https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174

Vol. 4, Núm. 2. abril-junio 2026, págs. 79 - 98

Implementación de un servidor de impresión bajo un enfoque de seguridad y sostenibilidad tecnológica

Implementation of a print server under a security and technological sustainability approach

Alfonso Gutiérrez Molina

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

amolina@unam.mx

ORCID: 0000-0002-7467-0651

Información del reporte:

Para citar este reporte técnico:

Gutiérrez Molina, A. (2026). Implementación de un servidor de impresión bajo un enfoque de seguridad y sostenibilidad tecnológica. *Cuadernos Técnicos Universitarios de la DGTIC, 4* (2), páginas (79 - 98). https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174

Resumen

Debido a la necesidad de contar con documentos físicos en el ambiente académico y laboral, el servicio de impresión es de gran importancia en el día a día; sin embargo, éste puede presentar problemas de desconexión y de acceso no autorizado, por lo que se decidió implementar un servidor de impresión regulado para solucionar dichas situaciones.

Esta implementación incluyó una actualización de *hardware*, así como el mantenimiento preventivo de un equipo reutilizado con la finalidad de fungir como servidor de impresión. Asimismo, se realizó la instalación del sistema operativo, una *suite* ofimática y herramientas de seguridad, que incluyen la instalación y configuración de un *firewall* y listas de control de acceso para restringir el uso de equipos no autorizados. La conexión de los dispositivos cliente al servidor se realizó mediante el uso de rutas *Universal Naming Convention* bajo el esquema cliente-servidor. De esta manera, se incorporaron mecanismos de autenticación y segmentación de red para fortalecer la seguridad.

Los resultados evidenciaron una reducción en los reportes o solicitudes relacionadas con fallas de impresión y reconfiguración de dispositivos, lo que permitió optimizar la carga operativa del área de Soporte Técnico. De igual manera, la reutilización de equipos de cómputo programados para su desincorporación contribuyó a la

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 80 - 98

disminución de residuos electrónicos, promoviendo así la sostenibilidad tecnológica. Esta estrategia demostró que la centralización de servicios, junto con el uso de *software* libre y aplicaciones de controles de seguridad, permite incrementar la eficiencia operativa, además de fortalecer la seguridad de la información y fomentar prácticas sostenibles dentro de la dependencia.

Palabras clave: Gestión de TI, seguridad de la información, servidor de impresión, *software* libre, sostenibilidad tecnológica.

Abstract

Due to the need for physical documents in academic and professional environments, printing services are of great importance on a daily basis; however, they often present problems with disconnections and unauthorized access. Therefore, it was decided to implement a regulated print server to address these issues.

This implementation included a hardware upgrade, as well as preventive maintenance of a repurposed computer to serve as the print server. The installation of the operating system, an office suite, and security tools was also carried out, including the installation and configuration of a firewall and access control lists to restrict the use of unauthorized equipment. Client devices were connected to the server using Universal Naming Convention paths under a client-server architecture. This incorporated authentication mechanisms and network segmentation to strengthen security.

The results showed a reduction in reports or requests related to printing failures and device reconfiguration, which optimized the workload of the Technical Support area. Similarly, the reuse of computers that were going to be discarded contributed to a decrease in electronic waste, thus promoting technological sustainability. This strategy demonstrated that centralizing services, using open-source software, and implementing security controls increases operational efficiency, strengthens information security, and fosters sustainable practices within the department.

Keywords: *IT management, information security, print server, open-source software, technological sustainability.*

1. INTRODUCCIÓN

En la actualidad, el uso de documentos digitales en ambientes laborales, académicos y personales se ha convertido en una práctica fundamental, ya que permite optimizar el manejo de la información, mejorar la eficiencia en procesos administrativos, colaborar entre varias personas a la vez y almacenar los datos de forma sencilla y segura. Por consiguiente, logra reducir costos, ahorrar tiempo y promover formas de trabajo ágil y sostenible, además de que facilita el trabajo remoto. A pesar de lo anterior, hoy en día existen situaciones específicas en las que el uso de un documento físico sigue siendo relevante, ya sea por razones legales, de seguridad, de accesibilidad, etc.

En algunas áreas de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), es imprescindible imprimir documentos; por ello, es primordial que el servicio de impresión siga operando de manera constante, funcional y eficaz al momento de ser necesario. En ocasiones, dicho servicio presentaba problemas como la pérdida de conexión entre el equipo de cómputo y la impresora,

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 81 - 98

el acceso de usuarios no autorizados y la dificultad para configurar una impresora predeterminada; esto podía derivar en problemas de seguridad, vulnerabilidades y retrasos en el servicio.

Debido a las situaciones expuestas con anterioridad, en el año 2025 se decidió implementar un servidor de impresión con el objetivo de brindar un servicio continuo, estable, seguro y disponible sólo para el personal autorizado.

2. DESARROLLO TÉCNICO

Un servidor de impresión es un equipo diseñado para que los usuarios puedan tener acceso a servicios de impresión. Para ello, los usuarios se conectan de manera remota por medio de una cuenta y contraseña establecidos, lo que permite que tengan acceso al servicio de impresión. Además, la utilización de credenciales de acceso permite gestionar el uso por medio de listas administradas a través de un *firewall* o a través de las herramientas del mismo sistema operativo. Lo anterior trae consigo beneficios significativos, tales como la disminución en el consumo de tóner, papel y energía eléctrica. Esto propicia la optimización de recursos materiales y la reducción de costos; la eliminación de equipos de impresión personales, ahorro de espacio y la disminución de solicitudes de servicio de soporte correctivo, lo que permite que el trabajo se centre en el mantenimiento preventivo de otras áreas (Albarracín *et al*., 2021).

El servidor de impresión que se propuso como solución está compuesto por una computadora de escritorio, una impresora láser monocromática, un *firewall*, *software* ofimático y un antivirus. Las características específicas de los componentes que conforman el servidor se presentan en el Anexo A del reporte.

