Implementación de un conjunto de servicios tecnológicos para favorecer el acceso, compartición y disponibilidad de la información en el fondo rotatorio municipal de valorización de Sincelejo

Armando Luis Pérez Covo
Víctor Andrés Román Garrido

Corporación Universitaria del Caribe – CECAR
Facultad de Ciencias Básicas, Ingenierías y Arquitectura
Programa de Ingeniería de Sistemas
Sincelejo, Sucre
2019

Implementación de un conjunto de servicios tecnológicos para favorecer el acceso, compartición y disponibilidad de la información en el fondo rotatorio municipal de valorización de Sincelejo

Armando Luis Pérez Covo
Víctor Andrés Roman Garrido

Trabajo de grado desarrollo tecnológico presentado como requisito para optar al título de Ingeniero de Sistemas

Director
Ing. Amaury Rodríguez Oviedo
Especialista en Tecnologías de la información

Corporación Universitaria del Caribe – CECAR
Facultad de Ciencias Básicas, Ingenierías y Arquitectura
Programa de Ingeniería de Sistemas
Sincelejo, Sucre
2019

Nota de Aceptación

4,95

Director

Evaluador 1

Evaluador 2

Sincelejo, Sucre, 26 de julio de 2019

Dedicatoria

Este trabajo de grado es dedicado a mis padres y hermanos, quienes han sido de gran apoyo en todo momento, también quiero agradecer a mi tutor de proyecto, que con su gran ayuda y esfuerzo se pudo lograr con éxito la culminación de este proyecto.

Armando Luis Pérez Covo

Dedicatoria

Dedico este trabajo de grado a mi madre, quien con su constancia y apoyo incondicional me motivó a dar lo mejor de mí y a no desfallecer a lo largo de estos años de formación que hoy culminan con este producto, a la memoria de mi padre, que, aunque no está con nosotros, me enseñó que a pesar de las dificultades que se nos puedan presentar en la vida, los sueños se alcanzan con disciplina y esfuerzo y a todos los que creen en mí y que me han aportado conocimientos valiosos a nivel personal y profesional.

Víctor Andrés Román Garrido

Agradecimientos

Luego de este gran logro nos gustaría expresar un agradecimiento especial a nuestro asesor de práctica y tesis Amaury Rodríguez, quien fué un apoyo fundamental durante el desarrollo de este proceso donde siempre se mostró interesado y dispuesto a orientarnos, aclararnos y corregirnos las veces que lo necesitamos, a el ingeniero Bladimir Manjarres, jefe de sistemas del Fondo rotatorio Municipal de Valorización de Sincelejo por recibirnos con gran acogida en la entidad y por su disposición para gestionar internamente lo referente a la implementación del proyecto y a nuestros evaluadores e ingenieros Jhon Méndez y Javier Padilla, quienes también se interesaron para que este proyecto se aprobara y se ejecutara con satisfacción , gracias a estos profesionales excepcionales, a la vida y a los amigos que con sus conocimientos nutrieron los nuestros y fortalecieron este trabajo.

Tabla de contenido

Lista de tablas

Lista de figuras

Resumen

El Fondo Rotatorio Municipal de Valorización de Sincelejo (FOMVAS) es un establecimiento público del municipio de Sincelejo, que tiene como misión “servir a la comunidad como instrumento de financiación, mediante el sistema de valorización, para la realización de proyectos de interés público". De acuerdo con el Plan Estratégico de Tecnológicas de la Información (PETI) 2018, presenta los siguientes problemas: Inadecuado control de acceso a los equipos de cómputo, a la red LAN, a la gestión de activos de tecnologías de información, al acceso remoto a los sistemas de información, a la gestión del acceso y uso del servicio de internet, así como a la gestión de la información de la entidad. Este proyecto tiene como objetivo la implementación de un conjunto de servicios tecnológicos para favorecer el acceso, compartición y disponibilidad de la información en el fondo rotatorio municipal de valorización de Sincelejo, a través de las siguientes fases: Selección de herramientas, Diseño e Implementación de servicios y la fase de capacitación de usuarios, que permitieron la implementación de los servicios de autenticación de usuario centralizada, gestión de inventario tecnológico, alojamiento centralizado de archivos digitales, de acceso remoto a través de servicios de red privada virtual, de asignación dinámica de direcciones IP, de filtrado de puertos de entrada y salida de la red corporativa, de gestión de la calidad del servicio de internet y de gestión del uso del servicio de internet compartido. Dichos servicios permitieron aumentar las condiciones de seguridad de la información, en términos de la confidencialidad y disponibilidad de la información de la entidad.

Palabras clave: Tecnologías de la Información (TI), Servicios tecnológicos, Software Libre.

Abstract

El Fondo Rotatorio Municipal de Valorización de Sincelejo (FOMVAS) is a public establishment in the municipality of Sincelejo, whose mission is "to serve the community as a financing instrument, through the valuation system, for the realization of projects of public interest". According to the Strategic Information Technology Plan (PETI) 2018, it presents the following problems: Inadequate control of access to computer equipment, to the LAN network, to the management of information technology assets, to remote access to information systems, to the management of access and use of the internet service, as well as the management of information of the entity.This project has the objective of implementing a set of technological services to favor access, sharing and availability of information in the municipal rotating fund of Valorization of Sincelejo, through the following phases: Selection of tools, Design and Implementation of services and a user training phase, which allowed the implementation of centralized user authentication services, technological inventory management, centralized hosting of digital files, remote access through virtual private network services, dynamic assignment of IP addresses, filtering ports of entry and exit of the corporate network, management of the quality of the internet service and management of the use of shared internet service. These services allowed to increase the security conditions of the information, in terms of the confidentiality and availability of the information of the entity.

Keywords: Information Technologies (IT), Technological Services, Open Source.

Capítulo 1

Introducción

El Fondo Rotatorio Municipal de Valorización de Sincelejo (FOMVAS) es un establecimiento público del municipio de Sincelejo, que tiene como misión "servir a la comunidad como instrumento de financiación, mediante el sistema de valorización, para la realización de proyectos de interés público, ejecutando obras civiles, de electrificación, saneamiento básico, recreación y cultura, etc., generando desarrollo en el municipio de Sincelejo" y se proyecta como una

> Entidad pública con un fortalecimiento institucional que se caracterice por su gestión en el desarrollo de actividad de obras de interés público dando respuesta a los retos que demanda el desarrollo del municipio de Sincelejo logrando la autosuficiencia en todos los esfuerzos de los diferentes grupos de interés que propicien grandes beneficios a la comunidad. (FOMVAS, s.f.).

El Fondo Rotatorio Municipal de Valorización de Sincelejo cuenta con una estructura organizacional apoyada en 3 niveles los cuales son: gestión directiva, gestión de operación misional y gestión de operación de soporte, que se apoyan en una infraestructura tecnológica (equipos de cómputo, red LAN, Acceso a Internet, entre otros) que permiten el acceso a los empleados a los diferentes recursos informáticos, sistemas de información (Tal como el Sistema de Información para la gestión de los procesos de nómina, presupuesto, contabilidad y tesorería) y servicios que ofrece el ente.

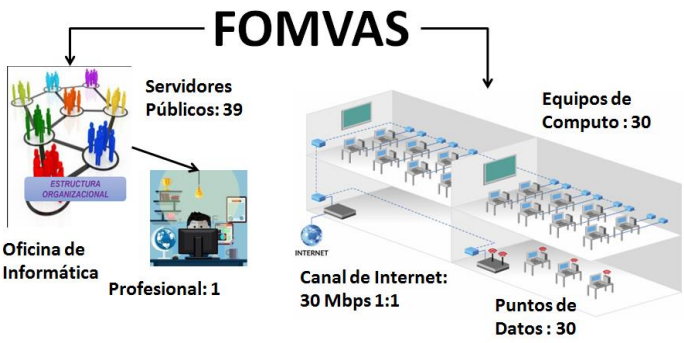

Figura 1. Estructura de red

Fuente: Elaboración propia.

De acuerdo con el análisis realizado por la entidad y divulgado en su Plan Estratégico de Tecnologías de Información para la vigencia 2018, el FOMVAS presenta los siguientes problemas a nivel de su infraestructura tecnológica y de servicios: Inadecuado control de acceso a los equipos de cómputo, a la red LAN, a la gestión de activos de tecnologías de información, al acceso remoto a los sistemas de información de la entidad, a la gestión del acceso y uso del servicio de internet, así como a la gestión de la información de la entidad. En relación al control de acceso a los equipos de cómputos, se ha determinado que existe un deficiente control del acceso a sus equipos de cómputos, por parte de los empleados que laboran en FOMVAS, manifestando que uno de los riesgos a los que se encuentra expuesta, es el acceso indebido a la información sensible de la entidad, siendo esta una preocupación permanente de los servidores públicos que laboran en la organización. Así mismo, en cuanto al control de acceso a la red LAN interna, el plan estratégico de las tecnologías de la información PETI de la entidad, menciona la inexistencia de controles de acceso y monitoreo del uso de la red interna, manifestando que no cuentan con herramientas que faciliten la separación de los servicios de red y la protección del acceso a los recursos compartidos a través de la misma.

Se menciona también la Inadecuada gestión de los activos de tecnologías de la información, que, aunque se lleva un control manual de las cantidades de activos de información que poseen en la entidad, no se lleva un registro que permita contar con la información detallada

de los activos y su ubicación al interior de la entidad, que favorezca los procesos de seguimiento permanente a los mismos. También se resalta, la dificultad para acceder a los sistemas de información desde una red externa, manifestando afectaciones a la disponibilidad de la información a los servidores públicos de la división técnica, ya que los sistemas de información que actualmente soportan los procesos de nómina, presupuesto, tesorería, contabilidad y de valorización solo pueden ser accesibles desde los usuarios conectados a la red LAN de la entidad, impidiéndoles cuando se encuentran en visitas de asistencia técnica fuera de la entidad el acceso a la consulta de dicha información en tiempo real.

De otro lado, Inadecuada gestión del ancho de banda del servicio de acceso a internet, afecta la implementación de procedimiento que permitan garantizar un control y una calidad de servicio en el acceso a Internet ofrecido a los servidores públicos desde la entidad, ocasionado por cualquier uso inadecuado del servicio por parte de los funcionarios. Incluso, la inadecuada gestión de la información utilizada por los servidores públicos se almacena en los diferentes activos de tecnología de la información, pero la misma, no se consolida, tampoco se comparte de manera que se pueda controlar el acceso a dichos recursos.

Estas problemáticas que afectan la prestación de servicios de la entidad, según el plan estratégico de tecnologías de información están relacionadas con la falta de implementación de herramientas que propendan por la aplicación de las políticas de seguridad de la información identificadas, así como la insuficiencia en la asignación de recursos humanos y financieros para el cumplimiento de los procesos informáticos.

Uno de los pilares fundamentales de las organizaciones con respecto a la información, es que haya una buena seguridad de esta, conllevando a respaldar la información de cualquier tipo de fallas e incidentes o incluso evitar algún tipo de extracción de la información por parte de intrusos que intenten vulnerar la seguridad. La ISO/IEC 27001 es un estándar de la seguridad de la información, que además de especificar los requisitos y etapas de un correcto sistema de gestión de la seguridad de la información, se refiere a la confidencialidad, integridad y

disponibilidad de la información, reconociendo estos conceptos como lo primordial dentro del SGSI. Un detalle a destacar del estándar, es que la información que mencionan no es únicamente la que se encuentra en medios informáticos, es decir puede estar en cualquier formato bien sea, digital, en papeles, etc. (Advisera, s.f.)

La disponibilidad desde una perspectiva de acceso, busca que la información sea accesible de forma eficaz y en el tiempo que se requiera por los usuarios, la integridad por su parte controla que la información no sea alterada por accidente o manipulada por personas con fines malintencionados y por otro lado la confidencialidad tiene como objetivo primordial permitir el acceso a la información únicamente a los usuarios que tengan autorización de acceso, de esta manera salvaguardando la información sensible de terceros (PMG, 2018).

Sin embargo, como el recurso económico es un factor fundamental a la hora de adoptar tecnologías en las organizaciones, se hace necesario resaltar las bondades del software libre; y de otro lado, el esfuerzo ingente de muchas empresas, por la comercialización de hardware con mejores prestaciones técnicas a un menor costo, que es entre otras cosas, computadoras con características de procesamiento, y almacenamiento no tan potentes, pero que a su vez pueden suplir gradualmente las necesidades de las organizaciones en cuanto a servicios tecnológicos.

