**Auditoría/Informe del proyecto del equipo Gryffindor CIT31-01**

# ÍNDICE

[ÍNDICE 2](#_Toc106178984)

[ÍNDICE DE FIGURAS 3](#_Toc106178985)

[ENUNCIADO 4](#_Toc106178986)

[RED PROPUESTA 5](#_Toc106178987)

[AUDITORIA 7](#_Toc106178988)

[1. Enumeración de redes, componentes, topologías y protocolos 7](#_Toc106178989)

[2. Identificación de los sistemas operativos instalados 7](#_Toc106178990)

[3. Análisis de servicios y aplicaciones 8](#_Toc106178991)

[4. Detección, comprobación y evaluación de vulnerabilidades 9](#_Toc106178992)

[5. Medidas específicas de corrección 10](#_Toc106178993)

[6. Recomendaciones sobre implantación de medidas preventivas. 11](#_Toc106178994)

[REFERENCIAS 14](#_Toc106178995)

# ÍNDICE DE FIGURAS

[Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022). 6](#_heading=h.2et92p0)

# ENUNCIADO

Usted trabaja para la una empresa de SmartBuildings. Ante la emergencia de Coronavirus se le pide desplegar un sistema de SmartCities para comunicar en tiempo real a los miembros del sistema sanitario. Para ello despliega en dos edificios sistemas basados en gateways Linux (puede escoger la distribución más apropiada). Dichos sistemas permiten enviar información mediante una interfaz web a una base de datos alojada en uno de los edificios. A dicha base de datos y servicio web solo se puede acceder desde la intranet del edificio. Además, en el servidor, debe alojar una plataforma web para que todo el público pueda enviar consultas y otra información para permitir servicios de telemedicina.

Debe planificar un sistema seguro que permita a los gateway enviar los datos al servidor, que además debe estar accesible a los habitantes del edificio y cualquier usuario doméstico (todos ellos usuarios de Windows). Dichos usuarios se conectan desde Intranet donde se dispone de una LAN WiFi que mantiene conectados los equipos mencionados y, además, dispositivos móviles.

Adicionalmente, el profesor dijo que tratásemos de hacer nuestro proyecto de mensajería sin alterar la infraestructura original.

# RED PROPUESTA

Inicialmente nos centramos por un diseño como el mencionado en el enunciado, tanto por simplicidad como por petición del enunciado, en el que se comunica el exterior con el interior mediante una VPN para evitar tener que alterar la infraestructura original de la empresa, incluyendo firewalls. La red VPN tiene la ventaja de cifrar el tráfico durante el establecimiento de conexión con los servidores, lo que hace que ya no aparezca texto en claro sensible con datos del usuario que pueda ser fácilmente expuesto en redes Wi-fi no muy seguras y dificulta que un ataque man-in-the-middle pueda acceder a estos, algo vital para el servicio de mensajería.

Al comienzo tratamos de usar la VPN pre-instalada de Windows, pero por comodidad decidimos emplear el software profesional OpenVPN. Según las instrucciones de instalación (WunderTech, 2022), hemos decidido que nuestra VPN es 192.168.60.0/24 es la VPN, llamada OpenVPN Servidor, la Clave pre-compartida es “SorbeteDeLimon” y el resto queda por defecto. Estos parámetros los utilizamos para el Firewall de su edificio también. El usuario es SSR con nombre completo “Albus Dumbledore”.

El edificio remoto tiene red 192.168.57.0/24, el edificio de la empresa 192.168.56.0/24 y la internet la simulamos con la 100.200.0.0/24, inicialmente tratamos de hacer una conexión entre dos ordenadores físicos virtualizando los edificios y con un módem físico entre medias, pero no funcionó así que pasamos a virtualizarlo todo en una máquina y quitarnos el router de en medio.

Hemos supuesto que en la infraestructura original los gateways son del tipo pfSense y utilizan un único firewall por edificio de política restrictiva hacia adentro, para mayor seguridad (menos funcionalidades supone menos potenciales vulnerabilidades), permitiendo la entrada por el puerto 443 y 80 (también está el 3306 para el mySQL pero para acceso local); y sin suponer mayor profundidad en la red, para permitir virtualizar varias máquinas.

La BBDD es SQL mediante xampp.