Aplicaciones de uso para el servidor de impresión:

Se consideró la posibilidad de que fuera necesaria la modificación ocasional de archivos o documentos directamente en el servidor de impresión, particularmente en situaciones que requieran atención inmediata o por necesidades operativas del área. En este sentido, se contempló la instalación de un *software* libre de ofimática básico que permita la creación, modificación y revisión de documentos sin comprometer la función principal del equipo. Adicionalmente, el equipo debe contar con mecanismos de seguridad que garanticen la integridad, disponibilidad y confidencialidad del servicio de impresión, por lo cual, se consideró necesaria la implementación de un *firewall* debidamente configurado, así como la instalación de un antivirus. Las herramientas elegidas para este fin fueron LibreOffice (ofimática), ZoneAlarm (*firewall*) y Avira (antivirus). El proceso de selección basado en pruebas de uso se explica a detalle en el Anexo B del reporte.

2.1 METODOLOGÍA

Debido a las características técnicas del equipo de cómputo de escritorio y con el propósito de optimizar su rendimiento, primero se llevó a cabo un proceso integral de mantenimiento preventivo y actualización de *hardware y software*. El mantenimiento preventivo en sistemas informáticos constituye una práctica fundamental para prolongar la vida útil de los equipos, reducir fallas y mejorar la eficiencia operativa (Vermaat *et al*., 2018).

En primera instancia, se realizó una limpieza interna y externa del equipo, lo que incluyó la remoción de polvo en componentes críticos, limpieza de ventiladores y sustitución de la pasta térmica en el disipador

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 82 - 98

de calor del CPU, con el fin de mejorar la disipación de calor y garantizar un funcionamiento térmico adecuado. Esto evitó el sobrecalentamiento, uno de los principales factores que afectan el desempeño y la estabilidad de los sistemas de cómputo (Andrews, 2019).

Como siguiente paso, se amplió la memoria RAM de 8 GB a 16 GB, lo que potenció la capacidad de procesamiento y el desempeño en multitareas y mejoró la eficacia del sistema operativo (Patterson & Hennessy, 2017). Posteriormente, se reemplazó el disco duro mecánico (HDD) de 1 TB por una unidad de estado sólido (SSD) de 500 GB para optimizar la velocidad de lectura y escritura del sistema.

Finalmente, se instaló el sistema operativo Windows 10 Pro de 64 bits, junto con el paquete de herramientas ofimáticas y *software* de seguridad, específicamente ZoneAlarm y Avira antivirus, con el objetivo de garantizar un entorno de trabajo seguro y eficiente. La implementación de soluciones de seguridad informática es esencial para la protección de datos y la prevención de amenazas cibernéticas (Stalling & Brown, 2018).

Instalación de LibreOffice

Después de haber descargado el instalador de LibreOffice, se procedió con la instalación correspondiente mediante el asistente. Durante el proceso, se recomienda seleccionar la configuración predeterminada; de esta manera, se asegura la instalación completa de los componentes principales de la *suite* ofimática, tales como procesador de texto, hoja de cálculo, presentaciones y manejador de bases de datos. Como siguiente paso, se verificó la correcta integración con el sistema operativo, comprobando la creación de accesos directos y la asociación de formatos de archivos compatibles.

Instalación de ZoneAlarm

Una vez descargado el *software* ZoneAlarm, se procedió a la instalación mediante el asistente correspondiente, verificando que la integración con el sistema operativo y la activación de los módulos de protección en tiempo real fuera correcta.

Posteriormente, se realizó la configuración inicial del *firewall*, ajustando los niveles de seguridad y definiendo reglas específicas para el filtrado de tráfico. La configuración correcta de las reglas en un *firewall* permite reducir vulnerabilidades y ataques en entornos organizacionales (Whitman & Mattord, 2021).

Como parte del proceso, se estableció la lista de control de acceso (ACL), especificando los equipos autorizados para hacer uso del servicio de impresión dentro de la red local. Las ACL permiten aplicar políticas de seguridad basadas en direccionamiento IP, puertos y protocolos, garantizando que únicamente los dispositivos previamente enlistados puedan acceder a los recursos compartidos dentro de la red local, fortaleciendo así la confidencialidad, integridad y disponibilidad de los recursos tecnológicos (Stalling & Brown, 2022).

Estas acciones se alinean con los controles establecidos en la ISO/IEC 27001:2022, norma que establece la necesidad de implementar controles técnicos apropiados para gestionar riesgos de seguridad de la información dentro del Sistema de Gestión de Seguridad de la Información (SGSI) (International Organization for Standardization, 2022).

Por consiguiente, la instalación y correcta configuración del *firewall* protegerá al sistema de accesos no autorizados, además de que garantizará un uso controlado y seguro de los servicios de la red local.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 83 - 98

Instalación de Avira

Se procedió con la descarga del *software* Avira antivirus desde su sitio oficial, verificando la compatibilidad con el sistema operativo del servidor de impresión; después, se ejecutó el archivo de instalación mediante el asistente correspondiente, seleccionando la configuración predeterminada para garantizar la activación de los módulos de protección.

Al terminar la instalación, se verificó la correcta actualización de las bases de datos de firmas de virus y se comprobó la activación de la protección del sistema en tiempo real para asegurar la detección y prevención de amenazas informáticas. Este *software* permite fortalecer la seguridad del equipo, reducir riesgos de infección por *malware* y garantizar la integridad de la información que se encuentra en el servidor.

Configuración de la impresora láser B/N

Como primer paso, se realizó la configuración y conexión directa de la impresora al servidor de impresión, utilizando la interfaz USB. Para garantizar el correcto funcionamiento, es indispensable contar con los controladores (*drivers*) actualizados del fabricante, ya que los controladores actúan como intermediarios entre el sistema operativo y la impresora, asegurando la compatibilidad y el acceso a todas las funciones de la impresora (Silberschatz *et al*., 2022).

