el tipo adecuado. Recuperado el 12 de febrero de 2018 de https://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado

Svempresas. (s.f.). Implementación de Sistema de Mesa de Ayuda y Administración de Tecnologías de Información (TI). Recuperado el 2 de junio de 2018 de http://svempresas.com/fiste/rokdownloads/Sistemas%20white%20Papers/PAPER_-_Cristina_Garcia_Uribe.pdf

Grupo Arión. (2017). Manejo de Tickets de Mesa de Ayuda por Web. Recuperado el 2 de junio de 2018 de https://www.grupoarion.com.mx/manejo-tickets-mesa-ayuda-web/

Guzmán, Á. (2012). ITIL v3 -Gestión de Servicios de TI . *ECORFAN Journal-Mexico.* *3*(7), 539-544 Recuperado de http://www.ecorfan.org/pdf/ECORFAN%20Journal-M%C3%A9xico%20V3%20N7_2.pdf

Helppeople cloud. (s.f.). Recuperado el 10 de enero de 2018 de https://helppeoplecloud.com/web/itil-v3-operacion-del-servicio/

Infopersonal. (2014). ¿Para qué sirve el help desk? Recuperado de http://infopersonaldecure.blogspot.com/2014/11/hel-desk.html

IT Governance Institute. (2007). COBIT 4.1. Recuperado el 25 de febrero de 2018 de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf

Kyocera. (2017). ¿Es la copia incremental la mejor opción para backup en la nube?. Recuperado el 25 de febrero de 2018 de https://smarterworkspaces.kyocera.es/blog/la-copia-incremental-la-mejor-opcion-backup-la-nube/

López, L. (2016). ServiceNow Express bajo estándar ITIL llegó para facilitarte la vida. Recuperado el 2 de junio de 2018 de http://www.gb-advisors.com/es/news-es/servicenow-express-estandar-itil/

Microsoft Azure. (s.f.). ¿Qué es la nube pública, privada e híbrida? Recuperado el 12 de febrero de 2018 de https://azure.microsoft.com/es-es/overview/what-are-private-public-hybrid-clouds/

Microsoft Azure. (s.f.). ¿What is cloud computing? Recuperado el 17 de julio de 2018 de https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

Office of Government Commerce. (2007). *ITIL v3 Service Operation.* Recuperado el 20 de febrero de 2018 de http://itiq.co.bw/wp-content/themes/IT-IQ/pdf/ITIL%20v3%20Service%20Operation.pdf

Oliveros, F. (2007). *Los mejores métodos resguardar tus datos más importantes*. Recuperado el 20 de febrero de e https://luisgyg.com/metodos-para-respaldo-de-informacion/

Programa Del Máster Dirección de Proyectos. (2017). Módulo 3. Diseño del Servicio. Recuperado el 12 de febrero de 2018 de http://www.uv-mdap.com/programa-desarrollado/bloque-vi-itil-v3/diseno-del-servicio-itil/

Raphael, C. (2011). Herramientas empresariales. Recuperado el 18 de febrero de http://herramientasempresariales.com.mx/2011/10/mesa-de-ayuda-%C2%BFque-es/

Rondanelli, O. (2013). Procesos ITIL® 2011. Recuperado de https://www.slideshare.net/acroar/procesos-itil-2011orlandorondanelli

Tecnofor. (2010). Ciclo de Vida de los Servicios. Recuperada de https://es.slideshare.net/tecnofor/ciclo-de-vida-de-los-servicios.