El material de nuestra red puede encontrarse en el github:

https://github.com/tardisfromtornspace/ProyectoGryffindorCIT31-01.git

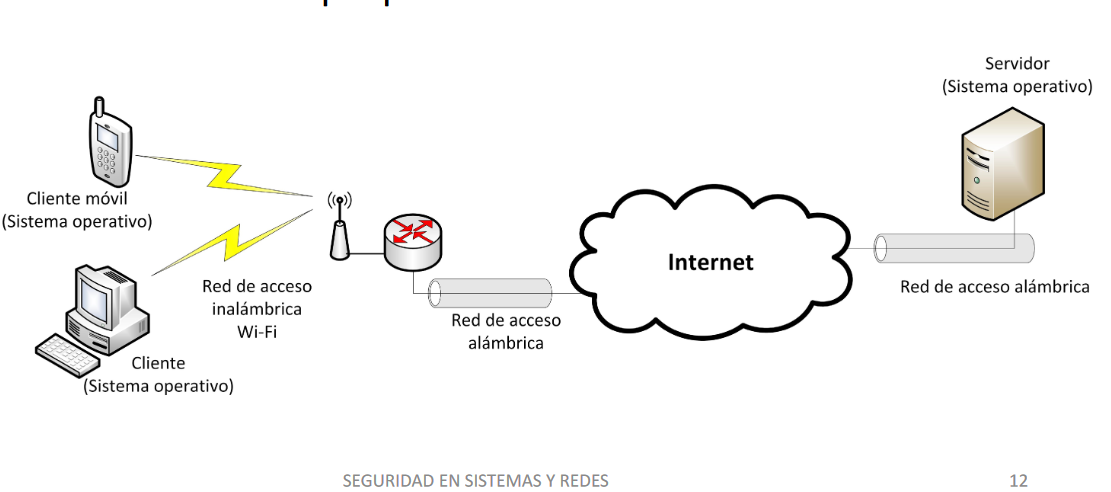


Figura 1: Modelo esquemático de la red propuesta **(Sánchez, 2022)**.

# AUDITORIA

Hemos decidido emplear una auditoría de caja blanca por falta de tiempo y para mayor eficiencia, con un conocimiento total de la red.

*Los ataques se hacen desde 3 sitios, edificio de la empresa, edifico remoto y desde la internet, con una Kali Linux o Windows donde corresponda*

## Enumeración de redes, componentes, topologías y protocolos

Hay 3 redes, mencionadas en el apartado red propuesta:

**LANA** – La red del edificio de la empresa 192.168.56.0/24 Tiene configurada una VPN. Tiene una máquina servidor (192.168.56.10) y el router pfSense1 (192.168.56.1)

**LANB** – La red edificio remoto 192.168.57.0/24. Tiene una máquina clienteRemoto (192.168.57.2) y el router pfSense2 (192.168.57.1)

**WAN** – Simulación del internet 100.200.0.0/24. Tiene a los dos routers (pfSense1 con 100.200.0.1 y pfSense2 con 100.200.0.2).

Todos ellos emplean topología en estrella, menos la conexión de WAN, simulada con un P2P. Todos ellos emplean máscara /24 por simplicidad.

Routers:

**pfSense1:** es el que conecta LANA con WAN

**pfSense2:** es el que conecta LANB con WAN

-Ambos actúan con el mismo tipo de firewall: política permisiva desde LAN y restrictiva desde WAN.

Usamos protocolo TCP/IP para las conexiones, salvo OpenVPN, que se especializa en el uso de UDP.

## Identificación de los sistemas operativos instalados

1. **pfSense1 (#R1):** pfSense 2.6.0-RELEASE FreeBSD 64-bit 12.3-STABLE
2. **pfSense2 (#R2)**: pfSense 2.5.2-RELEASE FreeBSD 64-bit 12.2-STABLE
3. **ClienteRemoto** **(#LANB1**): ~~Windows XP 32-bit con parche Service Pack 3~~ *No hemos usado el Windows XP por su gran número de vulnerabilidades conocidas y la imposibilidad de actualizar o parchear gran parte de ellas, así que hemos empleado un* Windows 7 Ultimate 32-bit bit 6.1.7601 Service Pack 1 Build 7601
4. **Servidor (#LANB2):** Windows 10 Education 64-bit, versión 1903, versión del SO 18362.592.