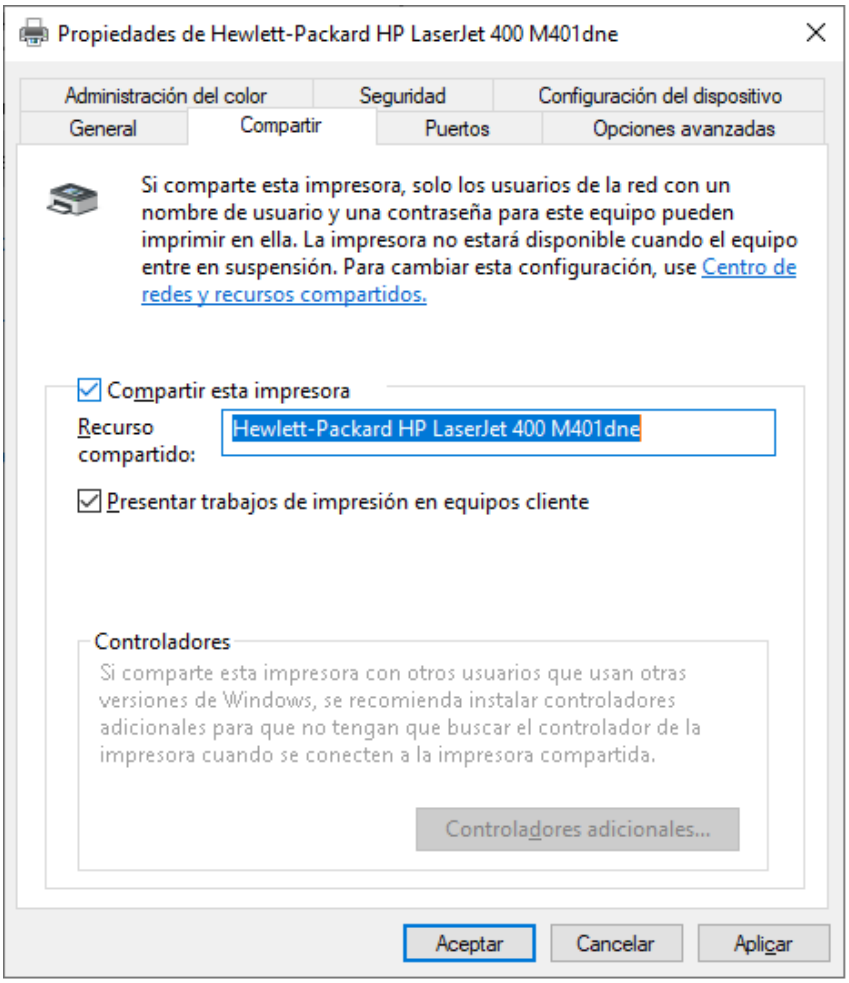
A pesar de que el sistema operativo Windows 10 Pro cuenta con mecanismos de detección automática de *hardware* (*Plug and Play*) que permiten reconocer e instalar dispositivos de manera básica, es recomendable asegurarse que la instalación de los controladores sean los específicos de la impresora para optimizar el rendimiento y evitar conflictos de compatibilidad. Como siguiente paso, se realizaron las configuraciones necesarias para compartir la impresora en red, habilitando las opciones de uso compartido y definiendo los permisos de acceso para los usuarios autorizados. Compartir recursos dentro de una red local es una práctica común en entornos organizacionales, pues permite optimizar la infraestructura, reducir costos y mejorar la eficiencia operativa (Kurose & Ross, 2021).

En la Figura 1 se puede observar la configuración de la impresora como un recurso compartido dentro de la red local.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 84 - 98

Figura 1

Configuración de la impresora como recurso compartido



Configuración de las listas de acceso en ZoneAlarm

Después de haber instalado ZoneAlarm, se procedió a la configuración de las listas de control de acceso (ACL), con el objetivo de regular el uso del servicio de impresión compartido en la red local. Para ello, se creó una lista conformada por las direcciones IP de los equipos autorizados. Las ACL son un mecanismo básico en la administración de redes, pues permiten filtrar el tráfico con base en parámetros como dirección IP, protocolo y puerto, proporcionando un control granular sobre servicios expuestos (Kurose & Ross, 2021).

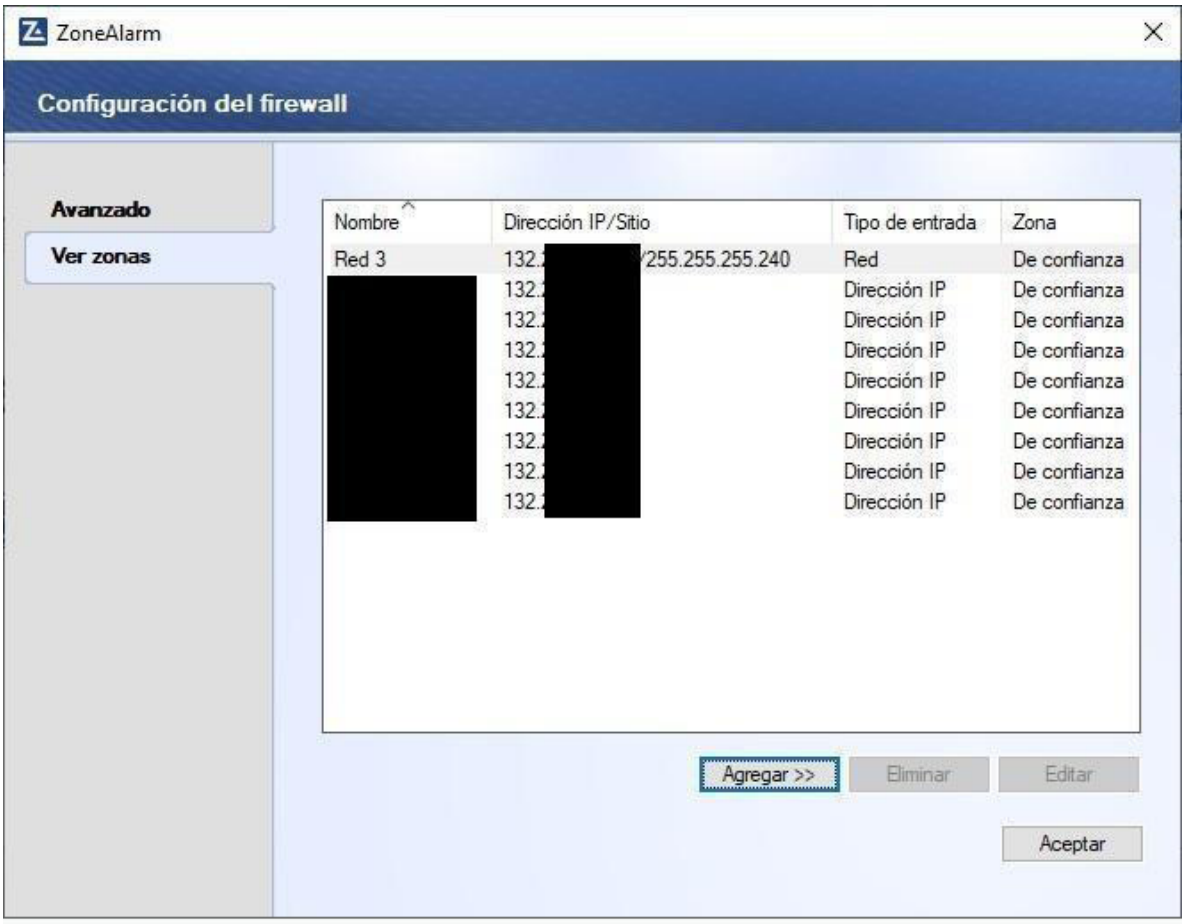
De esta manera, un *firewall* personal como Zone Alarm permite implementar políticas a nivel *host*, reforzando la protección perimetral y complementando otros controles de seguridad en la infraestructura de la red local (Stalling & Brown, 2022).

