ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

# IPES

# INFORME DE SEGURIDAD

## INFORME DE VULNERABILIDADES
## Escaneos NMAP
## MAYO 2026

**Bogotá, 2026**

| Elaboró | Revisó: | Aprobó: |
|---|---|---|
| Michael Brayan Pinilla Coy<br>Contratista | Hans Lwer Carlosama Alfarez<br>Profesional Especializado | Adriana Villamizar Nvarro<br>Subdirectora de Diseño y Analisis Estretegico |

# Tabla de Contenido


1. RESUMEN EJECUTIVO....3
2. INVENTARIO DE SERVIDORES CRITICOS ANALIZADOS....3
3. HALLAZGOS POR SERVIDOR....4
4. DEFINICIONES....4
5. HALLAZGO PRINCIPAL — VPN SIN AUTENTICACION MULTIFACTOR (MFA)....5
6. HALLAZGOS ADICIONALES....6
7. PLAN DE ACCION Y RECOMENDACIONES....7

## 1. RESUMEN EJECUTIVO

El presente informe documenta los hallazgos identificados durante la revision de seguridad de la infraestructura institucional, realizada el 30 de mayo de 2026. El analisis fue ejecutado por el Oficial de Seguridad de la Informacion utilizando herramientas especializadas de escaneo de red (Nmap 7.99) y deteccion de vulnerabilidades (OpenVAS / Greenbone Community Edition).

El hallazgo principal identificado corresponde a la ausencia de Autenticacion Multifactor (MFA) en la VPN institucional (FortiClient / FortiGate). Esta brecha fue detectada por el Oficial de Seguridad en su condicion de usuario regular de la entidad, evidenciando que el acceso a la red interna depende exclusivamente de credenciales de usuario y contrasena, sin ningun segundo factor de verificacion de identidad.

Complementariamente, el escaneo de puertos sobre los 5 servidores identifico servicios expuestos en la red interna que, en caso de compromiso de credenciales VPN, podrian ser accedidos por un actor malicioso dentro de los limites que establece el control de acceso basado en grupos de Active Directory y las politicas de firewall FortiGate activas.

| Hallazgo | Ambito | Nivel de Riesgo |
|---|---|---|
| VPN institucional sin MFA activo | Toda la infraestructura | **ALTO** |
| RDP expuesto en 3 servidores | 10.10.200.24 / 192.168.0.36 / 192.168.0.153 | **MEDIO** |
| Windows Server 2008/2012 sin soporte oficial | 192.168.0.36 Servidor Goobi | **ALTO** |
| Base de datos Oracle accesible en red interna | 192.168.0.160 BD Goobi | **MEDIO** |
| Base de datos MariaDB accesible en red interna | 192.168.0.153 App GLPI | **MEDIO** |
| Apache 2.4.46 y OpenSSL 1.1.1j desactualizados | 192.168.0.153 App GLPI | **MEDIO** |
| VNC activo en servidor de base de datos | 192.168.0.160 BD Goobi | **MEDIO** |
| BD HEMI (192.168.0.72) no respondio al escaneo | 192.168.0.72 BD HEMI | **INFO** |

## 2. INVENTARIO DE SERVIDORES CRITICOS ANALIZADOS

Se realizo escaneo de puertos y servicios sobre los siguientes 5 hosts identificados como servidores criticos institucionales:

| Direccion IP | Nombre / Funcion | Sistema Operativo | Resultado Escaneo |
|---|---|---|---|
| 10.10.200.24 | Aplicacion HEMI | Windows | Activo - 6 puertos detectados |
| 192.168.0.36 | Servidor Goobi | Windows Server 2008/2012 | Activo - 9 puertos detectados |
| 192.168.0.72 | BD HEMI | Desconocido | Sin respuesta - posible bloqueo firewall |

| | | | |
|---|---|---|---|
| 192.168.0.153 | Aplicacion GLPI | Windows | Activo - 9 puertos detectados |
| 192.168.0.160 | BD Goobi | Linux | Activo - 12 puertos detectados |