## Análisis de servicios y aplicaciones

|  |
| --- |
| **pfSense1 (#R1)**  ¿ESTE NMAP FUE POR EL LAN O EL WAN?   * PORT STATE SERVICE VERSION * **80**/tcp open http nginx * **443**/tcp open ssl/https?   Dispone solamente del servicio http en el puerto 80 para la configuración del pfsense. Lo mismo ocurre con el puerto 443, para la conexión por https que ha sido configurada en el pfSense1.  El puerto 1194 se encuentra abierto para la comunicación  por VPN, aunque Nmap no lo ha detectado. No lo habrá detectado porque este es el escáner desde la LAN, ¿correcto?  COMPLETAR AÑADIENDO EL NMAP DESDE EL OTRO LADO INDICANDOLO COMO UNA SEGUNDA PARTE  PORT STATE SERVICE VERSION  **pfSense2 (#R2)**:  ¿ESTE NMAP FUE POR EL LAN O EL WAN?  PORT STATE SERVICE VERSION   * **53**/tcp open domain Unbound * **80**/tcp open http nginx * **443**/tcp open ssl/http nginx   Similar a pfSense1, pero en este caso el puerto 53 se encuentra abierto.  Este servicio se utiliza para comunicar tramas DNS.  El puerto 1194 se encuentra abierto para la comunicación  por VPN, aunque Nmap no lo ha detectado. No lo habrá detectado porque este es el escáner desde la LAN, ¿correcto?  COMPLETAR AÑADIENDO EL NMAP DESDE EL OTRO LADO INDICANDOLO COMO UNA SEGUNDA PARTE  PORT STATE SERVICE VERSION  **ClienteRemoto** **(#LANB1**):  Resultados del nmap  PORT STATE SERVICE VERSION   * **135**/tcp open msrpc Microsoft Windows RPC * **139**/tcp open netbios-ssn Microsoft Windows netbios-ssn * **445**/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) * **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) * **49152**/tcp open msrpc Microsoft Windows RPC * **49153**/tcp open msrpc Microsoft Windows RPC * **49154**/tcp open msrpc Microsoft Windows RPC * **49155**/tcp open msrpc Microsoft Windows RPC * **49156**/tcp open msrpc Microsoft Windows RPC * **49157**/tcp open msrpc Microsoft Windows RPC   **AÑADIR APLICACIONES (LA LISTA DE ABAJO ESTÁ DESACTUALIZADA Y SE DEBEN ELIMINAR ALGUNAS APLICACIONES SI HACE FALTA)**  **https://www.ionos.es/digitalguide/servidores/configuracion/como-saber-el-nombre-de-mi-pc/**  Lista de aplicaciones**:**   1. (A RELLENAR)   **ACTUALIZAR LISTA DE SERVICIOS TRAS ELIMINAR APLICACIONES INNECESARIAS**  Lista de servicios (total, no hecha por Nmap, por lo que no se tendrá tan en cuenta):   * 1. ActiveX Installer (AxInstSV)   2. Adaptive Brightness   3. Application Experience   4. Application Identity   5. Application Information   6. Application Layer Gateway Service   7. Application Management   8. ASP.NET State Service   9. Background Intelligent Transfer Service   10. Base Filtering Engine   11. BitLocker Drive Encryption Service   12. Block Level Backup Engine Service   13. Bluetooth Support Service   14. BranchCache   15. Certificate Propagation   16. CNG Key Isolation   17. COM+ Event System   18. COM+ System Application   19. Computer Browser   20. Credential Manager   21. Cryptographic Services   22. DCOM Server Process Launcher   23. Desktop Window Manager Session Manager   24. DHCP Client   25. Diagnostic Policy Service   26. Diagnostic Service Host   27. Diagnostic System Host   28. Diagnostics Tracking Service   29. Disk Defragmenter   30. Distributed Link Tracking Client   31. Distributed Transaction Coordinator   32. DNS Client   33. Encrypting File System (EFS)   34. Extensible Authentication Protocol   35. Fax   36. Function Discovery Provider Host   37. Function Discovery Resource Publication   38. Group Policy Client   39. Health Key and Certificate Management   40. HomeGroup Listener   41. HomeGroup Provider   42. Human Interface Device Access   43. IKE and AuthIP IPsec Keying Modules   44. Interactive Services Detection   45. Internet Connection Sharing (ICS)   46. Internet Explorer ETW Collector Service   47. IP Helper   48. IPsec Policy Agent   49. KtmRm for Distributed Transaction Coordinator   50. Link-Layer Topology Discovery Mapper   51. Media Center Extender Service   52. Microsoft .NET Framework NGEN v2.0.50727\_X86   53. Microsoft .NET Framework NGEN v4.0.30319\_X86   54. Microsoft iSCSI Initiator Service   55. Microsoft Software Shadow Copy Provider   56. Mozilla Maintenance Service   57. Multimedia Class Scheduler   58. Net.Msmq Listener Adapter   59. Net.Pipe Listener Adapter   60. Net.Tcp Listener Adapter   61. Net.Tcp Port Sharing Service   62. Netlogon   63. Network Access Protection Agent   64. Network Connections   65. Network List Service   66. Network Location Awareness   67. Network Store Interface Service   68. Offline Files   69. OpenVPN Interactive Service   70. Parental Controls   71. Peer Name Resolution Protocol   72. Peer Networking Grouping   73. Peer Networking Identity