En la Figura 2 se puede observar la Lista de Control de Acceso (ACL).

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 85 - 98

Figura 2

Lista de Control de Acceso (ACL) de equipos autorizados para imprimir



Esta lista está conformada por la dirección IP de los equipos autorizados a imprimir.

Conexión y configuración de los equipos autorizados al servidor de impresión

Una vez configurada y compartida la impresora, y tras haber definido previamente la lista de acceso a la zona de confianza en el *firewall*, se procedió a la conexión de los equipos autorizados al servidor de impresión. La vinculación se realizó mediante el uso de rutas UNC (Universal Naming Convention), empleando la sintaxis *\\NombreDelHost\NombreImpresora*, lo que permite localizar y acceder a recursos compartidos dentro de una red local basada en arquitectura cliente-servidor, ya que este esquema facilita la administración centralizada de dispositivos y optimiza la adecuada gestión de recursos.

Es recomendable que el servidor de impresión, como los equipos cliente, cuenten con credenciales de usuario compatibles o una cuenta en común para garantizar un proceso de autenticación adecuado y evitar conflictos de permisos. Es importante mencionar que la autenticación es un mecanismo esencial de control de acceso lógico, pues permite verificar la identidad de los usuarios antes de otorgar acceso a los recursos compartidos en la red local (Silberschatz *et al*., 2022).

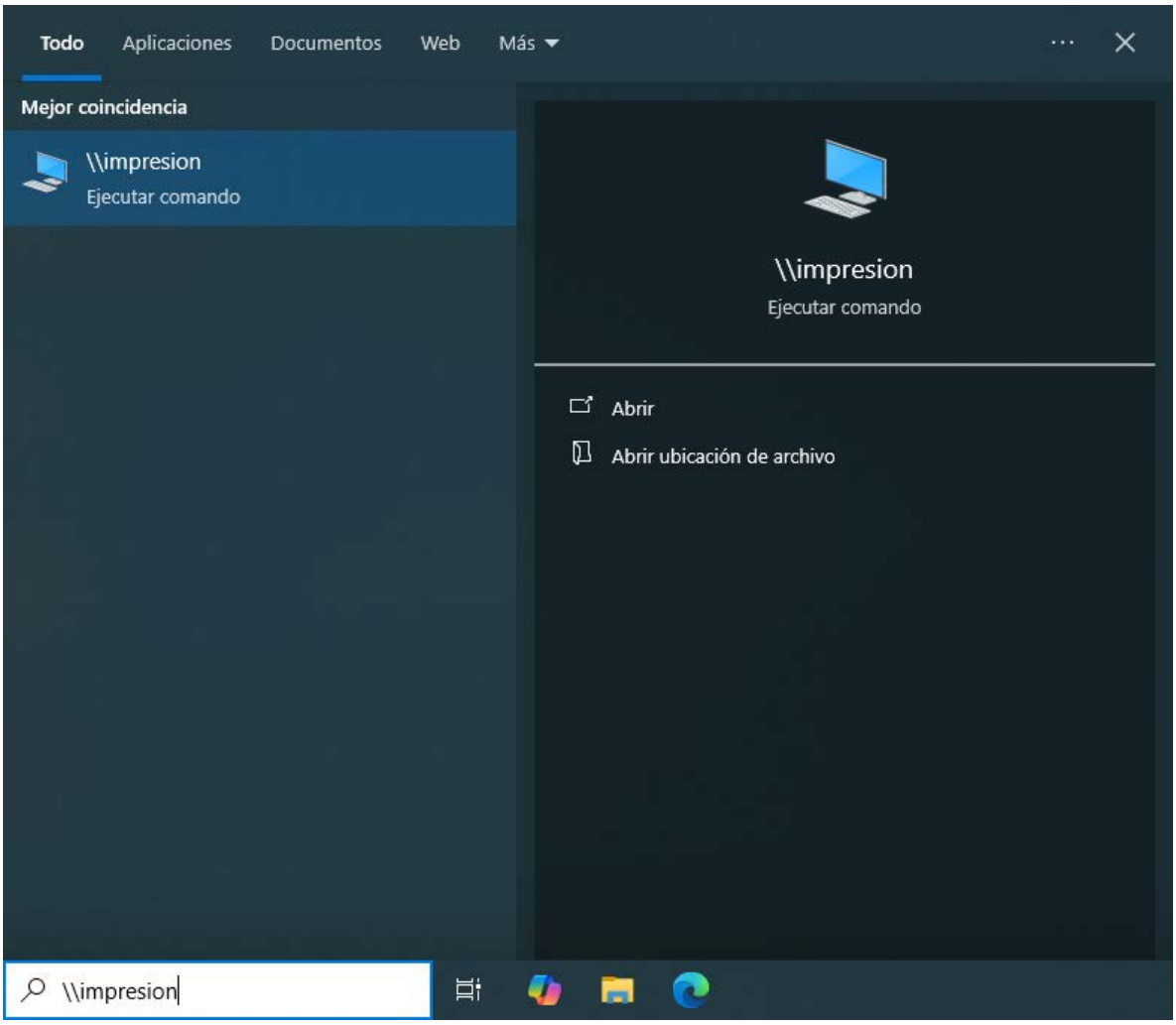
https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 86 - 98

Por consiguiente, la conexión y configuración de los equipos autorizados responde a una necesidad operativa fundamentada en las buenas prácticas técnicas y normativas de la administración de redes y seguridad de la información.