Las entidades públicas deben diagnosticar con precisión las herramientas de Tecnologías de la información y comunicación, que se vayan a adquirir, debido que se obtienen con dinero público, lo que implica que todas esas inversiones deben ser estudiadas a la luz de los principios de la administración pública colombiana. Por otra parte, el software libre, ofrece un conjunto de herramientas y recursos que permiten dar solución a distintos problemas que se esté presentando en dicho sector, que en algunos casos “al no tener costes de licencia y al tener el código fuente abierto, permite reducir los costes de implantación en la Administración ya que cualquier desarrollador de software puede ponerlo en funcionamiento y adaptarlo a sus necesidades particulares.” (García, 2013).

No obstante, uno de los motivos por los cuales la administración pública se ve impulsada a tener en cuenta el software libre, es por la posible disminución de los costos en cuanto a los modelos de licenciamiento ofertados generalmente, en la mayoría de los casos, de distribución y de uso libre, aunque puedan sin embargo, tener gastos asociados, directos o indirectos como por ejemplo, suscripciones de servicios y acuerdos de licencia, actualizaciones y ampliaciones requeridas, soporte técnico, tarifas de capacitación y mantenimiento (Bouras et al, 2014).

Según lo dispuesto en el Plan Estratégico de Tecnologías de Información del FOMVAS, la no atención de dichas problemáticas puede traer como consecuencia perdida de la información o modificación no autorizada de la misma, retrasos en los procesos, pérdida de la credibilidad o imagen institucional, demandas judiciales, entre otras afectaciones a la prestación del servicio encomendado a dicha entidad.

De otro lado, según el Ministerio de Tecnologías de la Información y Comunicaciones, IT4+ es un modelo integral de gestión estratégica con tecnología cuya base fundamental es la alineación entre la gestión de tecnología y la estrategia sectorial o institucional. El modelo facilita el desarrollo de una gestión de Tecnologías de Información que genera valor estratégico para el sector, la entidad, sus clientes de información y usuarios. El modelo está conformado por los siguientes componentes: Estrategia de TI, Gobierno de TI, Gestión de Información, Gestión de Sistemas de Información, Gestión de Servicios Tecnológicos y Apropiación y uso.

IT4+ está alineado con las estrategias empresariales y organizacionales que son tendencia en los diferentes sectores productivos y de servicios que permiten desarrollar una gestión de tecnologías de información que genere valor estratégico para las organizaciones y sus clientes. IT4+ contribuye al mejoramiento de la gestión empresarial porque facilita la administración, el control de los recursos y brinda información oportuna y objetiva para la toma de decisiones en todos los niveles de las organizaciones, sean entidades públicas o privadas.

La gestión de servicios tecnológicos en IT4+ hace referencia al servicio de adquisición, administración y operación de la infraestructura tecnológica al servicio de la organización, la alta disponibilidad para garantizar una operación continua y los servicios de soporte técnico a los usuarios. La importancia de la gestión de servicios tecnológicos se deriva de las necesidades de mantener en operación los sistemas de información de la organización, garantizar el acceso a los servicios, por parte de los usuarios internos y externos; así como la atención y el soporte a los mismos, en relación con las necesidades de infraestructura tecnológica y el cumplimiento de acuerdos de nivel de servicio definidos a nivel organizacional.

Con base a los problemas antes mencionados, el FOMVAS ha adoptado el marco de trabajo IT4+, tal como se precisa en el plan estratégico de Tecnologías de Información publicado en su sitio web, a partir del cual pretenden a través de una serie de planes, diseñar e implementar soluciones acordes a las problemáticas presentadas. Las soluciones están asociadas a la implementación de servicios tecnológicos que aporten a mitigar los riesgos asociados a las problemáticas identificadas.

Este proyecto tiene como objetivo la implementación de un conjunto de servicios tecnológicos para favorecer el acceso, compartición y disponibilidad de la información en el fondo rotatorio municipal de valorización de Sincelejo, a través de unas fases orientadas a satisfacer las necesidades priorizadas por la oficina de servicios informáticos de la entidad, consideradas como relevantes en el contexto organizacional del FOMVAS, organizadas en servicios de la siguiente manera: El servicio de autenticación de usuario centralizada, gestión de inventario tecnológico, alojamiento centralizado de archivos digitales, de acceso remoto a través de servicios de red privada virtual, de asignación dinámica de direcciones IP, de filtrado de puertos de entrada y salida de la red corporativa, de gestión de la calidad del servicio de internet y de gestión del uso del servicio de internet compartido.

Capítulo 2

Diseño Técnico y Metodológico

Para dar solución a las necesidades presentadas por el FOMVAS, se establecen dos aspectos esenciales que orientan la implementación del proyecto: En primer lugar, La concertación conceptual de los servicios requeridos por la entidad y finalmente, la definición de una metodología coherente que aporte al contexto en el que se presenta el problema y las posibles soluciones.

En relación con la concertación conceptual, hace referencia a la comprensión de la necesidad desde la perspectiva de la entidad y en atención a la delimitación del alcance de cada uno de los servicios requeridos por la entidad. En atención a lo anterior, se presentan un marco conceptual que sirvió como referente para establecer los requerimientos de la entidad y en particular los alcances que debería aportar cada servicio definido.

En atención al Servicio de autenticación de usuarios centralizada, es importante en primera instancia precisar que según la International Business Machines (IBM)

> La identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema" y que "La autenticación es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser. (IBM, s.f.).

En atención a lo anterior, al hace referencia a este servicio, se adopta como un método de autenticación, en el cual los usuarios de la infraestructura tecnológica tienen que identificarse y autenticarse con unas credenciales válidas para acceder a aplicaciones, servicios de red etc. La identificación y autenticación son verificadas a través de un servidor que se apoya en un protocolo especificado; tal como, el protocolo ligero de acceso a directorios (LDAP) (IPCop, s.f.).

Según Pino (2013), el Servicio de gestión de inventario tecnológico, es un método utilizado para recolectar información cuantitativa y cualitativa de los activos tecnológicos disponibles en una organización, ayudándoles de esta manera en la planificación e identificación de necesidades tecnológicas a corto plazo. Así mismo, el servicio de alojamiento de archivos digitales centralizados, hace alusión a "servicio de alojamiento de Internet diseñado exclusivamente para alojar archivos de usuario", donde dichos archivos se pueden compartir con los usuarios que se deseen y pueden ser imágenes, videos, textos, etc. (Techopedia, s.f.).

El Servicio de filtrado de contenido web, hace alusión a una herramienta "software diseñado para restringir los sitios web que puede visitar un usuario" (Kaspersky, s.f.). según Oscar Ardila (2015), el servicio de VPN (Virtual Private Network), que traduce al español "Red Privada Virtual", provee una red privada que se extiende a través de internet, concediendo que las máquinas conectadas puedan enviar y recibir datos de forma segura como si estuvieran conectados a una red local.

Según el instituto Puig castellar, el servicio de DHCP "Dynamic Host Configuration Protocol" estático, permite "especificar parámetros de red de manera automática de los equipos que lo solicitan dicho servicio, normalmente cuando se conecta a la red, lo que permite facilitar la configuración de red de los ordenadores*".* Así mismo, Según Tecnopedia el servicio QoS o de (Calidad de servicio), se refiere a la "capacidad de una red para lograr el máximo ancho de banda y tratar otros elementos de rendimiento de la red como la latencia, la tasa de error y el tiempo de actividad. La calidad del servicio también implica controlar y administrar los recursos de la red al establecer prioridades para tipos específicos de datos (video, audio, archivos) en la red."

Según CISCO, el servicio de Firewall, hace referencia a "un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad*".* La definición conceptual de este conjunto de servicios, fue concertada con la oficina de Informática de la entidad, estableciendo también el alcance de los servicios y unos criterios de flexibilidad en atención a la implementación de los mismos.

Tabla 1

Concertación de servicios maquina 1

CONCERTACIÓN DE SERVICIOS, ALCANCES Y CRITERIOS DE FLEXIBILIDAD		
SERVICIO	**ALCANCE**	**FLEXIBILIDAD**
Servicio de autenticación de usuarios centralizada	Facilitar la autenticación de todos los usuarios que laboran en el FOMVAS a los equipos de computo	Deseable que se puedan aplicar políticas de grupos de usuarios y restricciones en el acceso a los equipos sujetas al tiempo.
Servicio de gestión de inventario tecnológico	Facilitar la gestión de un inventario de los equipos de cómputo de la entidad.	Deseable que además de los equipos de cómputo, se puedan agregar al inventario otros activos de tecnología.
Servicio de alojamiento de archivos digitales centralizados	Facilitar que se puedan almacenar y compartir archivos de uso laboral de acuerdo con privilegios de usuarios específicos.	Deseable que se pueda sincronizar el almacenamiento con una ubicación privada en la nube a manera de copia de seguridad de los datos.

Fuente: Elaboración propia.

Tabla 2

Concertación de servicios maquina 2

CONCERTACIÓN DE SERVICIOS, ALCANCES Y CRITERIOS DE FLEXIBILIDAD		
SERVICIO	**ALCANCE**	**FLEXIBILIDAD**
El Servicio de filtrado de contenido web	Facilitar que se pueda controlar el uso del Internet, en cuanto a políticas de uso institucional.	Deseable que se puedan aplicar políticas de restricciones por grupos de usuarios.
El servicio de VPN	Facilitar que se pueda acceder de manera remota a recursos de la entidad, por necesidad laboral.	Deseable que se puedan otorgar esos privilegios de acceso remoto a usuarios específicos y que se pueda hacer seguimiento a sus accesos.
El servicio de DHCP	Facilitar que los equipos de cómputo de la entidad puedan obtener una dirección IP válida para conectarse a la red LAN y usar los servicios de Internet.	Deseable que se restringa el acceso a la Red LAN a cualquier equipo que no pertenezca a la entidad y que el mismo pueda acceder a recursos definidos por la política de seguridad

		institucional.
El servicio QoS	Facilitar que el uso de los recursos de red y de acceso a Internet se pueda utilizar de acuerdo con unas políticas de prioridad de acceso por usuarios.	Deseable que se pueda priorizar el acceso a los recursos además por aplicaciones, por tiempos de uso y por concurrencia en el acceso a los servicios.
El servicio Firewall	Facilitar la gestión de reglas de control de comunicaciones a través de la red.	Deseable simplicidad a la hora de crear reglas sobre protocolos y puertos.

Fuente: Elaboración propia.

Como parte de la concertación de los servicios con la entidad, también fue necesario determinar las capacidades que podría aportar la entidad a la implementación del proyecto, en términos de recursos, a través de la cual se evaluaron los siguientes aspectos:

Tabla 3

Evaluación de recursos

ASPECTO A EVALUAR	VENTAJAS	DESVENTAJAS
Recursos Humanos	✓ Disposición del talento humano de la oficina de informática de la entidad.	✓ Limitación en personal con conocimientos técnicos, tecnológicos o profesionales que puedan aportar a la implementación.
Recursos Tecnológicos	✓ Proyecto de implementación del Cableado Estructurado de la Entidad. ✓ Estaciones de Trabajo de los usuarios en buen estado	✓ Los sistemas operativos instalados en los diferentes equipos obedecen a versiones diferentes. ✓ No cuentan con equipos Servidores para la implementación de los servicios.
Recurso Financiero	✓ Existe un recurso para invertir en partes de equipos que puedan mejorar la infraestructura tecnológica.	✓ El rubro presupuestal para inversión en tecnología es limitado.

Fuente: Elaboración propia.

Para desarrollar el proyecto se diseñó la siguiente propuesta metodológica: Se definen cuatro fases de operación: La fase de selección de herramientas tecnológicas, la fase de diseño de servicios tecnológicos, la fase de implementación de los servicios tecnológicos y la fase de capacitación de usuarios. Es importante precisar que el orden de las fases mencionadas no implica que el inicio de una esté sujeto a la finalización de la otra, sino más bien que se traslapan en su ejecución de acuerdo con la coherencia del servicio abordado.

La fase de selección de herramientas tecnológicas tiene como propósito alinear las necesidades de la entidad, a partir de las problemáticas identificadas y los servicios tecnológicos que aportan a la solución de las mismas, así como, a la selección de las herramientas tecnológicas que facilitarían la implementación de los servicios y la evaluación de las mismas, en atención a las capacidades de la entidad en términos de recursos (Humanos, técnicos, tecnológicos, físicos y financieros). Esta fase permitirá determinar las herramientas que se implementarán y como aportan a la prestación de los servicios requeridos por la entidad.

La fase de diseño de servicios tecnológicos tiene como propósito la planificación del proceso de implementación de las herramientas tecnológicas identificadas, así como las necesidades de hardware, software, los requisitos de instalación y configuración, y los datos a recolectar para la implementación de cada uno de los servicios. Esta fase permitirá determinar las necesidades de hardware, software y recurso humano requerido para su implementación de conformidad con las capacidades institucionales, así como la priorización en la implementación de los servicios requeridos por la entidad.