Manager   74. Performance Logs & Alerts   75. Plug and Play   76. PnP-X IP Bus Enumerator   77. PNRP Machine Name Publication Service   78. Portable Device Enumerator Service   79. Power   80. Print Spooler   81. Problem Reports and Solutions Control Panel Support   82. Program Compatibility Assistant Service   83. Protected Storage   84. Quality Windows Audio Video Experience   85. Remote Access Auto Connection Manager   86. Remote Access Connection Manager   87. Remote Desktop Configuration   88. Remote Desktop Services   89. Remote Desktop Services UserMode Port Redirector   90. Remote Procedure Call (RPC)   91. Remote Procedure Call (RPC) Locator   92. Remote Registry   93. Routing and Remote Access   94. RPC Endpoint Mapper   95. Secondary Logon   96. Secure Socket Tunneling Protocol Service   97. Security Accounts Manager   98. Security Center   99. Server   100. Shell Hardware Detection   101. Smart Card   102. Smart Card Removal Policy   103. SNMP Trap   104. Software Protection   105. SPP Notification Service   106. SSDP Discovery   107. Superfetch   108. System Event Notification Service   109. Tablet PC Input Service   110. Task Scheduler   111. TCP/IP NetBIOS Helper   112. Telephony   113. Themes   114. Thread Ordering Server   115. UPnP Device Host   116. User Profile Service   117. Virtual Disk   118. VirtualBox Guest Additions Service   119. Volume Shadow Copy   120. WebClient   121. Windows Audio   122. Windows Audio Endpoint Builder   123. Windows Backup   124. Windows Biometric Service   125. Windows CardSpace   126. Windows Color System   127. Windows Connect Now - Config Registrar   128. Windows Defender   129. Windows Driver Foundation - User-mode Driver Framework   130. Windows Error Reporting Service   131. Windows Event Collector   132. Windows Event Log   133. Windows Firewall   134. Windows Font Cache Service   135. Windows Image Acquisition (WIA)   136. Windows Installer   137. Windows Management Instrumentation   138. Windows Media Center Receiver Service   139. Windows Media Center Scheduler Service   140. Windows Media Player Network Sharing Service   141. Windows Modules Installer   142. Windows Presentation Foundation Font Cache 3.0.0.0   143. Windows Remote Management (WS-Management)   144. Windows Search   145. Windows Time   146. Windows Update   147. WinHTTP Web Proxy Auto-Discovery Service   148. Wired AutoConfig   149. WLAN AutoConfig   150. WMI Performance Adapter   151. Workstation   **Servidor (#LANB2):**  Resultados del nmap  PORT STATE SERVICE VERSION   * **80**/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m * PHP/8.1.2) * **443**/tcp open ssl/http Apache httpd 2.4.52 ((Win64) * OpenSSL/1.1.1m PHP/8.1.2) * **3306**/tcp open mysql? * **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)   Los puertos 80 y 443 para la conexión http y https respectivamente.  En el puerto 3306 podemos encontrar la conexión a la base de datos  mysql. El puerto 5357 se utiliza para (¿se usa para qué? Esto se ha quedado a medias Ricardo)  Lista de aplicaciones (sacadas desde Aplicaciones y características porque tanto WMIC CONO Get-itemProperty solo nos dicen los que hemos instalado nosotros**):**   1. (A RELLENAR)   **AÑADIR APLICACIONES**  **APLICACIONES A DESINSTALAR DESDE APLICACIONES Y CARACTERÍSTICAS ANTES DE LISTARLAS: Casi todo, incluyendo Skype, Sticky Notes, Google Chrome, Tips, Visor 3D, Print 3D, Xbox…**  **AÑADIR LISTA DE SERVICIOS (desde Servicios)**  **Actualizar lo de abajo tras borrar las aplicaciones:**  Lista de servicios (total, no hecha por Nmap, por lo que no se tendrá tan en cuenta):   * 1. AarSvc\_2ce51   2. Actualizador de zona horaria automática   3. Adaptador de rendimiento de WMI   4. Administración de aplicaciones   5. Administración de autenticación de Xbox Live   6. Administración de capas de almacenamiento   7. Administración remota de Windows (WS-Management)   8. Administrador de conexiones automáticas de acceso remoto   9. Administrador de conexiones de acceso remoto   10. Administrador de conexiones de Windows   11. Administrador de configuración de dispositivos   12. Administrador de credenciales   13. Administrador de cuentas de seguridad   14. Administrador de cuentas web   15. Administrador de identidad de redes de mismo nivel   16. Administrador de mapas descargados   17. Administrador de pagos y NFC/SE   18. Administrador de sesión local   19. Administrador de usuarios   20. Adquisición de imágenes de Windows (WIA)   21. Agente de conexión de red   22. Agente de detección en segundo plano de DevQuery   23. Agente de directiva IPsec   24. Agente de eventos de tiempo   25. Agente de eventos del sistema   26. Agente de supervisión