En la Figura 3, se muestra la conexión del equipo cliente con el servidor.

Figura 3

Conexión cliente-servidor por medio de rutas UNC

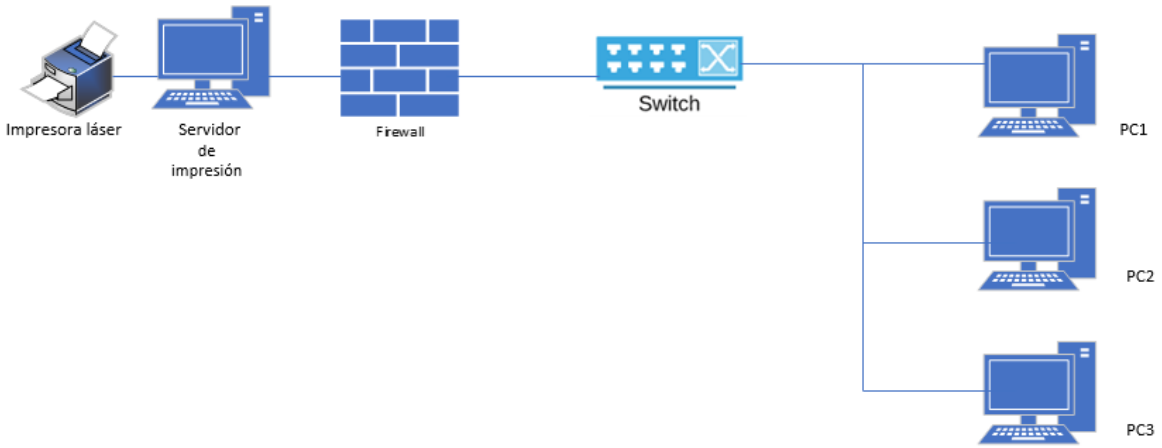


En la Figura 4, se puede apreciar el esquema básico del servidor de impresión.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 87 - 98

Figura 4

Diagrama básico de cliente-servidor



3. RESULTADOS

En el año 2023, se atendieron 74 solicitudes; en el año 2024, se atendieron 77 solicitudes; y en el año 2025, se atendieron 44 solicitudes. Los rubros de estos reportes fueron: configurar impresora, impresora no responde/lenta, usuario no puede imprimir, cambio de tóner, atasco de papel, mantenimiento preventivo/correctivo. A continuación, en las Tablas 1, 2, 3 y 4 y en las Figuras 5, 6, 7 y 8, se presentan los datos referentes a dichos servicios:

Tabla 1

Servicios atendidos en el año 2023

Tipo de servicios	No. de servicios
Configurar impresora	15
Impresora no responde/lenta	15
Usuario no puede imprimir	23
Cambio de tóner	5
Atasco de papel	11
Mantenimiento preventivo/correctivo	5
Total	74

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 88 - 98

Figura 5

Gráfico por rubro atendido en el año 2023

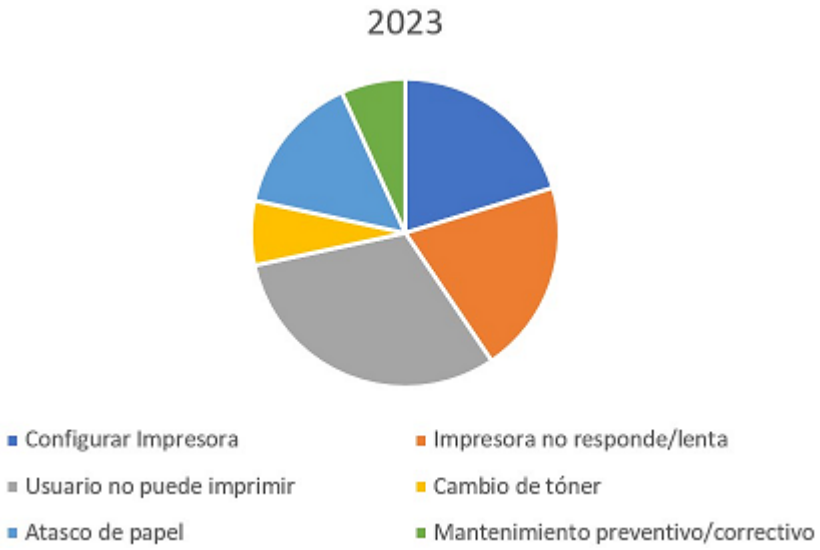


Tabla 2

Servicios atendidos en el año 2024

Tipo de servicios	No. de servicios
Configurar impresora	19
Impresora no responde/lenta	18
Usuario no puede imprimir	25
Cambio de tóner	4
Atasco de papel	8
Mantenimiento preventivo/correctivo	3
Total	77

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 89 - 98

Figura 6

Gráfico por rubro atendido en el año 2024

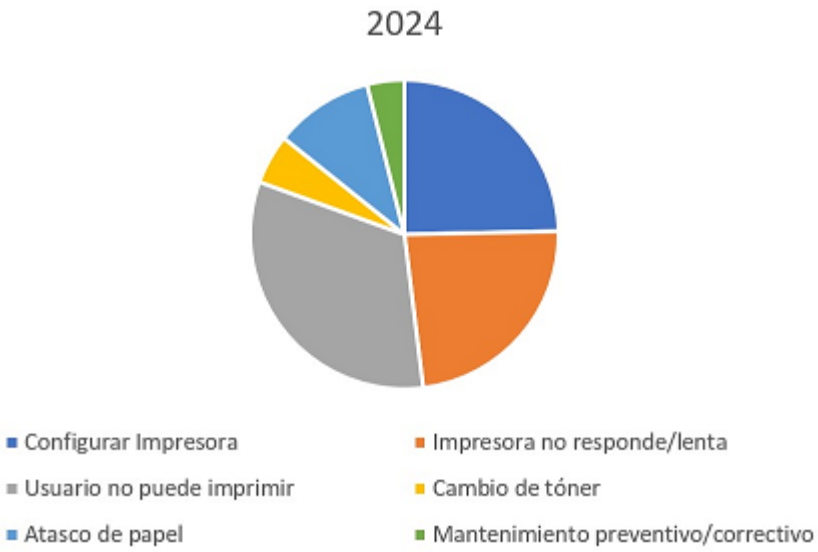


Tabla 3

Servicios atendidos en el año 2025

Tipo de servicios	No. de servicios
Configurar impresora	8
Impresora no responde/lenta	9
Usuario no puede imprimir	10
Cambio de tóner	5
Atasco de papel	6
Mantenimiento preventivo/correctivo	6
Total	44