La fase de implementación de los servicios tecnológicos tiene como propósito garantizar los procesos de adquisición, instalación, configuración, alistamiento, transición, prueba y producción de los servicios diseñados para la entidad. Las actividades de instalación, configuración y alistamiento se desarrollaron en ambientes simulados a través de máquinas virtuales y a través de equipos tecnológicos de pruebas, de tal manera que aportará al maduramiento de la solución y al monitoreo en la implementación en producción de dichos servicios. Las actividades de transición inician con la implementación gradual de los servicios y

la ejecución permanente de actividades de prueba que facilitarán determinar la estabilidad de los servicios implementados.

La fase de capacitación a los usuarios se desarrolla de manera paralela a la fase de implementación y tiene como actores principales a dos clases de usuarios en la entidad: Los usuarios administradores de los servicios y los usuarios que utilizan los servicios. En atención a esa clasificación de usuarios se definieron las actividades de sensibilización y apropiación del personal de la entidad, en coherencia con la priorización en la implementación de los servicios.

A continuación, se detallan las acciones adelantadas en cada una de las fases definidas en la metodología presentada:

Capítulo 3

1. Fase de selección de herramientas tecnológicas

Según Flores (2014) director general de Red Hat México, en la actualidad existe una gama soluciones tecnológicas que resuelven un sin número de problemas en entornos empresariales; soluciones comerciales que ameritan una inversión económica en licenciamiento, así como también soluciones con licenciamiento abierto, que implican el cumplimiento de las condiciones específicas estipuladas.

En esta fase se seleccionaron las herramientas de tecnologías de la información que apoyarán las necesidades diagnosticadas en el FOMVAS en el marco del plan estratégico de las tecnologías de la información PETI vigencia 2018, teniendo en cuenta para ello siete (7) criterios específicos de decisión: El recurso financiero, el tecnológico, el humano, el tipo de licenciamiento, la documentación, el soporte a usuarios y la comunidad que da soporte al uso de la herramienta.

Siendo el recurso financiero, la capacidad del FOMVAS para invertir en tecnologías; el recurso tecnológico, la infraestructura básica de tecnologías de la información con la que cuenta; el recurso humano, el personal técnico o profesional designado a gestionar los procesos informáticos; el tipo de licenciamiento, lo que se debe cumplir al adquirir la herramienta de tecnología de la información, bien sea una inversión económica o cumplir con condiciones específicas de la licencia; la documentación, hace alusión a los documentos de apoyo técnico disponibles de las herramientas de tecnología de la información ofrecida por sus creadores, que faciliten los procesos de instalación, configuración y usabilidad; el soporte a usuarios, está relacionado al tiempo que los desarrolladores brindarán apoyo a la herramienta y la comunidad, se refiere básicamente a la actividad de los usuarios experimentados con la herramienta en la internet en función a la resolución de problemas a nivel técnico de la herramienta.

Entre estos criterios descritos anteriormente se destacan el recurso financiero, ya que es justamente el dinero el que limita la adquisición de tecnologías de la información en las

empresas. Además, se consideran el tipo de licenciamiento y la comunidad, en cuanto a la documentación técnica de la herramienta, partiendo del hecho que las diseñan y desarrollan personas ajenas a la empresa donde se implementarán.

1.1. Problemas Identificados vs Servicios Tecnológicos

En primer lugar, se presenta la Matriz Servicios/Problemas, que facilita la identificación los servicios tecnológicos en atención a los problemas identificados en el FOMVAS:

Tabla 4

Problemas Identificados vs Servicios Tecnológicos

Servicios/ Problemas	DHCP estático	Autenticación de usuarios Centralizado	Gestión de activos tecnológicos	Alojamiento de archivos digitales centralizado	Filtrado de contenido web.	VPN	QoS	Firewall
Inadecuado control de acceso a los equipos de cómputos		X						
Inadecuado control de acceso a la red interna	X							
Inadecuada gestión de los activos de tecnología de la información			X					

Dificultad para acceder a los servicios de información desde una red externa						X		
Inadecuado control del ancho de banda del servicio de acceso a internet					X		X	X
Inadecuada gestión de la información				X				

Fuente: Elaboración propia.

De acuerdo a la tabla 4, se pueden apreciar los servicios tecnológicos establecidos por el FOMVAS que aportan a la mitigación de cada uno de los problemas identificados en el plan estratégico de las tecnologías de la información PETI.

A continuación, se describen de forma general los problemas que aquejan al FOMVAS en el marco de su infraestructura de tecnologías de la información y servicios.

1.1.1. Inadecuado control de acceso a los equipos de cómputos.

Se ha determinado que existe un deficiente control del acceso a sus equipos de cómputos, por parte de los empleados que laboran en FOMVAS, detallando que no se ha implementado un control de acceso adecuado a los activos informáticos y una política de uso responsable de las contraseñas de acceso a los equipos de cómputos. Así mismo, la entidad manifiesta que uno de los riesgos a los que se encuentra expuesta, es el acceso indebido a la información sensible de la entidad, siendo esta una preocupación permanente de los servidores públicos que laboran en la organización.

1.1.2. Inadecuado control de acceso a la red interna.

El Plan Estratégico de Tecnologías de Información también menciona la inexistencia de controles de acceso y monitoreo del uso de la red interna, tanto a usuarios internos, como a proveedores o terceros conectados a la misma. El Ingeniero a cargo de la gestión tecnológica de la entidad, detalla que no cuentan con herramientas que faciliten la separación de los servicios de red y la protección del acceso a los recursos compartidos a través de la misma, por lo cual, detalla que uno de los problemas más preocupantes es la fuga de datos a la que se expone la entidad.

1.1.3. Inadecuada gestión de los activos de tecnologías de la información.

Aunque el FOMVAS lleva un control de las cantidades de activos de información que poseen en la entidad, no se lleva un registro que permita contar con la información detallada de los activos y su ubicación al interior de la entidad, que favorezca los procesos de seguimiento, localización, mantenimiento y renovación de los mismos.

1.1.4. Dificultad para acceder a los sistemas de información desde una red externa.

El acceso a los sistemas de información existentes se realiza a través de la red de datos local de la entidad, ya que las aplicaciones que actualmente soportan los procesos de nómina, presupuesto, tesorería, contabilidad y de valorización solo pueden ser accesibles desde equipos

conectados a dicha red, enfatizando que esto afecta a la disponibilidad de la información para los servidores que hacen parte de la división técnica, que generalmente realizan actividades laborales en ambientes externos, lo cual les impide poder acceder a consultar o actualizar información en dichos sistemas información en tiempo real.

1.1.5. Inadecuada gestión del ancho de banda del servicio de acceso a internet.

Otra de las dificultades, está relacionada con la inexistencia de controles asociados al servicio de acceso a internet ofrecido a los servidores públicos de la entidad, lo cual impide que se haga una buena gestión del ancho de banda ofrecido, así como del uso que le dan los usuarios a dicho servicio.

1.1.6. Inadecuada gestión de la información.

La información utilizada por los servidores públicos se almacena en los diferentes activos de tecnología de la información, pero la misma, no se consolida, tampoco se comparte de manera que se pueda controlar el acceso a dichos recursos.

1.2. Herramientas de tecnologías de la información vs Servicios tecnológicos

Luego de una ardua investigación conceptual y técnica en cuanto a las herramientas de tecnologías de la información existentes que proporcionan los servicios tecnológicos establecidos en el apartado 1.1 “Problemas Identificados vs Servicios Tecnológicos”, las más relevantes en términos de reputación fueron: OpenLDAP, Active Directory, Apache Directory Server, Endian UTM, pfSense, Fortigate, OCS Inventory NG, Aranda Software, OwnCloud y NextCloud.

A continuación, se presenta la Matriz Servicios/Herramientas TI, que permite detallar el conjunto de herramientas asociadas a los servicios requeridos en el FOMVAS:

Tabla 5

Herramientas de tecnologías de la información vs Servicios tecnológicos

Servicios/ Herramientas TI	DHCP estático	Autenticación de usuarios centralizado	Gestión de activos tecnológicos	Alojamiento de archivos digitales centralizado	Filtrado de contenido web	VPN	QoS	Firewall
OpenLDAP		X						
pGina		X						
Active Directory		X						
Apache Directory Server		X						
Endian UTM	X				X	X	X	X
pfSense	X				X	X	X	X
Fortigate	X				X	X	X	X
OCS Inventory			X					
Aranda Software			X					
OwnCloud				X				
NextCloud				X				

Fuente: Elaboración propia.

A continuación, se presenta una breve descripción de las diferentes herramientas listadas en la tabla anterior:

1.2.1. pGina.

Según Nathan Yocom desarrollador del proyecto pGina, describe el proyecto como un "reemplazo flexible para el proveedor de credenciales predeterminado de Windows (o GINA en XP y sistemas anteriores). Con pGina, puede integrar clientes de Windows en sistemas de administración de identidades heterogéneos existentes". También puede admitir clientes de Windows con una sola base de datos OpenLDAP u otro backend de almacenamiento de identidades, sin la sobrecarga de una instalación completa de Active Directory (PGina, s.f.).

1.2.2. OpenLDAP.

Es un proyecto de implementación del protocolo LDAP, desarrollado bajo los lineamientos de software libre, en esencia se podría decir que es un tipo de base de datos jerárquica orientada a las consultas intensivas, tradicionalmente es utilizado como un servidor de autenticación en una red de datos, permitiendo de esta manera información centralizado de los datos de usuarios. El proyecto está publicado bajo su propia licencia OpenLDAP Public License y en el universo del software libre es uno de los proyectos más usados en cuanto a servidores de directorios (SomeBook, 2014).

1.2.3. Active Directory.

Es una herramienta que proporciona la empresa Microsoft para gestionar los recursos de red empresariales, bien sean usuarios, impresoras, permisos etc. Normalmente es implementado bajo un sistema operativo Windows server, ya que necesitas de otras herramientas para su correcto funcionamiento (Microsoft, 2017). Cabe destacar que también es una implementación del protocolo LDAP y que su implementación está ligada al pago de licencias de sistema operativo Windows Server y clientes que acceden al servidor Client Access License (CAL).

1.2.4. Apache Directory Server.

Es una implementación del protocolo LDAP, escrita en su totalidad con el lenguaje de programación JAVA, soporta el protocolo LDAP v3 y está disponible en la mayoría de sistemas

operativo al ser una herramienta multiplataforma, liberada bajo apache software license (Apache Directory, s.f.)

1.2.5. Endian UTM.

Es una distribución GNU/Linux, liberada bajo el licenciamiento GPL (General Public License) su versión comunity. Está basada en IPCop, diseñada para ser un sistema de fácil instalación y uso. Cumple con las funcionalidades de una UTM (Unified Threat Management) en español Gestión Unificada de Amenazas, es decir tiene funcionalidades de antivirus, firewall, IPS (sistema de prevención de intrusos), IDS (Sistema de detección de intrusos), filtrado de contenido web, NAT, VPN entre otras funcionalidades en cuanto a sistemas de seguridad perimetral (Endian, s.f.).

1.2.6. pfSense.

Es una distribución basada en el sistema operativo FreeBSD liberada bajo el licenciamiento de Apache license 2.0. Está personalizada y "específicamente diseñada para su uso como servidor de seguridad y enrutador que se administra completamente a través de la interfaz web. Además de ser una poderosa y flexible plataforma de enrutamiento, también incluye una larga lista de características relacionadas" (pfSense, s.f.).

1.2.7. Fortigate.

Es una UTM basado en hardware desarrollado por Fortinet. Distribuido bajo una licencia de software privado, "el sistema de FortiGate es un sistema capaz de detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, además cuenta con varios servicios de red tales como el servicio DHCP, routing, VPN, firewall entre otros servicios, los cuales se gestionan a través de una interfaz Web" (Fortinet, s.f.).

1.2.8. OCS Inventory NG.

Es una solución de origen francesa enfocada en la administración de activos de tecnologías de la información, está diseñada bajo una arquitectura de software cliente servidor, su principal función es inventariar todo el parque informático de una organización de forma automática y contar con la información de forma centralizada y ordenada, cabe destacar que es un software libre con licenciamiento GPL (General Public License) (OCS Inventory NG, s.f.).

1.2.9. OwnCloud.

Es una solución tecnológica que permite brindar un servicio del tipo alojamiento de archivo similar al popular Dropbox, esta solución está dividida en dos productos: en la versión estándar o mejor conocida como comunity y la versión enterprise, esta última liberada bajo un licenciamiento privativo, y la versión comunity bajo la licencia AGPLv3, la principal diferencia en cuanto a los software similares, es que owncloud permite crear una nube propia local en el centro de datos de la organización o de su preferencia, adquiriendo de esta manera control total de los archivos que reposan en el servidor (ownCloud, s.f.).