en tiempo de ejecución de Protección del sistema   27. Agrupación de red del mismo nivel   28. Aislamiento de claves CNG   29. Aplicación auxiliar de NetBIOS sobre TCP/IP   30. Aplicación auxiliar IP   31. Aplicación del sistema COM+   32. Archivos sin conexión   33. Asignador de detección de topologías de nivel de vínculo   34. Asignador de extremos de RPC   35. Asistente para la conectividad de red   36. Audio de Windows   37. Autenticación natural   38. Ayuda del Panel de control de Informes de problemas y soluciones   39. Ayudante para el inicio de sesión de cuenta Microsoft   40. BcastDVRUserService\_2ce51   41. BluetoothUserService\_2ce51   42. BranchCache   43. Captura de SNMP   44. CaptureService\_2ce51   45. Carpetas de trabajo   46. cbdhsvc\_2ce51   47. CDPUserSvc\_2ce51   48. Centro de seguridad   49. Cliente de directiva de grupo   50. Cliente de seguimiento de vínculos distribuidos   51. Cliente DHCP   52. Cliente DNS   53. Cliente web   54. Cola de impresión   55. Compilador de extremo de audio de Windows   56. Comprobador puntual   57. Conexión compartida a Internet (ICS)   58. Conexiones de red   59. Configuración automática de dispositivos conectados a la red   60. Configuración automática de redes cableadas   61. Configuración automática de WLAN   62. Configuración automática de WWAN   63. Configuración de Escritorio remoto   64. ConsentUxUserSvc\_2ce51   65. Contenedor de Microsoft Passport   66. Control parental   67. Coordinador de transacciones distribuidas   68. Copias de seguridad de Windows   69. CoreMessaging   70. CredentialEnrollmentManagerUserSvc\_2ce51   71. Detección de hardware shell   72. Detección SSDP   73. DeviceAssociationBrokerSvc\_2ce51   74. DevicePickerUserSvc\_2ce51   75. DevicesFlowUserSvc\_2ce51   76. Diagnostic Execution Service   77. Directiva de extracción de tarjetas inteligentes   78. Disco virtual   79. Dispositivo host de UPnP   80. DLL de host del Contador de rendimiento   81. Energía   82. Enrutamiento y acceso remoto   83. Estación de trabajo   84. Eventos de adquisición de imágenes estáticas   85. Experiencia de calidad de audio y vídeo de Windows (qWave)   86. Experiencias del usuario y telemetría asociadas   87. Extensiones y notificaciones de impresora   88. Fax   89. Firewall de Windows Defender   90. Google Chrome Elevation Service (GoogleChromeElevationService)   91. GraphicsPerfSvc   92. Hora de la red de telefonía móvil   93. Hora de Windows   94. Host de proveedor de detección de función   95. Host de sistema de diagnóstico   96. Host del servicio de diagnóstico   97. Identidad de aplicación   98. Información de la aplicación   99. Iniciador de procesos de servidor DCOM   100. Inicio de sesión secundario   101. Instalador de ActiveX (AxInstSV)   102. Instalador de módulos de Windows   103. Instantáneas de volumen   104. Instrumental de administración de Windows   105. Interfaz de servicio invitado de Hyper-V   106. KTMRM para DTC (Coordinador de transacciones distribuidas)   107. Llamada a procedimiento remoto (RPC)   108. MessagingService\_2ce51   109. Microsoft App-V Client   110. Microsoft Passport   111. Modo incrustado   112. Módulos de creación de claves de IPsec para IKE y AuthIP   113. Mostrar el servicio de directivas   114. Motor de filtrado de base   115. Mozilla Maintenance Service   116. Net Logon   117. OneSyncSvc\_2ce51   118. OpenSSH Authentication Agent   119. OpenVPN Interactive Service   120. Optimización de distribución   121. Optimizar unidades   122. Partida guardada en Xbox Live   123. PimIndexMaintenanceSvc\_2ce51   124. Plug and Play   125. Preparación de aplicaciones   126. PrintWorkflowUserSvc\_2ce51   127. Programador de tareas   128. Propagación de certificados   129. Protección de software   130. Protocolo de autenticación extensible   131. Protocolo de resolución de nombres de mismo nivel   132. Proveedor de instantáneas de software de Microsoft   133. Publicación de recurso de detección de función   134. Reconoc. ubicación de red   135. Recopilador de eventos de Windows   136. Redirector de puerto en modo usuario de Servicios de Escritorio remoto   137. Registrador de configuración de Windows Connect Now   138. Registro de eventos de Windows   139. Registro remoto   140. Registros y alertas de rendimiento   141. Servicio Administrador de funcionalidad de acceso   142. Servicio Asistente para la compatibilidad de programas   143. Servicio AssignedAccessManager   144. Servicio AVCTP   145. Servicio biométrico de Windows   146. Servicio Cifrado de unidad BitLocker   147. Servicio de administración de aplicaciones de empresa   148. Servicio de administración de radio   149. Servicio de administración de