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 90 - 98

Figura 7

Gráfico por rubro atendido en el año 2025

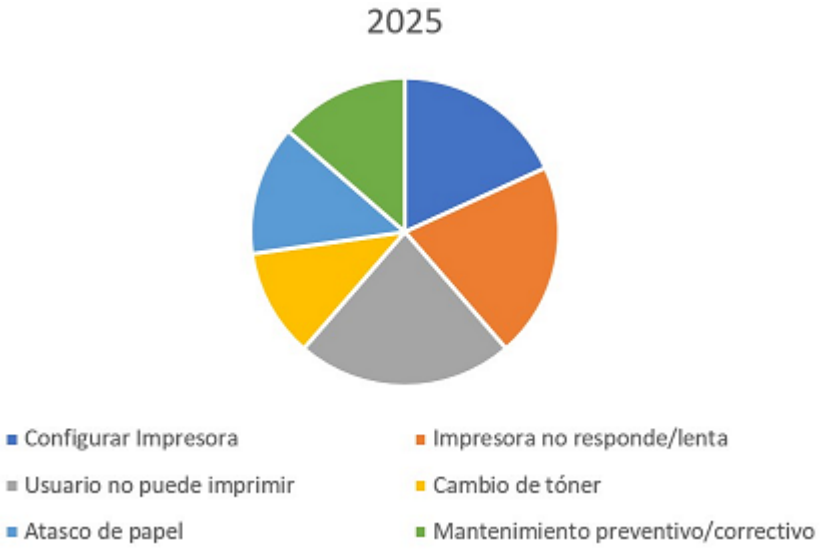


Tabla 4

Servicios atendidos del 2023 al 2025

Año	No. de servicios
2023	74
2024	77
2025	44

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 91 - 98

Figura 8

Gráfico de los servicios totales del 2023 al 2025

Con base en la información presentada en las gráficas y tablas que se mostraron, se puede observar la distribución y número de reportes atendidos correspondientes a los servicios de impresión. Este análisis cuantitativo permite identificar cuáles son las incidencias más recurrentes referentes a los servicios de soporte técnico solicitados para impresoras.

Los datos reflejan que la categoría o tipo de servicio solicitado con mayor frecuencia corresponde a la falla reportada por el usuario como "Usuario no puede imprimir", lo que sugiere posibles problemas de pérdida de conexión entre la computadora y la impresora conectada a la red local, deficiencias en la configuración de la red, errores relacionados a los controladores (*drivers*), permisos, etc. Tras la implementación del servidor de impresión, se logró reducir en gran medida los reportes referentes a impresoras.

Por otro lado, la configuración de direcciones IP en impresoras evidencia la necesidad de una administración adecuada de la red, especialmente en entornos donde se utiliza el direccionamiento IP estático, pues una planificación eficiente de este tipo de esquema puede contribuir a disminuir conflictos y desconexiones.

Por último, los servicios de soporte técnico referente al mantenimiento preventivo demuestran la importancia de estas acciones, ya que están orientadas a prolongar la vida útil de las impresoras y, por consiguiente, a la reducción de las fallas referentes a los mantenimientos correctivos.

4. CONCLUSIONES

La implementación de un servidor de impresión permitió garantizar la continuidad del servicio, evitando interrupciones en los procesos administrativos y operativos. Como resultado, se redujo de manera significativa el número de solicitudes de soporte técnico relacionados a la reconfiguración de impresoras,

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 92 - 98

lo que ha permitido que los tiempos de atención sean más breves y también que se liberen recursos del área de Infraestructura y Soporte Técnico para atender otras incidencias prioritarias.

Esta estrategia ha fortalecido la seguridad de las impresoras al centralizar la administración y aplicar listas de control de acceso (ACL) adecuados, de manera conjunta. Se ha promovido el uso de *software* libre para aprovechar las ventajas en términos de reducción de costos de licenciamiento, independencia tecnológica y flexibilidad operativa.

De igual manera, el reutilizar equipos de cómputo que estaban destinados a baja o desecho otorgó una segunda oportunidad a la vida útil de los equipos, fomentando de esta manera la reducción de residuos electrónicos y alinear prácticas referentes tanto a la sostenibilidad tecnológica como al aprovechamiento responsable de los recursos institucionales.

Como parte de la mejora continua, se contempla proponer la implementación de servidores de impresión por departamento, gestionados en su totalidad mediante *software* libre, incluyendo sistema operativo, *suite* ofimática y *firewall*. Esta propuesta permitirá una administración descentralizada, con mayor control, mejor eficiencia operativa y adaptable a las necesidades específicas de cada área.

Por último, se plantea trabajar con el área responsable en la DGTIC para la asignación de direccionamiento IP segmentado o no homologado, con el fin de fortalecer la organización del direccionamiento de red y mejorar la seguridad interna.

REFERENCIAS

Andrews, J. (2019). *CompTIA A+ guide to IT technical support (10th ed.)*. Cengage Learning.

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022)*. ISO.

Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.

Patterson, D. A., & Hennessy, J. L. (2017). *Computer organization and design: The hardware/software interface* (5th ed.). Morgan Kaufmann.

Vermaat, M.E., Sebok, S., Freund, S.M., Campbell, J., & Frydenberg, M. (2018). *Discovering computers* (16ª ed.). Cengage.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2022). *Operating system concepts* (10th ed.). Wiley.