1.2.10. NextCloud.

Es una herramienta que

> Ofrece tecnología de colaboración en línea y sincronización de archivos local líder en la industria. Consiste en combinar la conveniencia y la facilidad de uso de soluciones de nivel de consumidor como Dropbox y Google Drive con la seguridad, privacidad y control de las necesidades comerciales. (NextCloud, s.f.).

Liberada bajo un licenciamiento privativo, y la versión comunity bajo la licencia AGPLv3.

1.2.11. Aranda Software.

Es una herramienta que

> Administra y controla la información financiera de los elementos de configuración de tu organización, al auditar la depreciación de activos o al conocer características como el precio de compra, relaciones entre facturas y contratos, centro de costo, localización y garantías correspondientes. Por cada activo, podrás tener un registro de existencia y versión respectiva, así como de tu historial. (Aranda Software, s.f.).

1.3. Matriz de selección de herramientas TI en función a los recursos del FOMVAS

Para la selección de las herramientas de tecnologías de la información que se adaptarán a las necesidades de implementación de la entidad, se realizó una reunión con el responsable de los servicios informáticos de la entidad y se invitó al Ingeniero Amaury Rodríguez Oviedo como experto temático, para valorar los criterios definidos para la evaluación de las herramientas y la ponderación de dichos criterios, de tal manera que se pudiera identificar la más adecuada en torno a las necesidades identificadas y las capacidades institucionales del FOMVAS.

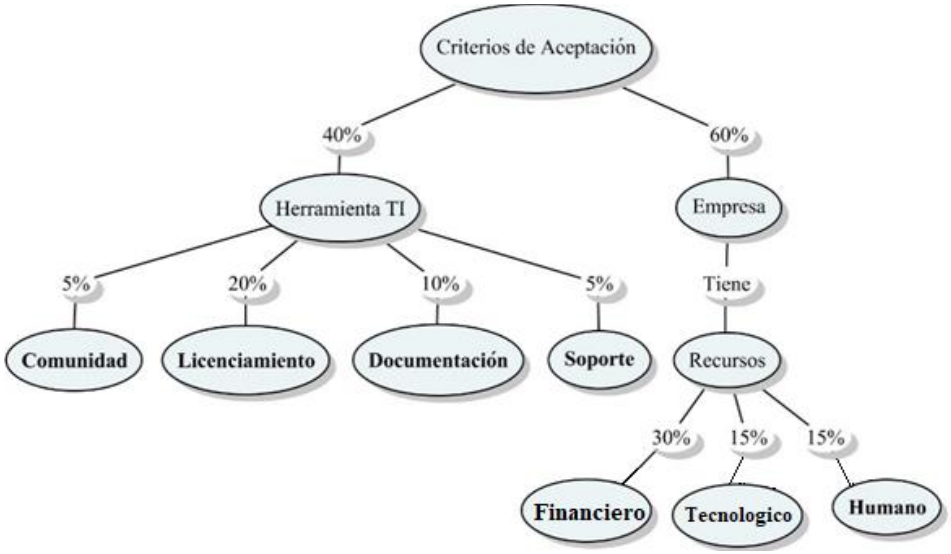

Figura 2. Criterio de aceptación

Fuente: Elaboración propia.

Se estableció que las capacidades del FOMVAS en relación con los recursos disponibles para la implementación del proyecto, tendrían una prioridad del 60% en la selección de la herramienta, mientras que las particularidades propias de la herramienta tendrían un 40%. La evaluación de dichos criterios permitió realizar una selección formal de las herramientas que permitiera descartarlas o aceptarlas de forma definitiva.

En la siguiente tabla se pueden observar los acuerdos que se obtuvieron de dicha reunión. En la parte superior se encuentran listados los criterios de decisión y en la parte lateral izquierda se encuentran las herramientas de tecnologías de la información destacadas en el apartado 1.2 “Herramientas de tecnologías de la información vs servicios tecnológicos”; se le dió un valor de uno (1) a los criterios que favorecen y cero (0) a los que no favorecen al FOMVAS, cabe destacar que la tabla fue diseñada y diligenciada con la ayuda del equipo mencionado.

Para aceptar las herramientas debido a que existen varias soluciones similares, se adoptó agruparlas de acuerdo a sus funcionalidades, estableciendo unos valores de (1) o (0) por cada criterio, de acuerdo con cada una de las herramientas de tecnología de la información identificadas. Posteriormente, se calculó el porcentaje de aceptación de cada una de las herramientas, presentado en la columna “Porcentaje” y finalmente se obtienen las herramientas candidatas en atención a la mayor puntuación porcentual.

Tabla 6

Matriz de selección de herramientas de tecnologías de la información

Matriz de selección de herramientas en función a los recursos del FOMVAS									
	Empresa 60%			Herramienta TI 40%				Total	
Criterios de decisión /Herramientas TI	Recurso Financiero 30%	Recurso Humano 15%	Recurso Técnico 15%	Licenciamiento 20%	Documentación 10%	Soporte 5%	Comunidad 5%	Porcentaje	Resultado
OpenLDAP	1	0	1	1 (Pública)	0	1	1	75	**Aceptada**
Active Directory	0	1	1	0 (Privada)	1	1	1	50	Rechazada
Apache Directory Server	1	0	1	1 (Pública)	0	1	0	70	Rechazada
Endian UTM	1	0	1	1 (Pública)	0	1	0	70	Rechazada
UTM pfSense	1	0	1	1 (Pública)	0	1	1	75	**Aceptada**
UTM Fortigate	0	1	1	0 (Privada)	1	1	1	50	Rechazada
OCS Inventory NG	1	0	1	1 (Pública)	0	1	1	75	**Aceptada**
Aranda Software	0	1	1	0 (Privada)	0	1	1	40	Rechazada
OwnCloud	1	1	1	1 (Pública)	1	1	1	100	**Aceptada**
NextCloud	1	0	1	1 (Pública)	0	1	0	70	Rechazada
Ubuntu Server	1	1	1	1 (Pública)	1	1	1	100	**Aceptada**
Debian Server	1	0	1	1 (Pública)	0	1	0	70	Rechazada
Windows Server	0	1	1	0 (Privada)	1	1	1	50	Rechazada

Valor	Descripción
1	Favorece
0	No favorece

Fuente: Elaboración propia.

Finalmente se puede observar que las herramientas de tecnologías de la información aceptadas de acuerdo a los criterios de decisión previamente establecidos fueron: OpenLDAP, pfSense, OCS Inventory NG, OwnCloud y Ubuntu server. Donde OpenLDAP se encargará de proveer el servicio de directorio, pfSense será una distribución que proveerá los servicios de Firewall, VPN, Filtrado de contenido web y Calidad de servicio, OCS Inventory NG por su parte se encargará de recolectar los datos de forma automática de los activos para el inventario tecnológico, OwnCloud brindará una nube privada de datos empresariales y por último Ubuntu Server será el sistema operativo donde se implantaran las herramientas de tecnología de la información.

1.4. Matriz Compilada de Servicios Tecnológicos

En la siguiente tabla, se presenta el conjunto de servicios tecnológicos establecidos por el FOMVAS “Servicios TI”, se conceptualizan los servicios tecnológicos “¿Qué es?”, se describe de forma general lo que aporta el servicio tecnológico dentro de una organización “¿Qué soluciona?” de igual forma se describe el problema que ataca directamente en el FOMVAS “Problema”, se especifican los beneficios que aporta el servicio tecnológico en el FOMVAS “Cómo aplica en el FOMVAS?”, así como también se especifican las herramientas de tecnologías de la información seleccionadas según las conveniencias de la entidad “Herramientas TI” y finalmente se denota el pilar de seguridad de la información al que aporta el servicio tecnológico.

Nota: Los pilares de la seguridad de la información están escritos de acuerdo a las iniciales de las mismas, es decir:
I= Integridad**, D=**Disponibilidad**, C=**Confidencialidad.

Tabla 7.

Matriz Compilada de Servicios Tecnológicos

Servicios TI	¿Qué es?	¿Qué soluciona?	Problema	¿Cómo aplica en el FOMVAS?	Herramienta T.I.	I	D	C
Servicio de gestión de activos tecnológicos	+Según Pino (2013) es un método utilizado para recolectar información cuantitativa de los activos tecnológicos disponibles en una organización, ayudándoles de esta manera en la planificación e identificación de necesidades tecnológicas a corto plazo.	+Identificación de los activos. +Identificación del estado de los activos (sirve o no sirve). +localización. +Asignación.	+No cuenta con información detallada de los activos, de su estado actual, localización y asignación que les facilite tomar decisiones (relacionadas con la gestión preventiva, correctiva y renovación de los activos) a mediano y corto plazo.	+Permite gestionar el ciclo de vida del activo.	+OCS Inventory		X	
Servicio de VPN	+Según Ardila (2015) es un servicio que provee una red privada que se extiende a través de internet, concediendo	+Teletrabajo	+Dificultades para acceder a la información relacionada con los sistemas de información SAV	+Permite acceder a los sistemas de información (Sistema avanzado de valoración SAV) y HELISA alojado	+pfSense (OpenVPN)		X	X

	que las máquinas conectadas puedan enviar y recibir datos de forma segura como si estuvieran conectados a una red de datos local.		(Sistema avanzado de valorización) y HELISA los cuales solo pueden ser utilizado desde la red interna de la organización.	en la intranet del FOMVAS				
Servicios TI	**¿Qué es?**	**¿Qué soluciona?**	**Problema**	**¿Cómo aplica en el FOMVAS?**	**Herramienta T.I.**	**I**	**D**	**C**
Servicio de Firewall	Es un dispositivo (hardware + software) que funciona como filtro entre redes, de esta manera restringe o da acceso a las comunicaciones entrantes o salientes que se dan entre las redes. Por lo general se usa como filtro entre el internet y la red de área local LAN.	+Bloquea el tráfico innecesario +Gestión del tráfico de red entre la LAN y la WAN (internet) +Gestión del tráfico entre redes LAN	+No existe control sobre las aplicaciones que utilizan puertos de comunicación entre la red interna y la internet +Inadecuada seguridad informática	+ Permite conceder y denegar el tráfico saliente y entrante de la red por parte del FOMVAS. +Protección contra amenazas externas.	+ pfSense (Packet Filter)	X	X	X
Servicio DHCP Estático	Según el instituto Puig castellar, es un servicio que permite	+Asignación de dirección IP a computadoras	+Cualquier persona que tenga acceso con un equipo de	+Permite la asignación de una dirección IP	+pfSense (DHCP Server)		X	x

	la asignación dinámica o estática de direcciones IP a las computadoras de una red LAN desde de un servidor centralizado.	de forma automática ó estática de acuerdo a la dirección física de la computadora.	cómputo o un móvil a la red corporativa gana privilegios de acceso a todos los recursos de red, afectando la seguridad de la información de la organización y de los activos.	automáticamente a computadores conocidos y la negación de acceso a equipos desconocidos.				
Servicios TI	**¿Qué es?**	**¿Qué soluciona?**	**Problema**	**¿Cómo aplica en el FOMVAS?**	**Herramienta T.I.**	**I**	**D**	**C**
QoS	+Se refiere a la "capacidad de una red para lograr el máximo ancho de banda y tratar otros elementos de rendimiento de la red como la latencia, la tasa de error y el tiempo de actividad. La calidad del servicio también implica controlar y administrar los recursos de la red al establecer	+Congestión de la red. +Abuso de ancho de banda.	+Inadecuado uso del canal de internet, afectado por la inexistencia de un control sobre los recursos de ancho de banda del canal, permitiendo que un usuario que haga mal uso de servicio afecte la disponibilidad del servicio para otros usuarios.	+Permite optimizar el canal de datos a usuarios críticos del FOMVAS.	+pfSense (Traffic Shaper)		X	

	prioridades para tipos específicos de datos (video, audio, archivos) en la red.'' (tecnopedia, s.f.)							
Servicios TI	**¿Qué es?**	**¿Qué soluciona?**	**Problema**	**¿Cómo aplica en el FOMVAS?**	**Herramienta T.I.**	**I**	**D**	**C**
Servicio de filtrado de contenido web.	+Es un servicio que permite el acceso o negación a los distintos sitios Web	+Restricciones de páginas WEB no permitidas	+Inadecuada gestión sobre los contenidos al cual acceden los usuarios a través del servicio de internet corporativo.	+Permite crear una lista blanca y negra de páginas web de acuerdo con las políticas de seguridad del FOMVAS.	+ pfSense (SquidGuard) + pfSense (Squid Proxy Server)			
Servicio de alojamiento de archivos digitales centralizado	+Es un servicio de alojamiento de archivos, diseñado exclusivamente para alojar archivos de usuarios, donde dichos archivos se pueden compartir con los usuarios que se deseen y estos pueden ser imágenes, videos, textos, etc.	+Permite tener un respaldo de la información en caso de que el equipo de cómputo local falle. +Ahorro de tiempo al compartir información internamente.	+Inexistencia de un respaldo de la información digital de los empleados. +Retrasos al compartir información entre usuarios internos	+Permite gestionar la información del FOMVAS.	+OwnCloud		X	X

Servicios TI	¿Qué es?	¿Qué soluciona?	Problema	¿Cómo aplica en el FOMVAS?	Herramienta T.I.	I	D	C
Servicio de autenticación de usuario centralizado	Es un método de autenticación, donde los usuarios tienen que identificarse y autenticarse con credenciales válidas para acceder a aplicaciones, servicios de red etc. donde dicha identificación y credenciales son verificadas en un servidor.	+Proporciona seguridad a los equipos de cómputo por medio del login de usuarios autorizados.	+Inadecuado control de acceso a los equipos de cómputo, permitiendo el acceso indebido a la información del FOMVAS por parte de servidores públicos sin autorización y terceros.	+Gestión de información de usuarios en el FOMVAS de manera centralizada. (base de datos de empleados) +Mayor control de administración de cuentas de usuarios de las computadoras	+openLDAP. +PGina.	X	X	X

Fuente: Elaboración propia.