Windows   150. Servicio de administrador de conexiones con servicios Wi-Fi Direct   151. Servicio de administrador de licencias de Windows   152. Servicio de almacenamiento   153. Servicio de Antivirus de Windows Defender   154. Servicio de asistente para perfil local   155. Servicio de asociación de dispositivos   156. Servicio de caché de fuentes de Windows   157. Servicio de cierre de invitado de Hyper-V   158. Servicio de compatibilidad con Bluetooth   159. Servicio de configuración de red   160. Servicio de configuración de traslación de IP   161. Servicio de datos del sensor   162. Servicio de datos espacial   163. Servicio de detección automática de proxy web WinHTTP   164. Servicio de directivas de diagnóstico   165. Servicio de dispositivo de interfaz humana   166. Servicio de enrutador de AllJoyn   167. Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos   168. Servicio de enumeración de dispositivos de tarjeta inteligente   169. Servicio de experiencia de idioma   170. Servicio de geolocalización   171. Servicio de Google Update (gupdate)   172. Servicio de Google Update (gupdatem)   173. Servicio de historial de archivos   174. Servicio de host HV   175. Servicio de implementación de AppX (AppXSVC)   176. Servicio de infraestructura de tareas en segundo plano   177. Servicio de inscripción de administración de dispositivos   178. Servicio de inspección de red de Antivirus de Windows Defender   179. Servicio de instalación de dispositivos   180. Servicio de instalación de Microsoft Store   181. Servicio de intercambio de datos de Hyper-V   182. Servicio de latido de Hyper-V   183. Servicio de licencia de cliente (ClipSVC)   184. Servicio de lista de redes   185. Servicio de mejora de visualización   186. Servicio de notificación de eventos de sistema   187. Servicio de Panel de escritura a mano y teclado táctil   188. Servicio de percepción de Windows   189. Servicio de perfil de usuario   190. Servicio de plataforma de dispositivos conectados   191. Servicio de Protección contra amenazas avanzada de Windows Defender   192. Servicio de protocolo de túnel de sockets seguros   193. Servicio de prueba comercial   194. Servicio de publicación de nombres de equipo PNRP   195. Servicio de puerta de enlace de audio de Bluetooth   196. Servicio de puerta de enlace de nivel de aplicación   197. Servicio de red de Xbox Live   198. Servicio de repositorio de estado   199. Servicio de sensores   200. Servicio de simulación de percepción de Windows   201. Servicio de sincronización de hora de Hyper-V   202. Servicio de solución de problemas recomendado   203. Servicio de supervisión de sensores   204. Servicio de transferencia inteligente en segundo plano (BITS)   205. Servicio de uso compartido de datos   206. Servicio de uso compartido de puertos Net.Tcp   207. Servicio de uso compartido de red del Reproductor de Windows Media   208. Servicio de virtualización de Escritorio remoto de Hyper-V   209. Servicio de virtualización de la experiencia de usuario   210. Servicio de Windows Insider   211. Servicio de zona con cobertura inalámbrica móvil de Windows   212. Servicio del iniciador iSCSI de Microsoft   213. Servicio del módulo de copia de seguridad a nivel de bloque   214. Servicio del sistema de notificaciones de inserción de Windows   215. Servicio enrutador de SMS de Microsoft Windows.   216. Servicio enumerador de dispositivos portátiles   217. Servicio FrameServer de la Cámara de Windows   218. Servicio host de proveedor de cifrado de Windows   219. Servicio Informe de errores de Windows   220. Servicio Interfaz de almacenamiento en red   221. Servicio Orquestador de actualizaciones   222. Servicio PowerShell Direct de Hyper-V   223. Servicio PushToInstall de Windows   224. Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)   225. Servicio Seguridad de Windows   226. Servicio telefónico   227. Servicio Volumetric Audio Compositor   228. Servicios de cifrado   229. Servicios de Escritorio remoto   230. Servidor   231. Shared PC Account Manager   232. Sistema de cifrado de archivos (EFS)   233. Sistema de eventos COM+   234. SMP de Espacios de almacenamiento de Microsoft   235. Solicitante de instantáneas de volumen de Hyper-V   236. SysMain   237. Tarjeta inteligente   238. Telefonía   239. Temas   240. Ubicador de llamada a procedimiento remoto (RPC)   241. UnistoreSvc\_2ce51   242. UserDataSvc\_2ce51   243. Uso de datos   244. VirtualBox Guest Additions Service   245. WalletService   246. WarpJITSvc   247. Windows Installer   248. Windows Search   249. Windows Update   250. Windows Update Medic Service   251. WpnUserService\_2ce51   252. Xbox Accessory Management Service |
|  |
|  |