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

Stallings, W., & Brown, L. (2022). *Computer security: Principles and practice* (5th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 93 - 98

ANEXO A. CARACTERÍSTICAS DEL *HARDWARE* DEL SERVIDOR

Equipo de escritorio

El equipo corresponde a una computadora personal de escritorio, que tiene la función de administrar y gestionar el servicio de impresión, por consiguiente, no requiere de un alto poder de procesamiento ni recursos avanzados de *hardware*. Es importante señalar que el equipo ya había cumplido su ciclo de vida útil conforme a los criterios institucionales de renovación tecnológica. No obstante, con el objetivo de optimizar el aprovechamiento de los recursos, reducir la generación de residuos electrónicos y mitigar los efectos de la obsolescencia programada, se determinó su reacondicionamiento y reutilización para implementarlo al servidor de impresión. A continuación, se presentan las características del equipo en la Tabla 5:

Tabla 5

Especificaciones físicas del equipo de escritorio

Especificaciones del equipo	
Procesador	Intel ® Core (™) i5-4460 CPU @ 3.20 GHz 3.20 GHz
RAM Instalada	16.0 GB (15.9 GB usable)
Tipo de sistema	Sistema operativo de 64 bits (procesador basado en x64)

Impresora HP LaserJet Pro 400 Serie M401

Es una impresora láser monocromática (blanco/negro), diseñada para trabajo de oficina moderado. Dado que la mayoría de los documentos generados corresponden a trámites administrativos e información interna, no se requiere salida a color. En consecuencia, utilizar una impresora monocromática para el servidor de impresión constituye una decisión técnicamente viable, económicamente eficiente y congruente con las políticas institucionales de uso responsable de los recursos.

A continuación, en la Tabla 6, se presentan las características de la impresora:

Tabla 6

Características físicas de la impresora láser B/N

Impresora HP Laser Jet Pro 400 serie M401	
Tecnología de impresión	Láser
Calidad de impresión en negro (óptima)	Hasta 1200 x 1200 ppp
Pantalla	LCD de 2 líneas (texto y gráficos)
Capacidad inalámbrica	No
Conectividad, estándar	1 USB 2.0 de alta velocidad 1 red Ethernet 10/100/1000T
Preparado para red	Estándar (Gigabit Ethernet incorporado)

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 94 - 98

ANEXO B. SELECCIÓN DE *SOFTWARE* BASADO EN PRUEBAS DE USO

Software de ofimática

Se determinó la necesidad de instalar en el servidor de impresión una *suite* ofimática para atender requerimientos operativos específicos. Para tal efecto, se evaluaron tres soluciones gratuitas de ofimática: LibreOffice, FreeOffice y Documentos de Google (incluidas las herramientas Hojas de cálculo y Presentaciones). La evaluación consideró criterios de funcionalidad, compatibilidad con formatos estándar, requerimientos técnicos y viabilidad de implementación en el entorno institucional. A continuación, se muestran las características más significativas de los aplicativos ofimáticos considerados a usarse en el servidor de impresión en la Tabla 7:

Tabla 7

Comparativa de aplicaciones de ofimática

Característica	LibreOffice https://es.libreoffice.org/	Free Office https://www.freeoffice.com/es/	Google Docs/Sheets/Slides https://gmail.com
Modelo	*Software* de escritorio	*Software* de escritorio	*Software* basado en la nube
Costo	Gratis (código abierto)	Gratis (propietario)	Gratis (con opción de paga para Workspace)
Colaboración en tiempo real	No	No	Sí
¿Se puede usar sin Internet?	Sí	Sí	Limitado en modo *offline*
Compatible con MS Office	Sí, alta compatibilidad	Sí, alta compatibilidad	Sí, pero limitado
Automatización/Macros	Sí, alto	Sí, medio	Sí, medio
Extensiones/Plugins	Sí, muchos	Sí, pocos	Integrado con *apps* web
Privacidad de datos	Sí, local	Sí, local	En la nube

Pruebas realizadas en aplicaciones de ofimática

Para poder determinar qué opción resultaba más conveniente, se evaluaron diversos factores y se llevaron a cabo pruebas básicas de funcionamiento. En una primera etapa, se consideraron las características físicas del servidor de impresión (Tabla 1), dado que estas pueden influir directamente al procesar y gestionar archivos ofimáticos. Las pruebas realizadas fueron las siguientes:

- Abrir un documento previamente creado en Microsoft Office y observar si el formato cambiaba: En este caso, LibreOffice presentó mejor compatibilidad con archivos .docx sin alterar el contenido de los mismos.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 95 - 98

- Abrir un trabajo o archivo de más de 50 páginas: En este punto se analizó cuál fue la opción a la que le tomó menos tiempo abrir y mostrar el contenido completo del documento. FreeOffice dio mejores resultados, LibreOffice tardó unos segundos más y Documentos de Google presentó una gran variación de tiempos según el navegador y la velocidad de la conexión a Internet.
- Pruebas de trabajo colaborativo: En este rubro, Documentos de Google fue, sin lugar a duda, la mejor opción, ya que el *software* está enfocado al trabajo en línea mientras que las otras aplicaciones están diseñadas para trabajar de manera local.
- Prueba de impresión: Aquí, LibreOffice presentó un mejor control y compatibilidad de impresión con Windows.
- Prueba de usabilidad: Para esta última prueba, se tomó en cuenta que el entorno gráfico y el comportamiento del aplicativo fueran similares al de Microsoft Office, pues dicho *software* representa la principal opción de los usuarios en cuanto a tareas de ofimática se refiere, por lo que era necesario buscar una herramienta que no representara un gran cambio frente a la experiencia de uso del aplicativo de Microsoft. LibreOffice resultó ser la opción más cómoda y familiar en este apartado, gracias a sus opciones de personalización de interfaz que permiten que esta sea prácticamente igual a la de Word.

En la Tabla 8 se presentan los resultados de las pruebas de manera concreta:

Tabla 8

Comparativo de pruebas

Prueba	LibreOffice	FreeOffice	Google Docs/Sheets/ Slides
Compatibilidad	✓	-	-
Velocidad de apertura de archivo	-	✓	-
Trabajo colaborativo	-	-	✓
Prueba de impresión	✓	-	-
Usabilidad	✓	-	-

Derivado de las pruebas realizadas y del análisis técnico y administrativo, se concluyó que la mejor opción es LibreOffice, pues representa la alternativa más viable para su uso e implementación en el servidor de impresión. La decisión se fundamenta en su carácter de *software* libre, ausencia de costos de licenciamiento, compatibilidad adecuada con formatos estándar utilizados en la dependencia y su funcionamiento sin necesidad de conexión a Internet. Por consiguiente, su bajo requerimiento de recursos técnicos resulta congruente con las capacidades del equipo reutilizado, garantizando estabilidad operativa sin comprometer el rendimiento del servidor de impresión.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 96 - 98

Firewall

Con el fin de fortalecer la seguridad del servidor de impresión, se decidió instalar un *firewall* adicional. Cabe mencionar que este no reemplazará al *firewall* integrado de Windows 10 Pro, sino que trabajará en conjunto para robustecer la protección del sistema.