2. Fase de diseño de servicios tecnológicos

2.1. Servicio de gestión de activos tecnológicos

Figura 3. Servicio de gestión de activos tecnológicos.

Fuente: Elaboración propia.

El servicio de gestión de activos tecnológicos está orientado a facilitar el control del proceso de inventario de los activos tecnológicos del FOMVAS, con el propósito de aportar a la implementación de los procesos institucionales de gestión de la seguridad de la información, en particular a la gestión de activos, tal y como se precisa en el apartado “Gestión de activos” del estándar ISO 27002 de 2015.

La adopción del servicio de gestión de activos tecnológicos por parte del FOMVAS, permitirá implementar los procesos de identificación, caracterización, localización, asignación y gestión del cambio de los activos tecnológicos existentes, que permiten manipular la información que apoya la gestión administrativa institucional; soportados en el uso de un sistema de información web centralizado, que facilita los procesos de registro, consulta, seguimiento y control del uso de los activos tecnológicos a lo largo de su ciclo de vida en la organización.

Los activos tecnológicos son todos aquellos que permiten a través de su hardware, software y dispositivos de red, convertir, almacenar, procesar, trasmitir, buscar y administrar la

información digital en una organización, organizados en 3 categorías, tales como las redes, los terminales y los servicios de tecnologías de información. Las redes apoyan los procesos de trasmisión de la información; los terminales apoyan los procesos de tratamiento, procesamiento y almacenamiento de la información; y finalmente los servicios de tecnologías de información aportan independencia de la infraestructura y una alta orientación a satisfacer las necesidades organizacionales.

Este servicio requiere que la organización recolecte y almacene en el sistema de información los datos de cada uno de los activos de tecnologías de información existentes, para lo cual se han definido un conjunto de datos mínimos necesarios para la inclusión de cualquier activo. Los cuales posteriormente serán utilizados para facilitar las labores de consulta y actualización del estado de los mismos, así como para la generación de informes que aporten a la toma de decisiones institucional.

La implementación del servicio de gestión de activos se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS controlar el inventario de activos tecnológicos de la entidad, apoyado en la utilización del sistema de información OCS Inventory NG, el cual es una herramienta open source, orientada a la administración y despliegue de activos tecnológicos.

El sistema de Información OCS Inventory NG apoyara los procesos de identificación y búsqueda de activos tecnológicos en la organización, así como los procesos de caracterización, localización, asignación y gestión del cambio, apoyándose en una estrategia de seguimiento optimizada, en la cual a cada uno de los activos se instala un software cliente, también denominado (Agente), que facilita la comunicación automática entre el activo y el servidor de inventario, permitiéndole la auto-descripción a cada activo, partiendo de un conjunto de características comunes que se trasmiten de manera periódica, en atención a los cambios que pudiera tener el activo.

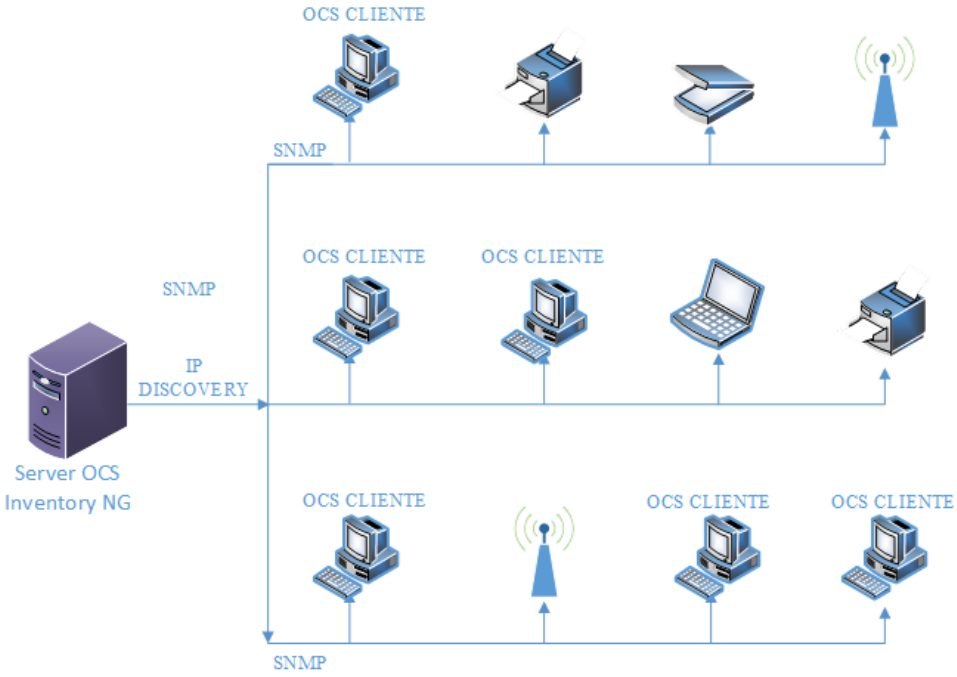

Figura 4. Representación de OcsInventory NG en red

Fuente: Elaboración propia.

El sistema de información OCS Inventory NG facilita la caracterización de los activos que tengan instalado el (Agente); sin embargo, reconociendo la existencia de activos a los cuales no es posible instalarlo, OCS Inventory NG realiza una exploración de la red a través del servicio IP Discover, para identificar activos conectados a la red, que no utilizan el (Agente), tales como impresoras, escáneres, enrutadores, móviles, entre otros. Así mismo, utiliza un servicio complementario de escaneo de la red apoyado en el protocolo SNMP para intentar recopilar la mayor cantidad de información de los dispositivos identificados, así como de sus características.

De igual manera, el administrador del sistema de información OCS Inventory NG podrá agregar datos personalizados que le permitan al sistema adaptarse a las necesidades específicas del FOMVAS, relacionada con la gestión de los datos, que permitan facilitar las actividades de consulta, seguimiento y control del inventario de activos.

2.2. Servicio de alojamiento de archivos digitales centralizado

El servicio de alojamiento de archivos digitales centralizado está orientado a facilitar la gestión de la información digital del FOMVAS, así como también apoyar la gestión de la seguridad de la información de la organización, tal y como se precisa en el apartado “Control de acceso a sistemas y aplicaciones” del estándar ISO 27002 de 2015

La adopción del servicio de alojamiento de archivos digitales centralizados por parte del FOMVAS, permitirá implementar los procesos de creación y almacenamiento de la información importante del FOMVAS, permitiendo así gestionar la información que apoya la estrategia empresarial de la entidad; soportados en el uso de un sistema de información web centralizado, que facilita los procesos de modificación, compartición, eliminación y control del uso de la información sensible a lo largo de su ciclo de vida en la organización.

Los archivos digitales centralizados, son toda aquella información que contienen diferentes tipos de formatos y que se encuentren almacenada en una sola ubicación, dichos formatos están clasificados por categorías, tales como fotos, videos, texto y audios, los cuales aportan información valiosa que permitan apoyar la estrategia de negocio del FOMVAS.

El servicio permite que el FOMVAS pueda recopilar y almacenar en el sistema de información los archivos digitales valiosos de cada uno de los empleados de la entidad, para lo cual se ha definido que toda aquella información que sea valiosa para el FOMVAS se llevara a cabo el proceso de inclusión tales como los productos que van generando cada uno de los servidores públicos en su día a día. Los cuales posteriormente serán utilizados para facilitar las labores de consulta y compartición de la información, así como para la generación de informes que aporten a la toma de decisiones institucional.

La implementación del servicio de alojamientos de archivos digitales centralizado se apoya bajo unos procesos y procedimientos, que permite a cada uno de los empleados del FOMVAS gestionar, respaldar y controlar la información valiosa de la entidad de la mejor

manera, apoyado en la utilización del sistema de información OwnCloud, el cual es una herramienta open source, orientada a la gestión y control de la información digital.

El sistema de Información OwnCloud apoyara los procesos de alojamiento y respaldo de archivos de cada uno de los empleados de la organización, así como los procesos de modificación, compartición y eliminación, por otra parte, los usuarios gestionarán la información por medio del gestor web de OwnCloud, en la cual el usuario deberá acceder en su navegador preferido a la URL *http://172.16.1.200/owncloud*, seguidamente aparecerá la página principal, en donde el usuario se deberá autenticarse para poder tener acceso a su apartado privado de alojamiento de archivos.

El sistema de información OwnCloud facilitará crear las carpetas que desee, permitiendo así clasificar la información y guardar en ellas los distintos archivos que sean importante para la entidad, por otro lado, el usuario podrá modificar y eliminar archivos, otros de los beneficios que ofrece esta herramienta es poder compartir información a aquellos usuarios que desee que tengan acceso y así mismo poder asignarle el nivel de privilegios que sé que tenga cada usuario en particular a su producto, ya sea de lectura, modificación o volver a compartir esa información con otros empleados.

2.3. Servicio de filtrado de contenido web

El servicio de filtrado de contenido web está orientado a facilitar el control de acceso a los sitios web que ofrece el servicio de acceso a internet al FOMVAS, con el propósito de aportar a la implementación de los procesos institucionales de gestión de la seguridad de la información, en particular al filtrado de contenido.

La adopción del servicio de filtrado de contenido web por parte del FOMVAS, permitirá implementar los procesos de identificación y establecimiento de reglas de los contenidos, que permiten restringir el acceso a los sitios web con contenidos que no aporten a la estrategia empresarial del FOMVAS, establecidos en conjunto por el jefe de sistemas y gerente de la

entidad, soportado en el uso de un software web especializado, facilitando los procesos de control del acceso al servicio de internet.

Los contenidos web son todo tipo de información que hacen parte de un sitio web y que a través del servicio de acceso a internet se podrá tener acceso a su contenido; tales como textos, videos, audios y fotos, que podrán ser visualizados por el usuario por medio de un navegador web.

El servicio requiere que la organización registre en la herramienta un conjunto de dominios web o de categorías de información a los cuales se desea restringir el acceso, definidos por las políticas de seguridad de la información de la entidad.

La implementación del servicio de filtrado de contenido web, se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS, controlar el acceso a los sitios web que no aporten a la estrategia de negocia de la entidad, apoyado en la utilización del software web pfSense, el cual es una herramienta que brinda varios servicios, entre ellos el servicio de filtrado de contenido web, dicha herramienta es open source, orientada al control del servicio de acceso a internet.

pfSense apoyará los procesos de identificación y filtrado de los sitios web a los que se acceden diariamente los empleados en la organización, apoyándose en una estrategia de control optimizada, en la cual se establecen un conjunto de reglas, es decir, registrar una a una los dominios de los sitios a los cuales se les desea hacer el respectivo filtrado mencionado.

El software web pfSense facilita el filtrado de contenido web por medio del registro de los dominios de las páginas web, así mismo, ofrece el servicio de listas negras donde se ven reflejado todos los sitios web y así mismos clasificados por su contenido, lo que facilitaría el filtrado a los sitios web por tipo de contenido.

2.4. Servicio de gestión de ancho de banda del servicio de acceso a internet

El servicio de gestión de ancho de banda está orientado a facilitar el control del uso inadecuado de la velocidad de subida y bajada de paquetes a través del servicio de acceso a internet del FOMVAS, con el propósito de aportar a la implementación de los procesos institucionales de gestión de la seguridad de la información, en particular al control del ancho de banda.

La adopción del servicio de gestión de ancho de banda por parte del FOMVAS, permitirá apoyar los procesos de identificación y asignación del ancho de banda a los equipos de cómputos, de este modo gestionar el uso adecuado del servicio de acceso a internet, soportado en el uso de un software web especializado, que facilite el control de las distintas velocidades asignadas a cada uno de los equipos de cómputos para el servicio de acceso a internet.