## Detección, comprobación y evaluación de vulnerabilidades

|  |
| --- |
| Para cada servicio y/o aplicación en cada una de las máquinas • Si la máquina es un S.O. o un dispositivo móvil, hay que utilizar las herramientas vistas en cada una de las unidades (p.ej. vulskan, ZAP, Sqlmap) • Para servicios WEB se puede usar la metodología OWASP como vimos • También análisis generales como de denegación de servicio con Apache Benchmarking  **pfSense1 (#R1):**   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. Eso sí si están abiertos por la parte de la WAN hay que corregirlo. 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS) 3. Además, hubo una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense). **Se corrigió antes de hacer el análisis (nueva contraseña es “Lapatata87pocha”) y por lo tanto no se ha tenido en cuenta en el apartado 5.** 4. También hubo una vulnerabilidad, y es usar un certificado autofirmado para el webConfigurator de conexión segura. Este se ha resuelto mediante el paso a autoridad de certificación propia generada y difundida por nosotros y que los navegadores de esa red la importaran para confiar en dicha autoridad de certificación, y en el nuevo certificado de servidor para conexión firmado por ésta. **Se corrigió antes de hacer el análisis y por lo tanto no se ha tenido en cuenta en el apartado 5.**   **pfSense2 (#R2)**:   1. 53/tcp open domain Unbound -> Potencial vulnerabilidad de dejar un puerto innecesario abierto, con todo lo que conlleva. Hay que corregirlo 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS) 3. Además, hubo una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense). **Se corrigió antes de hacer el análisis (nueva contraseña es “junio2020”) y por lo tanto no se ha tenido en cuenta en el apartado 5.** 4. También hubo una vulnerabilidad, y es que el conectar al firewall para configurarlo no se hacía en conexión segura, por lo que se podría fácilmente interceptar el mensaje y obtener la contraseña y clave no cifradas. Por lo tanto, pasamos a SSL/TLS y generamos un certificado a de otra CA propia generada y difundida por nosotros y que los navegadores de esa red la importaran para confiar en dicha autoridad de certificación, y en el nuevo certificado de servidor para conexión firmado por ésta. **Se corrigió antes de hacer el análisis y por lo tanto no se ha tenido en cuenta en el apartado 5.**   **ClienteRemoto** **(#LANB1**):   1. Microsoft Windows RPC - (HAY VULNERABILIDADES CON ESTO, PROGRESAD CON EL SW) 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. Windows 7)   **Servidor (#LANB2):**   1. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. Windows 10) |

## Medidas específicas de corrección

|  |
| --- |
| • De las vulnerabilidades descubiertas en el apartado anterior, cuales se corrigen y por qué. • Y cuales no y por qué  **• En la entrega que se haga YA deben estar corregidas**  **pfSense1 (#R1):**   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. Eso sí si están abiertos por la parte de la WAN hay que corregirlo. 2. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **pfSense2 (#R2)**:   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. Eso sí si están abiertos por la parte de la WAN hay que corregirlo. 2. ***53/tcp open domain Unbound*** -> Nuestra empresa no necesita que se empleen servicios DNS de momento, por lo que dejar este puerto abierto es innecesario y podría llevar a vulnerabilidades. En una red real se podría dejar abierto si usásemos servidores DNS, eso sí. Hay que corregirlo 3. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **ClienteRemoto** **(#LANB1**):   1. ***Microsoft Windows RPC:*** las interfaces MSRPC pueden usarse por un atacante para recolectar información importante y comprometer servidores (p.ej. robar la contraseña de la VPN y colarse). Se deben cerrar los puertos **135,**  **49152,** **49153,** **49154,** **49155,** **49156,** **49157**. Hay que corregirlo 2. ***5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)*** -> 1º el cliente que sepamos no necesita esto. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. Hay que corregirlo 3. **139**/tcp open netbios-ssn Microsoft Windows netbios-ssn -> Servicio empleado por RPC, si es posible debería cerrarse el puerto. Hay que corregirlo 4. **445**/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) -> Nuestro cliente remoto se supone que no debe tener un “grupo de trabajo” fuera de acceder a nuestra VPN. Cerrar puerto si es posible. Hay que corregirlo 5. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **Servidor (#LANB2):**   1. **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) -> 1º es una versión más antigua de HTTP que la empleada para la versión actual de nuestro servidor, que solo debe hacer lo mínimo pedido. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. Hay que corregirlo 2. (lista de vulnerabilidades, indicando si se corrige o no y por qué) |

## Recomendaciones sobre implantación de medidas preventivas.

Entrenar a nuestros trabajadores en medidas de seguridad, entre ellas no dejar la contraseña de usuario por ahí ni dejarla grabada, tratar de mantener su SW y HW actualizado, y tener mucho cuidado con la instalación de SW de terceros, a ser posible no instalarlo (pues, por ejemplo, en servicios de mensajería y especialmente en servicios móviles, los mensajes enviados se suelen guardar en una base de datos local del dispositivo que, dependiendo del algoritmo de cifrado empleado, podría ser descifrado). Esta última medida debería ser notificada a nuestros clientes también para que tengan cuidado en las redes móviles.

En cuanto a los dispositivos móviles, recomendaríamos que se siguieran algunos de los preceptos de seguridad en dispositivos móviles de mensajería instantánea (Centro Criptológico Nacional, 2021):

1. *Mantener el teléfono bloqueado. De esta forma, se reducirá el riesgo si el dispositivo cae en las manos equivocadas.*
2. *Sería recomendable eliminar las previsualizaciones de los mensajes y extremar las medidas cuando no se disponga del teléfono al alcance.*
3. *En la medida de lo posible, se recomienda la configuración de las aplicaciones para solo recibir mensajes de personas autorizadas.*
4. *Desactivar la conectividad adicional del teléfono cuando no se vaya a utilizar, como podría ser la conexión WiFi o Bluetooth, ya que además de reducir el consumo de batería, reduce la posible superficie de ataque sobre el dispositivo.*
5. *Utilizar aplicaciones de mensajería instantánea cuyo código fuente esté abierto a la comunidad y haya sido revisado. En ese sentido existen alternativas que, además, aseguran la confidencialidad en las comunicaciones, cifrando el tráfico extremo a extremo (e2e).*

Dejar los sistemas cerrados bajo llave (contraseña electrónica y llave física) dentro de una habitación con sistema de refrigeración y medidas anti-incendios, y filtros de aire (más una cámara de presión positiva) para prevenir polvo e insectos dentro de la cámara, con una trampa de luz ultravioleta para eliminar cualquier posible insecto que se cuele. El servidor debería estar desplegado en el edificio de la empresa, para mayor seguridad. Y tener cámaras con reconocimiento facial y otros métodos de seguridad biométrica.

También deberíamos añadir redundancias como medida extra en caso de caída o fallo (p. ej. backup de la BBDD, múltiples switches, generadores de emergencia) pero no lo hemos implementado porque o bien no se podían simular en máquina virtual, o se podrían simular pero a riesgo de falta de memoria (p.ej: un ordenador teniendo que soportar la red básica más los backups).

El control de acceso debería ser distribuido, de tal forma que dar privilegios más altos a alguien requiera de la colaboración de todos los administradores, para complicar corrupción permitiendo accesos maliciosos al sistema.

Para mejorar seguridad comunicaciones móviles, usaríamos la mejor encriptación, WPA3, y no escribas las contraseñas, y no hablar de los clientes públicamente ni de nada relacionado con las seguridad (nada fuera del entorno laboral). También los dispositivos móviles deberían tener una doble verificación de sistema biométrico y contraseña, y no estar rooteados. De hecho para mayor seguridad los móviles corporativos deberían resetearse cada mes para asegurarse de que no están rooteados.

Además como protección extra frente a alguien logrando robar credenciales de la VPN y acceder, deberíamos añadir un segundo firewall detrás del primero para evitar que alguien empleara el servicio VPN para mandar paquetes a servicios previamente inaccesibles; pero no lo hemos resuelto porque nos han pedido no alterar la infraestructura.

(Esta imagen de abajo es por referencia, no incluirla en la memoria final)Tabla

Descripción generada automáticamente)

# REFERENCIAS

Centro Criptológico Nacional. (1 de 3 de 2021). *https://www.ccn-cert.cni.es*. Obtenido de Centro Criptológico Nacional: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html

Sánchez, B. B. (1 de 5 de 2022). *moodle.* Obtenido de Enunciado y propuesta Segundo Parcial: https://moodle.upm.es/titulaciones/oficiales/pluginfile.php/9386654/mod\_resource/content/3/Enunciado%20y%20propuesta%20Segundo%20parcial.pdf

WunderTech. (8 de 06 de 2022). *WunderTech*. Obtenido de WunderTech: https://www.youtube.com/watch?v=cxhIpmov4TY