## 3. HALLAZGOS POR SERVIDOR

### Aplicacion HEMI - 10.10.200.24

| Puerto | Estado | Servicio | Version | Riesgo |
|---|---|---|---|---|
| 80/tcp | open | HTTP | Microsoft IIS 10.0 | **BAJO** |
| 443/tcp | open | HTTPS | SSL/HTTPS | **BAJO** |
| 2000/tcp | open | tcpwrapped | Desconocido | **MEDIO** |
| 3389/tcp | open | RDP | Microsoft Terminal Services | **MEDIO** |
| 5060/tcp | open | tcpwrapped | Posible VoIP | **BAJO** |
| 8080/tcp | open | HTTP alterno | Microsoft IIS 10.0 | **BAJO** |

## 4. DEFINICIONES

### Servidor Goobi - 192.168.0.36

Nmap detecto Windows Server 2008 R2 / 2012 como sistema operativo. Estos sistemas operativos no cuentan con soporte oficial de Microsoft desde enero 2020 y octubre 2023 respectivamente, lo que implica ausencia de parches de seguridad.

| Puerto | Estado | Servicio | Version | Riesgo |
|---|---|---|---|---|
| 135/tcp | open | MSRPC | Windows RPC | **BAJO** |
| 139/tcp | open | NetBIOS | Windows NetBIOS | **MEDIO** |
| 445/tcp | open | SMB | Windows Server 2008-2012 | **MEDIO** |
| 2179/tcp | open | vmrdp | Virtual Machine RDP | **BAJO** |
| 3389/tcp | open | RDP | Microsoft Terminal Services | **MEDIO** |
| 49155-49157/tcp | open | MSRPC dinamico | Windows RPC | **BAJO** |

### BD HEMI — 192.168.0.72

El host 192.168.0.72 no respondio al escaneo de puertos realizado con Nmap. Esto puede indicar que el servidor tiene reglas de firewall que bloquean el trafico de escaneo (lo cual seria una buena practica) o que el servidor se encontraba inactivo al momento del analisis. Se recomienda verificar con el area de infraestructura el estado actual de este servidor.

**Aplicacion GLPI — 192.168.0.153**

Se detectaron versiones desactualizadas de Apache (2.4.46) y OpenSSL (1.1.1j) con fecha de lanzamiento en 2021. Estas versiones pueden contener vulnerabilidades conocidas sin parche aplicado.

| Puerto | Estado | Servicio | Version | Riesgo |
|---|---|---|---|---|
| 80/tcp | open | HTTP | Apache 2.4.46 (Win64) | **MEDIO** |
| 135/tcp | open | MSRPC | Windows RPC | **BAJO** |
| 139/tcp | open | NetBIOS | Windows NetBIOS | **MEDIO** |
| 443/tcp | open | HTTPS | Apache 2.4.46 + OpenSSL 1.1.1j | **MEDIO** |
| 445/tcp | open | SMB | Windows SMB | **MEDIO** |
| 3306/tcp | open | MySQL/MariaDB | MariaDB 10.4.18 | **MEDIO** |
| 3389/tcp | open | RDP | Microsoft Terminal Services | **MEDIO** |

**BD Goobi — 192.168.0.160**

| Puerto | Estado | Servicio | Version | Riesgo |
|---|---|---|---|---|
| 22/tcp | open | SSH | OpenSSH 8.7 (protocol 2.0) | **BAJO** |
| 111/tcp | open | RPCbind | 2-4 RPC #100000 | **MEDIO** |
| 1521/tcp | open | Oracle TNS | Oracle TNS Listener | **MEDIO** |
| 2000/tcp | open | tcpwrapped | Desconocido | **MEDIO** |
| 5060/tcp | open | tcpwrapped | Desconocido | **BAJO** |
| 5500/tcp | open | Oracle XML DB | Oracle XML DB Enterprise | **MEDIO** |
| 5903/tcp | open | VNC | VNC protocol 3.8 | **MEDIO** |

## 5. HALLAZGO PRINCIPAL — VPN SIN AUTENTICACION MULTIFACTOR (MFA)

**Descripcion del Hallazgo**

Durante el acceso rutinario a la VPN institucional mediante FortiClient, el Oficial de Seguridad de la Informacion identifico que el proceso de autenticacion solicita unicamente usuario y contrasena, sin requerir un segundo factor de verificacion de identidad (MFA). Este hallazgo fue identificado desde el perfil de un usuario regular de la entidad.