Este servicio requiere que la organización recolecte y almacene en el software web los datos de cada uno de las velocidades de trasmisión que cada usuario necesita para hacer uso del servicio de acceso a internet de manera adecuada y óptima para su labor en la institución, para lo cual se han definido un conjunto de velocidades de trasmisión mínimas y máximas que dependerán de cada departamento u oficina, los cuales posteriormente serán utilizados para facilitar el control del ancho de banda del servicio de acceso a internet.

La implementación del servicio de gestión de ancho de banda del servicio de acceso a internet se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS controlar el uso adecuado del ancho de banda de la entidad, apoyado en la utilización del software web pFsense, el cual es una herramienta open source, orientada al control del uso adecuado del servicio de acceso a internet.

PfSense apoyará los procesos de identificación y control de ancho de banda a los empleados del FOMVAS que hacen uso del servicio de acceso a internet, apoyándose en una estrategia de control optimizada, en la cual se establecen un conjunto de reglas donde se deben

registrar las diferentes velocidades trasmisión de datos y asignarla a cada oficina ó a cada empleado en particular de la organización.

El software web PfSense facilita el control del ancho de banda del servicio de acceso a internet a través de la asignación por defecto de reglas, donde se establece el valor fijo de la velocidad de subida y bajada de paquetes a cada uno de los empleado de la entidad, así mismo se tendrá en cuenta que existen usuarios que se ven con la necesidad de contar con mayor velocidad de transmisión de datos que otros usuarios, es decir, la asignación del ancho de banda dependerá de las actividades que realicen día a día en función al uso del servicio de acceso a internet.

2.5. Servicio DHCP estático

El servicio DHCP estático está orientado a facilitar el control de acceso a la red LAN institucional del FOMVAS, con el propósito de aportar a la implementación de los procesos institucionales de gestión de la seguridad de la información, en particular al control de la red interna.

La adopción del servicio DHCP por parte del FOMVAS, permitirá implementar los procesos de identificación y asignación de permisos a los recursos compartidos de la entidad a través de los activos tecnológicos existentes, que permiten manipular la información que apoya la gestión administrativa institucional; soportados en el uso de un software especializado web, que facilita los procesos de registro, consulta y control de los activos tecnológicos que hacen uso de los recursos compartidos de la organización.

Este servicio requiere que la organización recolecte y almacene en el software web algunos de los datos que identifican a un activo en una red datos; tales como la dirección MAC y la dirección IP, para lo cual el servicio ha definido un conjunto de datos mínimos necesarios para la inclusión de cualquier equipo de cómputo. Los cuales posteriormente serán utilizados para facilitar el control de acceso adecuado a la red interna, así como para garantizar la seguridad de la información de los recursos compartidos de la institución.

La implementación del servicio DHCP se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS controlar el acceso inadecuado a la red de dato local de la entidad, apoyado en la utilización de un software web especializado PfSense, el cual es una herramienta open source, orientada al control de acceso adecuado a la red interna de la organización.

El software web PfSense apoyara los procesos de identificación y registro de cada uno de los equipos de cómputos que hacen parte del FOMVAS, en la cual a cada uno de los activos se le obtiene la dirección MAC (Media Access Control), la cual es un identificador único para cada tarjeta de red instalada en el equipo ya sea una tarjeta inalámbrica o una tarjeta Ethernet, estas tarjetas de red permiten la comunicación de datos entre computadoras que se encuentren en la misma red.

PfSense permitirá mapear la dirección MAC de la tarjeta de red con una dirección IP, es decir, cuando un equipo de cómputo intente conectarse a la red, inmediatamente PfSense a través del servicio DHCP verificará si la dirección MAC de ese equipo se encuentra registrada, en caso de que este registrada el servicio DHCP le asignara una dirección IP correspondiente a la red de la entidad y de esta manera pueda hacer uso de los recursos compartidos que hay en la entidad.

Por otro lado, cuando el usuario empiece a utilizar su equipo de trabajo, este no tendrá problema alguno, ya que no tiene que hacer ninguna configuración en particular, el equipo de cómputo automáticamente hace la petición de la dirección IP y como se encuentra registrado al servicio, el servidor DHCP le asignara la dirección IP, dicha dirección fue establecida una vez en el registro, de esta manera el usuario podrá seguir operando su equipo de cómputo de la igual forma en la que la hacía antes.

2.6. Servicio de autenticación de usuario centralizada

El servicio de autenticación de usuario centralizado está orientado en facilitar el control de acceso a los equipos de cómputo con los que cuenta el FOMVAS, con el propósito de aportar

a la implementación de los procesos institucionales de gestión de la seguridad de la información, al control de credenciales, tal y como se precisa en el apartado “Gestión de acceso de usuarios” del estándar ISO 27002 de 2015.

La adopción del servicio de autenticación de usuarios centralizado por parte del FOMVAS, permitirá implementar los procesos de identificación y autenticación del acceso a los equipos de cómputos existentes, que permiten apoyar el control administrativo institucional; soportados en el uso de la herramienta de software centralizada OpenLDAP, que facilita los procesos de registro y consulta de los usuarios para poder acceder a los distintos sistemas operativos de la organización.

Los usuarios son todas aquellas personas que por medio de sus cuentas de usuarios pueden acceder a cualquier herramienta de software, lo cual le permite convertir, almacenar, procesar, trasmitir, buscar y administrar la información digital en dichas herramientas.

Este servicio requiere que la organización recolecte y almacene en OpenLDAP los datos de cada uno de los empleados del FOMVAS existentes, para lo cual se han definido un conjunto de datos mínimos necesarios para la inclusión de los usuarios. Los cuales posteriormente serán utilizados para facilitar el control de acceso a los sistemas operativos.

La implementación del servicio de autenticación de usuarios centralizados se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS controlar el acceso indebido a los diferentes sistemas operativos existentes en el FOMVAS, apoyado en la utilización de la herramienta de software OpenLDAP, el cual es una herramienta open source, orientada al control de acceso de los equipos de computos.

OpenLDAP apoyará los procesos de identificación y registro de los empleados de la organización, así como el proceso de autenticación, apoyándose en una estrategia de seguimiento optimizada, en la cual a cada uno de los activos se instala un software cliente, también llamado (PGina), que facilita la comunicación automática entre el activo y el servidor de directorio.

2.7. Servicio de Firewall

El servicio de firewall está orientado en facilitar el control del flujo del tráfico de la red entrante y saliente del FOMVAS, con el propósito de aportar a la implementación de los procesos institucionales de gestión de la seguridad de la información, en particular a la gestión de activos.

La adopción del servicio de firewall por parte del FOMVAS, permitirá implementar los procesos de identificación y asignación de permisos a los diferentes puertos existentes, que apoya la gestión administrativa institucional; soportados en el uso de una herramienta web centralizada, que facilita los procesos de registro y control del flujo de tráfico que se genera diariamente entre las diferentes redes de datos en la organización.

> Los números de puertos son aquellas direcciones lógicas de cada aplicación o proceso que utiliza una red o Internet para comunicarse. Un número de puerto identifica de forma única una aplicación basada en la red en una computadora. A cada aplicación / programa se le asigna un número de puerto entero de 16 bits. Este número es asignado automáticamente por el sistema operativo, manualmente por el usuario o se establece como predeterminado para algunas aplicaciones populares. (Techopedia, s.f.).

Este servicio requiere que la organización establezca en el software web un conjunto de reglas a los distintos puertos que identifican a un programa en una red datos, para lo cual el servicio ha definido un conjunto de datos mínimos necesarios para la creación de estas reglas. Los cuales posteriormente serán utilizados para facilitar el control de acceso adecuado a la red interna, así como para garantizar la seguridad de la información de los recursos compartidos de la institución.

La implementación del servicio del firewall se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS controlar el acceso inadecuado a los distintos puertos con los que cuentan las

aplicaciones en red de dato local de la entidad, apoyado en la utilización de un software web especializado PfSense, el cual es una herramienta open source, orientada al control de acceso adecuado a la red interna de la organización.

El software web PfSense apoyara los procesos de identificación y registro de cada uno de los puertos que identifican a cada aplicación que haga parte del FOMVAS, estos puertos pueden ser propios de cada aplicación o en su defecto se le asignan un numero de puerto cuando se instala, la cual es un identificador único para cada aplicación o software de red de datos, los cuales permiten la comunicación de datos entre otras aplicaciones que se encuentren en la red.

PfSense permitirá restringir la comunicación con los distintos puertos de las aplicaciones a los que no se desea que haya comunicación entre ellos, es decir, cuando un equipo de cómputo intente comunicarse con algún un puerto, inmediatamente pfSense a través del servicio de firewall verificará si el puerto tiene permiso, en caso de que tenga permiso este podrá comunicarse con dicho puerto sin problema.

2.8. Servicio de VPN

El servicio de VPN está orientado a facilitar el acceso adecuado a aquellos equipos de cómputos que se encuentren en una red externa a los recursos compartidos que una organización posee en su red interna por medio del servicio de acceso a internet, con el propósito de aportar a la implementación de los procesos institucionales de gestión de la seguridad de la información, en particular a la disponibilidad de la información, tal y como se precisa en el “Acceso a redes y servicios en red” del estándar ISO 27002 de 2015.

La adopción del servicio de VPN por parte del FOMVAS, permitirá implementar los procesos de identificación, registro de usuario y establecimiento de reglas del puerto de comunicación, que permiten el acceso a los distintos servicios y archivos compartidos del FOMVAS para aquellos empleados que hacen parte de la entidad pero que laboran en ambientes externos, de tal manera que se le garantice la disponibilidad de la información de la entidad, soportado en el uso de un software web especializado, facilitando los procesos de acceso y el control del uso de los recursos compartidos del FOMVAS.

Una conexión VPN permite a un dispositivo conectarse a una red de datos local de una entidad sin necesidad que dicho dispositivo se encuentre físicamente conectado a la red de la empresa, sino a través de Internet, es decir, un dispositivo que no se encuentre en la entidad pero que tiene la necesidad de estar conectado a la red de dato local para hacer uso de los recursos compartidos. tanto este dispositivo como la red a la que se desea tener acceso deberán contar con acceso a internet, luego por medio de una red virtual que crea el servicio de VPN se podrá hacer la correcta conexión a la red institucional (Xataka, 2018).

El servicio requiere que la organización registre en el software web a los distintos usuarios a los cuales se desea facilitar el acceso a la red interna, para lo cual ya se han establecidos en las políticas de seguridad de la información de la entidad. Los cuales posteriormente permitirán acceder a los recursos compartidos de la entidad.

La implementación del servicio de VPN se apoya en un conjunto de procesos y procedimientos que permiten al administrador de los servicios de tecnologías de información del FOMVAS facilitar el acceso a la red interna para aquellos empleados que laboran en ambientes externos, apoyado en la utilización del software web PfSense, el cual es una herramienta que brinda varios servicios, entre ellos el servicio de VPN, dicha herramienta es open source, orientada al control del servicio de acceso a internet.

pfSense apoyará los procesos de identificación y control de acceso de red interna de la organización, apoyándose en una estrategia de control optimizada, en la cual registran los empleados y se establecen un conjunto de reglas, es decir, registrar los usuarios y posteriormente habilitar los puertos necesarios para permitir el acceso adecuado a la red a la red. Luego para realizar la conexión adecuada se instala un software cliente, que facilita la comunicación automática entre el dispositivo y el servidor de VPN.

3. Fase de Implementación de los servicios tecnológicos

La implementación de los servicios se realizó en atención a las siguientes actividades: Definición de la infraestructura de tecnología requerida para los servicios, infraestructura requerida por los clientes, instalación y configuración de las herramientas seleccionadas, configuración de los servicios de tecnología definidos, pruebas de los servicios, despliegue de los servicios, transición de los servicios y puesta en producción de los mismos.

3.1. Infraestructura de tecnología de la información requerida para los servicios

3.1.1. Requisitos mínimos de hardware recomendados para el funcionamiento de los servicios

Los requisitos mínimos de hardware para el funcionamiento de los servicios se establecen en atención a las necesidades de la entidad y las capacidades en términos de recursos, priorizando tres aspectos esenciales: La capacidad de procesamiento, la capacidad de memoria RAM y la capacidad de almacenamiento de información de los equipos requeridos.

Para la implementación de los servicios identificados se podrían utilizar diferentes maquinas servidoras, sin embargo, en concertación con el jefe de informática de la entidad, se identifica la necesidad mínima de utilización de dos máquinas físicas que actúen como servidoras en relación con los servicios definidos.

Una de las maquinas servidoras que se identificó como necesaria, fue la que prestaría los servicios de autenticación, almacenamiento y gestión de inventario de la entidad, a la cual denominamos VALYRIA; y la otra sería la que soporta los servicios de Firewall, DHCP, VPN, QoS y Filtrado de contenido web, la cual denominamos como WINTERFELL.