El *firewall* puede implementarse mediante *hardware*, *software* o una combinación de ambos. Su función principal consiste en monitorear el tráfico de red y controlar el acceso al servidor, actuando como un sistema que aplica la política de seguridad de la red privada y la Internet (Cuenca, 2016). A través del *firewall*, es posible generar listas de control de acceso que definan qué usuarios pueden utilizar el servicio de impresión.

Para la implementación del *firewall* se consideraron tres opciones: Zone Alarm, TinyWall y Comodo Firewall. Con el objetivo de seleccionar la solución más adecuada, se llevaron a cabo pruebas de funcionalidad, compatibilidad y desempeño, así como comparativos técnicos entre las alternativas seleccionadas. En la Tabla 9 se muestra la comparativa de las tres opciones consideradas para instalación en el servidor de impresión.

Tabla 9

Comparativa del firewall (cortafuegos)

Características	ZoneAlarm https://www.ZoneAlarm.com/	TinyWall https://tinywall.pados.hu/	Comodo Firewall https://www.comodo.com/?af=7639
Modelo	*Software* de escritorio	*Software* de escritorio	*Software* de escritorio
Costo	Versión gratuita/ Versión paga	Versión 100% gratuita	Versión gratuita/ Versión paga
Requisitos de *hardware*	Uso medio de RAM y CPU	Uso mínimo de RAM y CPU	Uso medio de RAM y CPU
Nivel de usabilidad	Fácil	Medio	Avanzado
Perfil de usuario	Intermedio	Principiante	Avanzado
Nivel de protección	Seguro	Seguro	Muy seguro

Pruebas realizadas para la elección del *firewall*

Para seleccionar el mejor *firewall* a implementarse en el servidor de impresión, se siguieron la siguiente metodología y criterios: mismo equipo y sistema operativo, un *firewall* a la vez y uso de la configuración por defecto. Las pruebas realizadas consistieron en pruebas de control de tráfico entrante/saliente, rendimiento de los recursos de *hardware* del equipo, desactivación del *firewall* sin autorización y usabilidad, así como experiencia previa del usuario. En la Tabla 10 se observa el comparativo de las pruebas realizadas a los tres *firewalls* considerados para instalar en el servidor de impresión.

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 97 - 98

Tabla 10

Comparativo de pruebas

Prueba	Zone Alarm	TinyWall	Comodo *Firewall*
Pruebas de tráfico entrante/saliente	Alto	Alto	Muy alto
Rendimiento	Medio	Excelente	Bajo
Usabilidad	Alto	Medio	Alto
Desactivación	Alto	Medio	Muy alto

Elección del *firewall*

Se determinó que ZoneAlarm es la solución más adecuada para su implementación en el servidor de impresión con base en los siguientes criterios: presenta un buen equilibrio con respecto a la seguridad, rendimiento y usabilidad; es totalmente compatible con Windows 10 Pro, garantizando una integración estable con el sistema operativo y con el *firewall* nativo, permitiendo un esquema de seguridad por capas, sin conflictos de *software*.

La interfaz de ZoneAlarm es intuitiva y permite configurar listas de control de acceso y reglas de seguridad de manera sencilla, facilitando la administración del servidor y reduciendo el riesgo de errores de configuración por parte del personal técnico. El nivel de seguridad incluye monitoreo del tráfico de la red, realización de bloqueos de conexiones no autorizadas y emisión de alertas en tiempo real, permitiendo que sólo los usuarios autorizados puedan acceder al servicio de impresión. Además, mantiene un impacto moderado en el rendimiento del servidor, asegurando que el servicio de impresión no se vea afectado. Al ser una instalación ligera y de fácil gestión, se ajusta a los recursos del servidor reutilizado, evitando la necesidad de actualizar *hardware* o generar costos adicionales de licenciamiento. Por estas razones, la elección de ZoneAlarm proporciona una protección robusta y confiable al servidor de impresión, cumpliendo con los principios de seguridad y eficiencia operativa.

Antivirus

El objetivo de instalar un antivirus en el servidor de impresión es añadir una capa adicional de seguridad para proteger los archivos y el sistema contra amenazas que puedan comprometer su funcionamiento. Los antivirus emplean bases de datos de firmas de *malware* conocidas para identificar *software* malicioso y también son capaces de analizar el comportamiento del sistema en busca de actividades sospechosas (Arango, 2023).

Para la implementación en el servidor, se consideraron tres opciones gratuitas: Avira, AVG y Avast. Para la implementación del antivirus, la evaluación se basó en los siguientes criterios: compatibilidad con el sistema operativo Windows 10 Pro, consumo bajo de recursos para garantizar que el antivirus no afecte el rendimiento del servidor, facilidad tanto de configuración como de actualización y, por último, la eficiencia en la detección de amenazas y cobertura frente a *malware* conocido y emergente. En la Tabla 11 se muestra una comparativa de los tres antivirus considerados a instalar en el servidor de impresión:

https://doi.org/10.22201/dgtic.30618096e.2026.4.2.174 Vol. 4, Núm. 2. abril-junio 2026, págs. 98 - 98

Tabla 11

Comparativa de antivirus

Característica	AVIRA https://www.avira.com/es	AVG https://www.avg.com/es-mx/homepage#pc	AVAST https://www.avast.com/es-mx/index#pc
Protección contra *malware*	Bueno	Excelente	Excelente
Rendimiento	Excelente	Bueno	Bueno
Funciones extras	Excelente	Bueno	Bueno
Versión gratuita	Excelente	Excelente	Excelente
Privacidad	Excelente	Bueno	Bueno
Usabilidad	Excelente	Excelente	Bueno

Elección del antivirus

Finalmente, se seleccionó Avira para proteger el servidor de impresión debido a su bajo consumo de recursos, compatibilidad con Windows 10 Pro y facilidad de gestión, además de que ofrece actualizaciones automáticas de su base de datos de *malware*, lo que garantiza la protección frente a nuevas amenazas de manera continua y confiable.