La entidad cuenta con los siguientes controles de acceso activos que mitigan parcialmente el riesgo:

- Autenticacion centralizada contra Active Directory (AD) integrada con FortiGate.
- Control de acceso basado en grupos: cada usuario accede unicamente a los servicios autorizados segun su perfil.
- Politicas de firewall activas en FortiGate que restringen el trafico entre segmentos de red.

Sin embargo, estos controles dependen exclusivamente de la confidencialidad de las credenciales del usuario. La ausencia de MFA significa que si un atacante obtiene las credenciales de un usuario (mediante phishing, fuerza bruta o filtracion de datos), podra acceder a la red interna sin ningun obstáculo adicional, heredando todos los permisos del usuario comprometido.

**Vector de Ataque**

| Paso | Accion del Actor Amenaza | Impacto Potencial |
|---|---|---|
| 1 | Obtiene credenciales VPN de un usuario institucional mediante phishing, fuerza bruta o filtracion | Acceso a credenciales institucionales validas |
| 2 | Se conecta a la VPN con las credenciales obtenidas sin necesidad de segundo factor | Acceso a la red interna institucional |
| 3 | Accede a los recursos y servicios permitidos por el grupo de AD del usuario comprometido | Acceso no autorizado a informacion y sistemas segun perfil del usuario |
| 4 | Si el usuario comprometido pertenece a grupos privilegiados (TI, Administradores), el impacto se amplifica significativamente | **Acceso a infraestructura critica, servidores y bases de datos** |

**Solucion Recomendada — MFA con Google Workspace**

La entidad cuenta con Google Workspace activo, lo que permitiria implementar MFA, mas sin embargo es pertinente que el ingeniero de infraestructura evalue la viabilidad tecnica y costos operativos.

## 6. HALLAZGOS ADICIONALES

**Windows Server 2008/2012 sin Soporte Oficial**

El servidor Goobi (192.168.0.36) opera sobre Windows Server 2008 R2 o 2012, sistemas que

alcanzaron su fin de soporte extendido en enero 2020 y octubre 2023 respectivamente. Microsoft no emite parches de seguridad para estas versiones, dejando el sistema expuesto a vulnerabilidades conocidas sin posibilidad de remediacion mediante actualizaciones del fabricante.

- Recomendacion: Planificar migracion a Windows Server 2022 o superior.
- Responsable: Ingeniero de Infraestructura TI / Contratista.
- Prioridad: Alta.

**Versiones Desactualizadas en Servidor GLPI (192.168.0.153)**

- Apache 2.4.46: Version de 2021, se recomienda actualizar a 2.4.62 o superior.
- OpenSSL 1.1.1j: Version de 2021 con soporte terminado. Actualizar a OpenSSL 3.x.
- MariaDB 10.4.18: Validar si la version actual cuenta con parches de seguridad vigentes.

**RDP Expuesto en Red Interna**

El protocolo RDP (puerto 3389) se detecto activo en 3 de los 4 servidores analizados (App HEMI, Servidor Goobi, App GLPI). Aunque las politicas de firewall y los grupos de AD limitan el acceso, se recomienda validar que unicamente los administradores autorizados tengan acceso a este servicio.

**BD HEMI sin Respuesta al Escaneo**

El servidor 192.168.0.72 (BD HEMI) no respondio al escaneo de Nmap. Se recomienda confirmar con el area de infraestructura si el servidor esta activo y verificar que el bloqueo al escaneo sea resultado de una politica de firewall intencionada.

## 7. PLAN DE ACCION Y RECOMENDACIONES

| Accion | Responsable | Plazo | Prioridad |
|---|---|---|---|
| Solicitar al contratista Fortinet evaluar posibilidad de configuración MFA con Google Workspace en FortiGate | Coordinador GIRT / Ing. Infraestructura | Inmediato | **ALTO** |
| Planificar migracion de Windows Server 2008/2012 a version con soporte | Ing. Infraestructura / Contratista | Corto plazo | **ALTO** |
| Actualizar Apache y OpenSSL en servidor GLPI (192.168.0.153) | Ing. Infraestructura / Contratista | Corto plazo | **MEDIO** |
| Verificar y documentar reglas de firewall para puertos RDP, Oracle y MariaDB | Ing. Infraestructura | Corto plazo | **MEDIO** |
| Confirmar estado y politicas de firewall para BD HEMI | Ing. Infraestructura | Inmediato | **MEDIO** |

| | | | |
|---|---|---|---|
| (192.168.0.72) | | | |