Tabla 8

Requisitos mínimos de hardware VALYRIA.

Requisitos mínimos de hardware recomendados - VALYRIA	
Procesador	Mínimo Intel core I5 Doble Núcleo a 3 Ghz
Memoria RAM	Mínimo 8GB
Espacio en disco duro	Mínimo 500GB

Fuente: Elaboración propia.

Tabla 9

Requisitos mínimos de hardware WINTERFELL

Requisitos mínimos de hardware recomendados - WINTERFELL	
Procesador	Intel Pentium a 3Ghz
Memoria RAM	Mínimo 4GB
Espacio en disco duro	Mínimo 250GB

Fuente: Elaboración propia.

Es importante precisar que el servidor WINTERFELL, requiere de al menos dos tarjetas de red ethernet a mínimo 100Mbps.

Nota: Las Maquinas servidoras descritas anteriormente, son máquinas físicas, no virtualizadas.

3.1.2. Requisitos recomendados de hardware para el funcionamiento de los servicios.

Aunque los requisitos mínimos se fundamentan en pruebas realizadas en ambientes restringidos, se han definido unas recomendaciones que aporten al mejoramiento de la prestación de dichos servicios, sin embargo, su implementación está sujeta a las capacidades de la entidad.

Tabla 10

Requisitos recomendados de hardware VALYRIA

Requisitos mínimos de hardware- VALYRIA	
Procesador	Recomendado Xeon E7- 8890
Memoria RAM	Mínimo 16GB
Espacio en disco duro	Mínimo 1TB

Fuente: Elaboración propia.

Tabla 11

Requisitos recomendados de hardware WINTERFELL

Requisitos mínimos de hardware- WINTERFELL	
Procesador	Recomendado XEON E7- 8890
Memoria RAM	8GB
Espacio en disco duro	500GB

Fuente: Elaboración propia.

3.1.3. Requisitos software para el funcionamiento de los servicios

Para la implementación del proyecto, además de las herramientas previamente seleccionadas, se requieren otras herramientas como requisitos obligatorios para el correcto funcionamiento de todas las herramientas de tecnologías de la información.

Las herramientas de requisito obligatorio, están descritas en la documentación técnica oficial de cada herramienta tecnológica (ownCloud, OCS Inventory NG,openLDAP)

A continuación**,** se detallan los requisitos de software requeridos para la implementación de los servicios:

Tabla 12

Requisitos para el funcionamiento de los servicios

Herramientas TI	Versión
Ubuntu Server	v16.04.2 LTS
Apache2	v2.4.18
PHP	v7.0.32
MySQL	v14.14
PERL5	v22
phpLDAPadmin	v3.3
OpenLDAP	v2.4.42
OCS Inventory NG	v2.5
OwnCloud Server	v10.01
pfSense	v2.4.4

Fuente: Elaboración propia.

3.1.4. Requisitos de red

Para el funcionamiento de los servicios tecnológicos se requiere una infraestructura de red LAN, que permitan la conexión entre los computadores de la red, apoyada en un cableado estructurado de mínimo categoría 5e o superior y una conexión con acceso internet.

3.2. Infraestructura de tecnología de la información requerida para los clientes

3.2.1. Requisitos mínimos de software para el funcionamiento de los servicios en clientes

Para garantizar el acceso a los servicios, se hace necesario la implementación de los siguientes softwares en las estaciones clientes:

Tabla 13

Requisitos de software para el funcionamiento de los servicios en clientes

Herramientas TI	Versión
Windows OS	7
OCS Agent	v2.5
pGina	v3.1.8.0 Stable
ownCloud desktop	v2.0
Navegador web	N/A

Fuente: Elaboración propia.

3.2.2. Requisitos de red

Garantizar la conectividad de cada estación de trabajo a la Red LAN de la entidad.

3.3. Instalación y configuración preliminar de las herramientas de tecnologías de la información.

3.3.1. Servidores.

El conglomerado de servicios tecnológicos está soportado bajo una plataforma de hardware y software; donde algunas herramientas tecnológicas son dependientes, es decir requieren de otras herramientas de tecnologías de la información para su correcto funcionamiento.

Partiendo de lo anterior se estableció un orden en cuanto a la instalación de todas las herramientas de tecnologías de la información de la siguiente manera:

Primeramente, se instaló el sistema operativo Ubuntu Server 16.04 LTS en una máquina servidora limpia, es decir sin ningún otro sistema operativo previamente instalado en el disco duro principal. Es en este sistema operativo donde se instalaron las diferentes herramientas de tecnologías de la información; para ello cabe resaltar que previamente se descargó el archivo de instalación desde el sitio oficial de Ubuntu.

En este procedimiento el asistente de instalación solicita una serie de datos que se deben diligenciar de acuerdo al idioma, ciudad donde se encuentre localizado el servidor etc.; una vez finalizada la instalación, se configuran los parámetros de red básico tales como dirección IP, mascara de subred, DNS, etc. Para obtener información detallada de la instalación ver el anexo 4 “Manual de Instalación y configuración de Ubuntu server 16.04 LTS”.

En segunda instancia se descargó e instaló el paquete LAMP Server desde los repositorios oficiales de Ubuntu server.

A través del gestor de paquetes TASKSEL, éste permite realizar una instalación sencilla, rápida y preconfigurada de las aplicaciones apache2, MySQL, php, perl y python. En la medida que el proceso de instalación avanzaba, la aplicación solicita asignar la contraseña de acceso del usuario ROOT a la base de datos MySQL. Para obtener más información detallada de la instalación ver el anexo 4 “Manual de Instalación LAMP Server”.

Seguidamente se descargó e instaló el paquete OpenLDAP y los módulos adicionales requeridos tales como MemberOf y AccessLog. En este proceso el asistente de instalación solicitó el nombre de dominio de la organización, el nombre de la organización, la contraseña de acceso del usuario administrador del servidor OpenLDAP, entre otros parámetros técnicos relevante para el correcto funcionamiento del directorio. Para obtener información detallada de la instalación ver el anexo 4 “Manual de Instalación de OpenLDAP en Ubuntu server 16.04 LTS”.

Luego se descargó e instaló el cliente phpLDAPadmin. Una vez instalado el cliente, se configuraron los parámetros requeridos para conectar al servidor OpenLDAP desde el cliente web. Para obtener información detallada de la instalación ver el anexo 4 “Manual de Instalación del cliente phpLDAPadmin”.

Una vez finalizada la anterior instalación descrita, se descargó e instaló la herramienta OwnCloud. Esta se encuentra en los repositorios oficiales de Ubuntu server como un paquete listo para desplegar. Una vez descargada, se creó una base de datos y un usuario con los privilegios de acceso a la base de dato en MySQL; por último, se configuraron los parámetros de conexión de ownCloud con la base de datos previamente creada y se asignó la contraseña de

acceso con privilegios de administrador requerida para configurar y personalizar la herramienta ownCloud. Para obtener información detallada de la instalación ver el anexo “Manual de Instalación de OwnCloud en Ubuntu server 16.04 LTS”.

Después se descargó e instaló la herramienta OCS Inventory NG desde su sitio oficial. Al igual que en la herramienta ownCloud, se debe crear una base de datos y un usuario con privilegios de acceso a la base de datos. Para finalizar la instalación se configuraron los parámetros de conexión de la base de datos con OCS Inventory NG. Para obtener más información detallada de la instalación ver el anexo 4 “Manual de Instalación de OCS Inventory NG”.

Por último, Se descargó el archivo de instalación de la UTM pfSense desde el sitio oficial.

Así como el sistema operativo Ubuntu Server, esta herramienta se debe instalar sobre una maquina limpia, es decir sin ningún sistema operativo en el disco duro principal. Una vez finalizada la instalación, para acceder por primera vez a la interfaz gráfica web, esta requiere que se le asignen las interfaces de red y su respectiva configuración de red básica con la cual va a operar la UTM. Para obtener más información detallada de la instalación ver el anexo 4 “Manual de Instalación de pfSense”.

3.3.2 Clientes.

Los servicios tecnológicos que operan bajo una arquitectura de software cliente-servidor tales como la autenticación de usuarios centralizada, gestión de activos tecnológicos y VPN emplean un software cliente específico para establecer conexión con su aplicación servidora.

Las estaciones de trabajo del FOMVAS en su totalidad, cuentan con el sistema operativo Windows en diferentes versiones, es decir Windows 7, 8 y 10, esto conlleva a descargar e instalar el software cliente para el sistema operativo Windows y para la arquitectura de software especifica bien sea 32 o 64 bits.

En primer lugar, se descargó e instaló el software cliente de la herramienta OCS Inventory NG denominado (Windows Agent) desde el sitio oficial. Este agente se encarga de recopilar los datos de los activos informáticos y automáticamente reportar el informe a la aplicación servidora; debido a la naturaleza de la aplicación, la herramienta se instaló en cada activo de cómputo de la infraestructura empresarial. Para obtener más información detallada de la instalación ver el anexo “Manual de Instalación Agente Ocs Inventory NG”.

Seguidamente se descargó e instaló la herramienta (OwnCloud desktop client) desde el sitio oficial; esta herramienta permite sincronizar carpetas locales en el sistema operativo windows con las carpetas del servicio de alojamiento centralizado de cada usuario.

Luego se descargó e instaló la herramienta pGina desde su sitio oficial; esta herramienta básicamente sirve como un puente entre el sistema operativo Windows y el servidor de directorio OpenLDAP, es decir, permite establecer una conexión entre los activos de cómputo del FOMVAS y el servidor OpenLDAP que facilita el proceso autenticación de usuario centralizada. Para obtener más información detallada de la instalación ver el anexo “Manual de Instalación de pGina en Windows”

Por último, se descargó e instaló la herramienta cliente (OpenVPN Connect) desde el sitio oficial. Esta herramienta de tecnología de la información es la que permite crear el canal VPN desde una red externa hacia la red de área local del FOMVAS, es de aclarar que esta herramienta solo debe ser instalada en el equipo de cómputo del personal capacitado que lo requiera, como es el caso del encargado de la parte de sistemas y empleados que laboren en campo, es decir en sitios diferentes al interior de las oficinas del FOMVAS.

3.5. Configuración

Luego que se finalizaron las actividades de instalación y configuración preliminar, empieza una de las partes más importantes en el marco del funcionamiento de los servicios tecnológicos.

En esta parte del proyecto es donde se configuran de manera personalizada las herramientas de tecnologías de la información teniendo como fundamento las necesidades diagnosticadas en el proyecto.

Es decir, se establecieron las categorías de URL que bloquearía el servicio de filtrado de contenido web, se establecieron las WhiteList, se gestionó el servidor de directorios LDAP, se configuró la integración entre OwnCloud y el servidor de directorios LDAP, Se configuraron las reglas de firewall particulares según las necesidades y políticas del FOMVAS, se configuraron los software cliente, para que tuvieran una conexión satisfactoria con su aplicación servidora, se mapearon las direcciones IP privadas y MAC para la asignación de manera estática del servicio DHCP Y por último se estableció el ancho de banda de navegación por grupos de usuarios, según las necesidades y políticas del FOMVAS.

NOTA: Para mayor información referente a la configuración avanzada de las herramientas de tecnologías de la información, ver los manuales en los anexos del informe.

3.6. Pruebas

Para esta actividad se creó un ambiente de prueba, con los activos informáticos de las oficinas de Archivo, Técnica, Sistemas, Jurídica y Recepción del FOMVAS. Todos los activos informáticos tienen una plataforma de hardware básica en su mayoría, es decir poseen un procesador Intel Celeron, Pentium o Intel Core i3 con 2GB o 4 GB de memoria RAM y una capacidad de almacenamiento de 300 GB o 500GB.

Cabe resaltar que estas oficinas fueron seleccionadas a partir de la experiencia del ingeniero a cargo de sistemas Bladimir Manjarres, especificando que estos activos informáticos, no afectarían de forma general, la prestación de los servicios del FOMVAS en caso de que se presentara alguna falla en la implementación de los servicios de tecnologías de la información.

A los activos informáticos seleccionados para realizar el conjunto de buenas prácticas, se les instalaron todos los softwares clientes necesarios, teniendo en cuenta que no se realizará ninguna modificación a la configuración de las cuentas de usuario definidas en el equipo. Esto se

fundamentó en la razón, de que, si el servicio de autenticación de usuario centralizada fallara, se pudieran volver a utilizar los equipos a través del usuario de cuenta local existente, sin ningún problema.

Las pruebas técnicas y de funcionamiento en el FOMVAS se realizaron de manera gradual, es decir, la primera etapa comprendió un total de 10 días con los 4 activos informáticos de Archivo, división técnica y Sistemas; en ese lapso no ocurrieron complicaciones, partiendo de ese hecho, se fueron adicionando activos informáticos a la prueba. La siguiente etapa comprendió un total de 20 días, en esta se adicionaron las oficinas administrativa y gerencia sumando un total de 15 activos informáticos. Durante el tiempo de la prueba se realizó una bitácora que le permitiera a la oficina de informática hacer un registro de los eventos, incidentes que pudieran afectar la prestación de los servicios, o los problemas identificados durante este periodo.

Transcurrido el tiempo de prueba, se realizó una reunión con el responsable de la oficina de informática y se evaluaron las condiciones de la implementación de los servicios, a partir de la cual se pudo concluir que los servicios tecnológicos estaban operando de la manera esperada y que se podía implementar en todas las oficinas sin ningún problema para que los usuarios hicieran uso de los mismos.

3.8. Despliegue

Validados los servicios, se inicia el proceso de masificación en la implementación de los mismos, realizando las instalaciones de los softwares clientes requeridos y las configuraciones necesarias para facilitar el acceso a todos los servicios implementados.

3.7. Transición de los servicios tecnológicos

Esta actividad fue relevante a la hora de adoptar los nuevos servicios de tecnologías de la información ya que en el FOMVAS contaba con dos sistemas de información en producción. Un software contable denominado (Helisa) y el software avanzado de valorización (SAV). Es de

destacar que ambas aplicaciones son de escritorio, pero con una particularidad en especial, ambas funcionan con una base de datos que está compartida en la red de red local a través de la compartición de archivos de Windows. Partiendo de lo anterior, se tuvo que reconfigurar el direccionamiento IP de los sistemas de información y la ruta al directorio de datos en red. Esto se realizó debido a que la red corporativa local se le asignó un nuevo segmento de direccionamiento IP a través del servicio de DHCP estático.

También es de resaltar que la antigua forma en la que se autenticaban los usuarios frente a el sistema operativo Windows no se deshabilitó de manera definitiva, es decir los servidores públicos del FOMVAS tenían la posibilidad de autenticarse a través de las cuentas de usuarios locales o a través del nuevo método de autenticación (autenticación de usuarios centralizada).

3.8. Operación

Una vez se superaron todas las actividades de migración y pruebas realizadas, en una reunión adelantada con el jefe de la oficina de informática, se determinó que la etapa de transición se había desarrollado de manera exitosa y se abría paso a las actividades de operación o de producción de los servicios implementados.

Para esta etapa, se acordó con el jefe de la oficina informática, un proceso de seguimiento a la infraestructura y acompañamiento semanal a la prestación de los servicios implementados, a través de los cuales se hizo seguimiento permanente

4. Fase de Capacitación de usuarios

A medida que se llevaban a cabo las distintas implementaciones de los servicios tecnológicos en el FOMVAS, paralelamente también se iban sensibilizando a los empleados sobre los objetivos y alcances del proyecto. Para llevar a cabo dicha actividad, se utilizaron diferentes medios, los cuales se detallan en las diferentes estrategias que se ejecutaron en la entidad encaminadas al uso y apropiación de dichas herramientas.

4.1. Folletos Informativos

A lo largo del proyecto se entregaron diferentes folletos informativos a cada uno de los servidores públicos que laboran en la organización; que tenían como propósito permitirles a los usuarios reconocer el objetivo del proyecto y el impacto sobre la organización en términos de seguridad de la información.

En los folletos se mostraron varias preguntas con relación a la información que posee una empresa, invitándolos a reflexionar sobre las mismas, con el objetivo que el servidor público tuviera una perspectiva sobre que se trataba dicho folleto y hacia donde se dirigía con la información presentada.

Se logró sensibilizar a los servidores públicos sobre el proyecto, es decir, sobre el valor e importancia que tiene la información en una entidad y en particular en el FOMVAS, así mismo se logró sensibilizar a los empleados en la necesidad de proteger la información. Por otra parte, también se logró difundir contenido acerca de cómo se pretendía mitigar los riesgos a los cuales se enfrentaba la información, de igual forma se plasmaron todos los servicios tecnológicos que permitirían apoyar la seguridad de la información en el FOMVAS.

4.2. Capacitación Grupal

Para llevar a cabo la capacitación, con el apoyo del jefe de la oficina de informática, se dividió el total de empleados del FOMVAS en tres grupos de igual número de servidores

públicos, de tal manera que las reuniones se desarrollaran en grupos pequeños, que facilitaran las actividades de formación. En las capacitaciones se explicó nuevamente el objetivo del proyecto y se otorgó espacios a los empleados para aclarar dudas e inquietudes alrededor del mismo. Con cada uno de los grupos se siguió el mismo procedimiento.

Posteriormente se procedió a explicar el uso de los servicios con los que el usuario interactuaría en su día a día, atendiendo a las preguntas que iban surgiendo a medida que se orientaba la capacitación, de este modo hubo interacción entre ambas partes. Al final se llevaron a cabo todas las reuniones y actividades que dieron lugar al uso y apropiación de los servicios tecnológicos por partes de los empleados.

4.3. Acompañamiento personalizado

Las capacitaciones personalizadas permitieron fortalecer las actividades de uso y apropiación de las herramientas tecnológicas propuestas, aportando a las personas que tuvieron dificultades, diferentes actividades de formación para mejorar sus competencias sobre las herramientas implementadas. Estas capacitaciones se desarrollaron con cada uno de los servidores públicos y se hizo énfasis en aquellos que tuvieron dificultades con el uso de las mismas. Se daba por finalizado el proceso de acompañamiento personalizado, cuando el servidor público consideraba que tenía dominio sobre los servicios implementados.

5. Conclusiones

A partir del desarrollo del proyecto se puede concluir lo siguiente:

- ✓ Mejoramiento en las condiciones para el control de acceso de los equipos de cómputo adscritos al FOMVAS, permitiendo que cualquier empleado pueda tener acceso a los equipos de la entidad utilizando una cuenta de usuario debidamente creada y validada a través del servicio de autenticación centralizado. El control de usuarios impide el acceso a los equipos de cómputo en calidad de administradores, mejorando las condiciones de seguridad en cuanto a las condiciones para la instalación y configuración de aplicaciones en cada uno de los equipos de cómputo de la entidad.
- ✓ Fortalecimiento en el control de acceso a la red LAN de FOMVAS, permitiendo así la automatización de la configuración de red de los equipos de cómputo, a través del servicio DHCP; para obtener privilegios de acceso a la red, el equipo debe estar registrado en el servidor de gestión de DHCP estático, de lo contrario el servicio DHCP, impediría que cualquier usuario que no tenga conocimiento del segmento de red, se pueda conectar a la red LAN desde un equipo ajeno a la organización.
- ✓ Fortalecimiento en la gestión de los activos de tecnologías, apoyando las labores manuales de levantamiento y seguimiento al inventario de equipos de cómputo de la entidad, a través del sistema de información OCS Inventory NG, así como de la utilización de agentes en los equipos clientes. El seguimiento, favorece los procesos de gestión de cambios y de identificación de la utilización de los equipos de cómputo en la entidad.
- ✓ Ampliación de las capacidades institucionales en términos del acceso a los recursos de información de la entidad, apoyados en la utilización de una red privada virtual, controlada por el sistema de autenticación centralizada de la entidad.
- ✓ Fortalecimiento de la gestión del acceso y uso del servicio de internet, apoyadas en la definición de grupos y políticas de calidad de servicio, a través del servicio QoS de la herramienta PfSense.

- ✓ Mejoramiento de los procesos de almacenamiento de la información, centralización y compartición de documentos, en atención a los perfiles de usuarios definidos y específicamente autorizados a través del servicio de autenticación centralizada.
- ✓ Aumento en las condiciones de seguridad de la información, en términos de la confidencialidad y disponibilidad de la información de la entidad.

6. Recomendaciones

- ✓ Aumentar el personal con competencias técnicas o tecnológicas en la oficina de informática de la entidad que aporte a los procesos de seguimiento, soporte a usuario y acompañamiento permanente al proceso de gestión de los servicios adoptados.
- ✓ Aumentar la inversión financiera en tecnologías de información, priorizando las actividades de fortalecimiento de la plataforma tecnológica, tanto en términos de hardware, como de licenciamiento de software, así como para la implementación de acciones de redundancia en la prestación de los servicios y de contingencia.
- ✓ Implementar acciones de capacitación permanente que favorezcan el proceso de apropiación de los servicios tecnológicos.
- ✓ Implementar acciones de evaluación de los servicios que propendan por el mejoramiento de los mismos.

Referencias Bibliográficas

Advisera (s.f.). *¿Qué es norma ISO 27001?: Una introducción simple a los aspectos básicos.* Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001/.

Apache Directory (s.f.). *LDAP and Kerberos server written in Java.* Recuperado de https://directory.apache.org/apacheds/.

Aranda Software (s.f). Aranda CMDB. Recuperado de https://arandasoft.com/wp-content/uploads/2019/07/datasheet-cmdb-2019-oficial.pdf

Ardila, O. (2015). *Platzi: ¿Qué es y cómo usar un VPN?* Recuperado de https://platzi.com/blog/como-usar-una-vpn/.

Bouras, C. et al (2014). *Policy recommendations for public administrators on free and open source software usage.* Recuperado de https://www-sciencedirect-com.ezproxy.cecar.edu.co:2443/science/article/pii/S0736585313000361#.

CISCO (s.f). *What Is a Firewall?* Recuperado de https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

Endian (s.f.). *Endian Firewall Community.* Recuperado de https://www.endian.com/community/features/.

Flores, G. (2014). *El Open Source Empresarial: una alternativa probada en TI. Recuperado de* https://mundocontact.com/el-open-source-empresarial-una-alternativa-probada-en-ti/.

FOMVAS (2018). *Misión y visión.* Recuperado de http://fomvassincelejo.gov.co/entidad/mision-y-vision

FOMVAS (2018). *Plan estratégico de tecnologías de información*. Recuperado de http://fondorotatoriosincelejo.micolombiadigital.gov.co/sites/fondorotatoriosincelejo/content/files/000174/8659_11peti.pdf.

Fortinet (s.f.). *Seguridad de red*. Recuperado de https://www.fortinet.com/.

García, D. (2013). The law 11/2007, of electronic access of the citizens to the public services and the use of the free software in the public administration. *Revista General De Información y Documentación, 23(1), 27-42*. recuperado de https://search-proquest.com.ezproxy.cecar.edu.co:2443/docview/1432302105?accountid=34487.

International Business Machines (s.f.) *IBM: Identificación y autenticación.* Recuperado de: https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.0.1/com.ibm.mq.csqzas.doc/

sy10240_.htm.

Institut Puig Castellar (s.f.). *Servicio DHCP*. Recuperado de https://elpuig.xeill.net/Members/vcarceler/c1/didactica/apuntes/ud4/na7.

IPCorp. (s.f.) *IPCorp: Autenticación LDAP* Recuperado de http://www.ipcop.org/2.0.0/es/admin/html/proxy-auth-ldap.html.

Kaspersky (s.f.). *¿Qué es un filtro web?* Recuperado de https://latam.kaspersky.com/resource-center/definitions/web-filter.

Microsoft (2017). *Active Directory Domain Services Overview*. Recuperado de https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

Ministerio de las Tecnología de la Información y Comunicación (2016) *Documento actualizado modelo de gestión IT4+* Recuperado de http://www.mintic.gov.co/arquitecturati/630/propertyvalues-8170_documento_pdf.pdf .

NextCloud (s.f.). *You should control your data.* Recuperado de https://nextcloud.com/.

OCS Inventory NG (s.f,). *About OCS Inventory*. Recuperado de https://www.ocsinventory-ng.org/en/.

Owncloud (s.f.). *What is this ownCloud thing?* Recuperado de https://owncloud.org/faq/#whatis.

PfSense (s.f.). *Take A Tour of pfSense.* Recuperado de https://www.pfsense.org/about-pfsense/.

PGINA (s.f.). *Windows Authentication without Active Directory*. Recuperado de http://pgina.org/.

Pino (2013) *UNAL: Análisis tecnológico, herramienta de toma de decisiones* Recuperado de http://www.ing.unal.edu.co/eventos/gestec_innovacion/img/presentaciones/auditorio1/ponencias/3_pinojesus.pdf.

PMG (2018). *PMG SGSI: Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad*. Recuperado de https://www.pmgssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/.

SomeBooks (2013). *¿Qué es OpenLDAP?* Recuperado de http://somebooks.es/12-5-que-es-openldap/.

Techopedia (s.f.). *Port Number.* Recuperado de https://www.techopedia.com/definition/15702/port-number.

Techopedia (s.f.). *Techopedia: What Is File Hosting Service?* Recuperado de: www.techopedia.com/definition/25310/file-hosting-service .

Tecnopedia (s.f). *Quality of Service*. Recuperado de: https://www.techopedia.com/definition/9049/quality-of-service.

Xataka (2018). *¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene? Recuperado de:* https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene