Tecnológico de Monterrey

Índice

I Introducción

Aunque la tecnología ha mostrado ser un parteaguas en la manera en que se vive y experimenta la vida, esta ha avanzado a pasos agigantados y, con ello, ha traído una serie de retos, amenazas y riesgos. Según un informe de la empresa de ciberseguridad Norton LifeLock, en 2020 se registraron, a nivel mundial, más de 4,000 millones de datos comprometidos [Norton, 2020]. En este sentido, la importancia de la ciberseguridad se presenta; la protección de datos sensibles y confidenciales, tanto de empresas como de personas, es esencial. Esto implica implementar medidas de seguridad para prevenir el acceso prohibido a la información, así como encontrar posibles vulnerabilidades y lograr parcharlas.

Por otro lado, en México, una PyME se define como una empresa con menos de 250 empleados y un volumen de ventas anual que no excede los 100 millones de pesos mexicanos. La Asociación de Emprendedores de México (ASEM) destaca que las PyMEs se caracterizan por su tamaño reducido, su independencia de la propiedad y una gestión poco estructurada [ASEM, 2021]. Por otro lado, la Cámara Nacional de Comercio, Servicios y Turismo de la Ciudad de México (CANACO) enfatiza que las PyMEs tienen una estructura organizativa sencilla, un ámbito de actuación local o regional y una capacidad limitada de producción y comercialización en comparación con las grandes empresas [CANACO, 2021]. A pesar de sus limitaciones, las PyMEs son un pilar fundamental de la economía mexicana, representando la mayoría de las empresas registradas en el país y generando una gran cantidad de empleo en el sector privado. [Economia, 2021]

Desde un punto de vista más optimista, con la búsqueda de seguridad surgen soluciones que simplifican el proceso de mejora en la red. Una opción que ofrece un periodo de prueba de 14 días, y que será utilizada en el futuro para hacer un análisis de las vulnerabilidades de la red de la PyME, es Nessus. Esta aplicación fue desarrollada por Tenable y es capaz de detectar y analizar una amplia variedad de susceptibilidades en dispositivos y sus sistemas operativos, y, al finalizar, proporciona informes detallados sobre los hallazgos.

II Sobre La PyME

Durante el análisis de vulnerabilidades, se busca otorgar una solución con el objetivo de robustecer el sistema interno de la PyME elegida. Esta empresa es llamada "Innovadora de la Educación" y está a cargo de varios colegios que llevan por nombre "Instituto Bilingue la Silla". Esta institución educativa abarca los niveles formativos desde la educación maternal hasta la educación secundaria. El organismo cuenta actualmente con dos campus en Monterrey, uno ubicado

en Distrito Tec y el segundo en Sierra Alta. Entre ambos campus se cuenta con aproximadamente 1,200 alumnos inscritos.

Las oficinas generales de la institución se encuentran en Distrito Tec, y fue ahí donde fuimos recibidos para encontrar algunas vulnerabilidades en su sistema. Considerando que este establecimiento tiene un aproximado de 15 empleados, el presupuesto con el que contaban para hacer la mejora de las vulnerabilidades era muy bajo, de $15,000; por lo que las soluciones que se buscan deben de ser asequibles y concretas.

III Importancia de la seguridad y detalles de los datos

Tras conocer un poco el contexto general de la institución, se busca ahondar un poco más en el tipo de información que se maneja en las oficinas centrales y la importancia de salvaguardarla. En los dispositivos electrónicos utilizados dentro de las oficinas se maneja información bastante sensible, podemos encontrar información financiera, como lo son los ingresos y egresos de la institución, o también la información personal de los empleados y de las familias que forman parte de la institución. La organización es bastante celosa de su información, principalmente de la información personal de cada familia y colaboradores que forman parte de la escuela.

Para ser más específicos, a la institución no le agradaría que la información que tienen sobre sus integrantes se filtre ya que podemos encontrar datos como lo podrían ser nombres, direcciones, ingresos mensuales, cuentas bancarias, información sobre salud mental, divorcios y defunciones, entre otro tipo de antecedentes de cada familia. Además, los reportes financieros de la institución son información clasificada, nadie más que el contador de la institución y algún directivo debería tener acceso a estos estados de cuenta para poder hacer las declaraciones anuales. Por esta misma razón, debemos mantener los datos bajo custodia y manejarlos con mucho cuidado, debemos buscar las vulnerabilidades más peligrosas en los dispositivos de la organización para que ningún cibercriminal pueda robar o secuestrar estos datos y poner en peligro la integridad de la escuela como la de sus colaboradores. Al estar conscientes de lo anterior, antes de iniciar con el proceso de investigación se brindó un documento de confidencialidad para que ambas partes estuvieran de acuerdo con la responsabilidad que esto llevaba.

IV Análisis de Vulnerabilidades

4.1 Detalles del sistema y vulnerabilidades críticas

Antes de iniciar a realizar el análisis de vulnerabilidades con la plataforma de Nessus, pedimos a las oficinas un breve reporte de los dispositivos que estaban conectados a la red de internet. Nos comentaron que tienen, aproximadamente:

- 10 computadoras portátiles con sistema operativo Windows

- 1 computadora portátil de marca Apple
- 2 computadoras de escritorio de con sistema operativo Windows
- 4 impresoras de marca Xerox
- Los teléfonos personales de cada empleado, además de relojes y otros dispositivos.

Aunque la PyME nos brindó la información de los dispositivos físicos ubicados en las oficinas, nos dió un cuarto en donde estar y no nos permitió explorar nada más. Por lo tanto, ni la información exacta de para qué se utiliza cada dispositivo, ni sus direcciones IP, están presentes en el reporte. Sin embargo, la topología de la red se muestra a continuación:

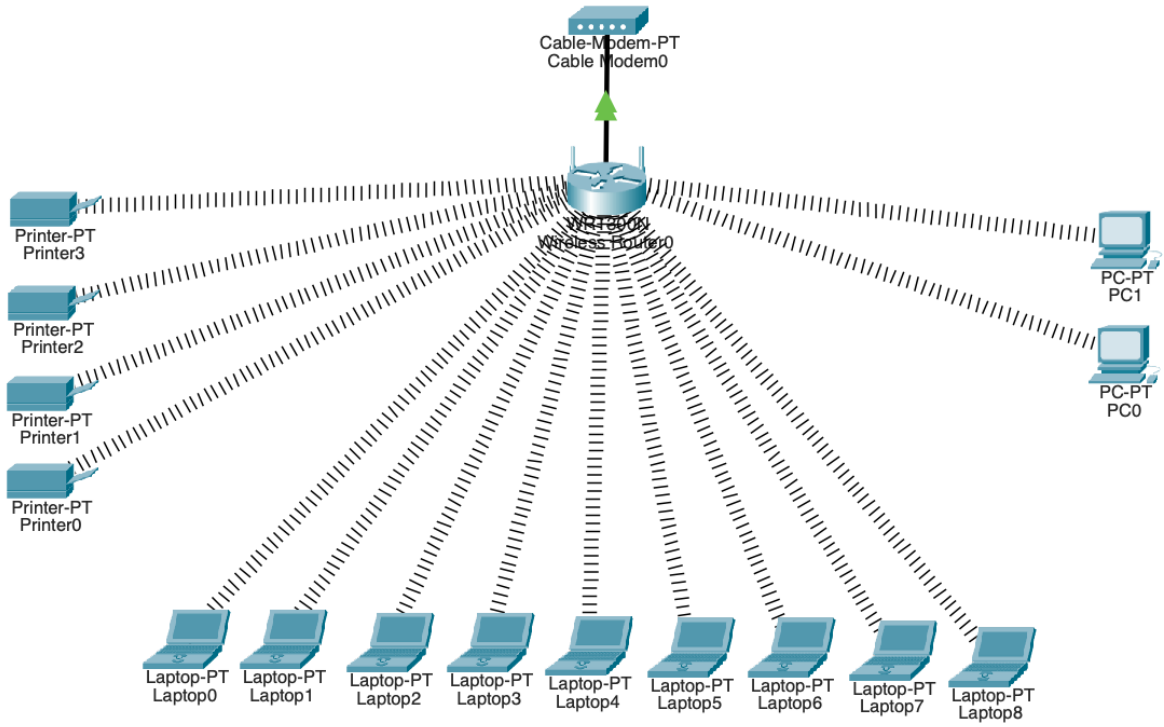

Figura 1: Topología tentativa de red de la PyME.
Realizada con Packet Tracer

También, algo que es importante aclarar antes de explorar los resultados obtenidos con el programa es que, al no contar con una licencia profesional, nos limitó a 16 direcciones de IP diferentes, entonces, varios de los dispositivos mencionados anteriormente no se encontrarán presentes en el siguiente desglose. De las 77 vulnerabilidades que Nessus encontró, el 13% son de nivel crítico, 10% de nivel alto, 6% de nivel medio, 2% de nivel bajo y el 69% pertenece a la categoría 'info'.

A continuación se enlistan las 9 peores vulnerabilidades encontradas:

	Vulnerabilidad	Puntuación de peligro	Hosts	CVE
1.	SSL Version 2 and 3 Protocol Detection	9.8	192.168.14.10 192.168.14.11 192.168.14.87 192.168.14.2	N/A
2.	Security Update for Microsoft Visual Studio Code (January 2023)	7.8	192.168.14.58	CVE-2023-21779
3.	SSL Certificate Signed Using Weak Hashing Algorithm	7.5	192.168.14.11 192.168.14.10 192.168.14.87 192.168.14.2	CVE-2004-2761
4.	SMB NULL Session Authentication	7.3	192.168.14.72	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117
5.	IP Forwarding Enabled	6.5	192.168.14.1	CVE-1999-0511
6.	DHCP Server Detection	3.3	192.168.14.1	N/A
7.	Apple Mac OS X (Multiple Issues)	9.8 - 3.7	192.168.14.58	Varios
8.	Microsoft Windows (Multiple Issues)	10 - 8.1	192.168.14.87 192.168.14.2	N/A
9.	Apache Httpd (Multiple Issues)	9.8 - 7.5	192.168.14.58	CVE-2021-34798 CVE-2021-39275

Figura 2: Vulnerabilidades encontradas por Nessus

4.2 Especificaciones sobre las vulnerabilidades

"El puntaje CVSS (Common Vulnerability Scoring System) es un sistema de puntuación estándar que se utiliza para evaluar la gravedad de las vulnerabilidades de seguridad informática" (IBM, 2023). Su objetivo es proporcionar un número del 1 al 10 que indica el nivel de riesgo en particular, este resultado se basa en la complejidad de la vulnerabilidad, la importancia del activo afectado y el impacto potencial en la confidencialidad, integridad y disponibilidad de los datos, entre otros.

Por otro lado, el CVE es un diccionario de vulnerabilidades de seguridad que brinda un identificador único a cada posible problema que identifica. [Corporation, 2021] El objetivo es contar con una lista actualizada de vulnerabilidades conocidas, lo que facilita la mitigación e identificación de los problemas de una manera más sencilla, así como mejorar la comunicación entre diferentes equipos de seguridad, por ser un lenguaje mundial. Entonces, las vulnerabilidades encontradas, explicadas de una manera más profunda:

1. **SSL Version 2 and 3 Protocol Detection**

   - **Significado:** La versión del Secure Sockets Layer (SSL) utilizado para crear un enlace encriptado entre la escuela y sus clientes, utiliza un protocolo para encriptar con vulnerabilidades conocidas. Siendo susceptible a un ataque de intermediario.
   - **Importancia:** Encontrar una solución para la vulnerabilidad debería de estar en las prioridades más altas de la escuela ya que a través de este enlace se comunica una gran cantidad de información familiar sensible, desde sus salarios a reportes de su salud. Los clientes le están confiando estos datos a la organización y sería un gran problema si esta información es desencriptada y robada por un tercero.
   - **Posible Solución:** La solución recomendada es deshabilitar el uso de este SSL en la aplicación que la organización está utilizando. Este puede ser reemplazado por Transport Layer Security (TLS) 1.2 o mayor; el cual tiene métodos de cifrado seguros.
   - **CVSS:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H descompuesto
     - **CVSS:3.0:** Indica que se está utilizando la versión 3.0 del sistema de puntuación CVSS.
     - **AV:L:** Indica que el atacante necesita tener acceso a la red o al sistema para explotar la vulnerabilidad (Access Vector = Local).
     - **AC:L:** Indica que el atacante necesita tener acceso a una cuenta en el sistema para explotar la vulnerabilidad (Access Complexity = Low).
     - **PR:N:** Indica que no se requiere autenticación del usuario para explotar la vulnerabilidad (Privileges Required = None).
     - **UI:R:** Indica que la explotación de la vulnerabilidad requiere la interacción del usuario, por ejemplo, haciendo clic en un enlace malicioso (User Interaction = Required).
     - **S:U:** Indica que la confidencialidad de la información se ve afectada por la vulnerabilidad, pero no la integridad ni la disponibilidad (Scope = Unchanged).
     - **C:H:** Indica que la vulnerabilidad puede tener un impacto crítico en la confidencialidad de la información (Confidentiality = High).
     - **I:H:** Indica que la vulnerabilidad puede tener un impacto crítico en la integridad de la información (Integrity = High).
     - **A:H:** Indica que la vulnerabilidad puede tener un impacto crítico en la disponibilidad del sistema o la información (Availability = High)
   - En resumen, la vulnerabilidad es crítica porque tiene un alto impacto en disponibilidad de la información, integridad y confidencialidad, también, solo se requiere acceso a la red o al sistema para explotarla.

2. **Actualización de Softwares**:

   Security Update for Microsoft Visual Studio Code (January 2023)
   Apple Mac OS X (Multiple Issues) - macOS 11.x <11.6.3 Multiple Vulnerabilities
   Microsoft Windows (Multiple Issues) - Unsupported Windows OS (remote)
   Apache Httpd (Multiple Issues) - Apache <2.4.49 Multiple Vulnerabilities

   - **Significado:** Las 4 vulnerabilidades mencionan una falta de actualización de aplicaciones o del sistema operativo del dispositivo que la presenta. Para la primera, la versión del programa Visual Studio Code que corre el dispositivo actual (Mac con IP de 192.168.14.58) no es el más actualizado. Actualmente está instalada la 1.73.1 y la más reciente es la 1.74.3. Para la segunda, el sistema operativo de la computadora (Mac con IP de 192.168.14.58) no es el más reciente, esta tiene instalada la versión 11.5.2 y la más reciente es la macOS Big Sur 11.6.3. Para la tercera vulnerabilidad, se encontró que en dos dispositivos diferentes (Windows con IP de 192.168.14.87 y 192.168.14.2), la versión de Windows 7 no estaba instalada correctamente, pues faltaba un paquete o no era compatible con las computadoras. Finalmente, la cuarta vulnerabilidad dice que la versión de Apache Httpd instalada en la computadora del host es la 2.4.46, cuando la más reciente es la 2.4.49.
   - **Importancia:** Además de que las versiones más recientes de los programas muestran una mejor funcionalidad y compatibilidad, para la parte de seguridad cibernética las actualizaciones de software suelen incluir correcciones de nuevas vulnerabilidades y amenazas que han sido encontradas. Al no contar con la versión más reciente, es posible ser víctima de un ataque cibernético y malware.
   - **Posible solución:** Aunque la solución más lógica es actualizar la aplicación, descubrimos que en las oficinas de la PyME no utilizan Visual Studio Code. Por lo tanto, para este escenario específico la solución más óptima es eliminar la aplicación. De tal manera se liberaría espacio y posibles ventanas de ataques en un futuro. Para las demás vulnerabilidades, la recomendación es dar una capacitación a los empleados de la razón por la que mantener un a computadora en el sistema operativo más reciente es esencial, para así salvaguardar la integridad de la empresa.
   - **CVSS:** CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H descompuesto:
     - **CVSS:3.0:** Indica que se está utilizando la versión 3.0 del sistema de puntuación CVSS.
     - **AV:L:** Indica que el atacante necesita tener acceso a la red o al sistema para explotar la vulnerabilidad (Access Vector = Local).
     - **AC:L:** Indica que el atacante necesita tener acceso a una cuenta en el sistema para explotar la vulnerabilidad (Access Complexity = Low).

  - **PR:N:** Indica que no se requiere autenticación del usuario para explotar la vulnerabilidad (Privileges Required = None).
  - **UI:R:** Indica que la explotación de la vulnerabilidad requiere la interacción del usuario, por ejemplo, haciendo clic en un enlace malicioso (User Interaction = Required).
  - **S:U:** Indica que la confidencialidad de la información se ve afectada por la vulnerabilidad, pero no la integridad ni la disponibilidad (Scope = Unchanged).
  - **C:H:** Indica que la vulnerabilidad puede tener un impacto crítico en la confidencialidad de la información (Confidentiality = High).
  - **I:H:** Indica que la vulnerabilidad puede tener un impacto crítico en la integridad de la información (Integrity = High).
  - **A:H:** Indica que la vulnerabilidad puede tener un impacto crítico en la disponibilidad del sistema o la información (Availability = High)
- En resumen, la vulnerabilidad es crítica porque tiene un alto impacto en disponibilidad de la información, integridad y confidencialidad, también, solo se requiere acceso a la red o al sistema para explotarla.

3. **SSL Certificate Signed Using Weak Hashing Algorithm**

- **Significado:** Un certificado SSL se encarga de establecer una conexión segura y encriptada entre un servidor web y el navegador del cliente. Este incluye información sobre el dominio del sitio web, la clave pública del servidor y la firma digital de la Autoridad de Certificación que emitió el certificado. Un algoritmo de Hash débil tiene debilidades conocidas que pueden ser explotadas por atacantes para comprometer la integridad del certificado, así, se podría crear uno que pareciera legítimo, permitiendo una intercepción de información confidencial transmitida entre servidor y cliente.
- **Importancia:** Arreglar esta vulnerabilidad es esencial, pues, si el certificado SSL es modificado por un atacante, puede llevar a la exposición de información confidencial como contraseñas, datos sobre tarjetas de crédito, información personal, etc. Además, se podrían utilizar estos certificados falsos para realizar, con éxito, ataques de phishing y engañar a los usuarios para que proporcionen información importante o instalen malware en sus dispositivos.
- **Posible Solución:** Primero que nada, es importante actualizar los certificados SSL, asegurándose de usar algoritmos hash seguros, como el SHA-256 o superior. También, es recomendable revocar los certificados antiguos o inseguros, reduciendo la posibilidad de un posible ataque. Finalmente, utilizar herramientas de análisis de vulnerabilidades, como Nessus, mínimo una vez al mes, para estar al tanto del estatus de la seguridad de los dispositivos conectados a la red.

- **CVSS:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N descompuesto:
  - **CVSS:3.0:** Indica que se está utilizando la versión 3.0 del sistema de puntuación CVSS.
  - **AV:N:** Indica que el atacante no necesita acceso a la red o al sistema para explotar la vulnerabilidad (Access Vector = Network).
  - **AC:L:** Indica que el atacante necesita tener acceso a una cuenta en el sistema para explotar la vulnerabilidad (Access Complexity = Low).
  - **PR:N:** Indica que no se requiere autenticación del usuario para explotar la vulnerabilidad (Privileges Required = None).
  - **UI:N:** Indica que la explotación de la vulnerabilidad no requiere la interacción del usuario (User Interaction = None).
  - **S:U:** Indica que la confidencialidad de la información se ve afectada por la vulnerabilidad, pero no la integridad ni la disponibilidad (Scope = Unchanged).
  - **C:N:** Indica que la vulnerabilidad no tiene impacto en la confidencialidad de la información (Confidentiality = None).
  - **I:H:** Indica que la vulnerabilidad puede tener un impacto alto en la integridad de la información (Integrity = High).
  - **A:N:** Indica que la vulnerabilidad no tiene impacto en la disponibilidad del sistema o la información (Availability = None).
- En resumen, en este caso se tiene un impacto alto en la integridad de la información, pero no afecta a la confidencialidad ni a la disponibilidad. Por otro lado, el atacante no necesita interacción con el usuario ni acceso al sistema para explotar la vulnerabilidad.

4. **SMB NULL Session Authentication**

- **Significado:** El equipo correspondiente a la dirección IP 192.168.14.72 está corriendo una versión de sistema operativo que permite acceso a ciertas operaciones o archivos sin autenticación (sin pedir usuario o contraseña). SMB se refiere a un protocolo de intercambio en una red de archivos o dispositivos periféricos, y en este caso se detectó que es posible autenticarse en una instancia de este protocolo sin credenciales.
- **Importancia:** Es posible que un atacante aproveche esta vulnerabilidad para obtener acceso a archivos del equipo, para obtener información confidencial o incluso en algunos casos hacer que el sistema falle.
- **Posible Solución:** Dependiendo del sistema operativo, es posible establecer manualmente el acceso a los archivos compartidos en el equipo y asegurarse de que solo sean compartidos con usuarios aprobados, o ya bien dejar de compartir esos archivos.
- **CVSS:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L descompuesto:

  - **CVSS:3.0:** Indica que se está utilizando la versión 3.0 del sistema de puntuación CVSS.
  - **AV:N:** Indica que el atacante no necesita acceso a la red o al sistema para explotar la vulnerabilidad (Access Vector = Network).
  - **AC:L:** Indica que el atacante necesita tener acceso a una cuenta en el sistema para explotar la vulnerabilidad (Access Complexity = Low).
  - **PR:N:** Indica que no se requiere autenticación del usuario para explotar la vulnerabilidad (Privileges Required = None).
  - **UI:N:** Indica que la explotación de la vulnerabilidad no requiere la interacción del usuario (User Interaction = None).
  - **S:U:** Indica que la confidencialidad de la información se ve afectada por la vulnerabilidad, pero no la integridad ni la disponibilidad (Scope = Unchanged).
  - **C:L:** Indica que la vulnerabilidad tiene un impacto bajo (pérdida limitada) en la confidencialidad de la información (Confidentiality = Low).
  - **I:L:** Indica que la vulnerabilidad tiene un impacto bajo (pérdida limitada) en la integridad de la información (Integrity = Low).
  - **A:L:** Indica que la vulnerabilidad tiene un impacto limitado en la disponibilidad del sistema o la información (Availability = Low)

- En resumen, mediante esta vulnerabilidad sería posible que un atacante obtuviera información sensible en el equipo afectado, comprometiendo la confidencialidad de esta. No obstante, no se vería afectada la integridad o la disponibilidad de la información. Esta vulnerabilidad presenta un alto riesgo para información sensible o confidencial.

5. **IP Forwarding Enabled**

- **Significado:** El host remoto tiene habilitada la opción de reenvío de IP, sistema que se utiliza para aceptar y posteriormente retransmitir información y paquetes recibidos por un medio físico.
- **Importancia:** Mientras el host remoto no sea un router, un atacante puede aprovechar este reenvío de información para enrutar ciertos paquetes evitando firewalls y filtros NAC, que en general, son sistemas encargados de proteger redes de tipo privadas.
- **Posible Solución:** Si se comprueba que el host remoto no es un router, se debe deshabilitar esta opción, ejecutando ciertos comandos:
  - Para Windows: echo 0 > /proc/sys/net/ipv4/ip_forward
  - Para MacOS X: sysctl -w net.inet.ip.forwarding=0
  - Para Linux: echo 0 > /proc/sys/net/ipv4/ip_forward

- **CVSS:** CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L descompuesto:
  - **CVSS:3.0:** Indica que se está utilizando la versión 3.0 del sistema de puntuación CVSS.
  - **AV:A:** Indica que el atacante necesita tener acceso al dominio de difusión para explotar la vulnerabilidad (Access Vector = Adjacent).
  - **AC:L:** Indica que el trabajo que cuesta hacer el ataque es bajo, no representa ninguna dificultad (Access Complexity = Low).
  - **PR:L:** Indica que se requiere autenticación del usuario para explotar la vulnerabilidad (Privileges Required = Low).
  - **UI:N:** Indica que la explotación de la vulnerabilidad no requiere la interacción del usuario, es decir, que se activa sólo (User Interaction = None).
  - **S:C:** Indica que la confidencialidad de la información se ve afectada por la vulnerabilidad, y que sus efectos alcanzan a aquellos con los que interactúa (Scope = Changed).
  - **C:L:** Indica que la vulnerabilidad tiene un impacto bajo (pérdida limitada) en la confidencialidad de la información (Confidentiality = Low).
  - **I:L:** Indica que la vulnerabilidad tiene un impacto bajo (pérdida limitada) en la integridad de la información (Integrity = Low).
  - **A:L:** Indica que la vulnerabilidad tiene un impacto limitado en la disponibilidad del sistema o la información (Availability = Low)
- En resumen, aunque esta vulnerabilidad está catalogada como de gravedad media, es de suma importancia corregirla pues se estaría viendo afectada directamente información sensible y de una manera bastante sencilla.

6. **DHCP Server Detection**

- **Significado:** El DHCP, Protocolo de Configuración Dinámica de Host, se encarga de asignar automáticamente direcciones IP a los dispositivos de la red. Para esto, este servidor cuenta con información importante y confidencial, como lo podrían ser la lista de servidores web, información sobre el diseño de la red o sobre los dominios, la cual, se puede ver expuesta.
- **Importancia:** Aunque es una vulnerabilidad de baja importancia y no representa un riesgo mayor, un atacante podría acceder a esta información y por ende, conocer bien la red.
- **Posible Solución:** Se recomienda mantener información de este tipo fuera de la red, o filtrarla, para eliminar lo que no es importante.
- **CVVS:** CVSS2AV:A/AC:L/Au:N/C:P/I:N/A:N descompuesto:

  - **CVSS2:** Indica que se está utilizando la versión v2 del sistema de puntuación CVSS.
  - **AV:A:** Indica que el atacante necesita tener acceso al dominio de difusión para explotar la vulnerabilidad (Access Vector = Adjacent).
  - **AC:L:** Indica que el trabajo que cuesta hacer el ataque es bajo, no representa ninguna dificultad (Access Complexity = Low).
  - **Au:N:** Indica que el atacante no necesita autenticarse para explotar la vulnerabilidad (Authentication = None)
  - **C:P:** Indica que la vulnerabilidad tiene un impacto parcial (considerable exposición de la información) en la confidencialidad de la información (Confidentiality = Partial).
  - **I:N:** Indica que no existe impacto en la integridad de la información (Integrity = None).
  - **A:N:** Indica que no existe impacto en la disponibilidad del sistema o la información (Availability = None)

- En resumen, no se ve vulnerada información importante, pero se recomienda prestar atención a esta inseguridad para evitar posibles ataques en un futuro.

V Plan de Análisis de las Vulnerabilidades

Tras haber realizado el análisis de vulnerabilidades que el Instituto Bilingüe la Silla tiene dentro de sus oficinas generales, el siguiente paso es elaborar un plan de análisis para corregirlas, evitando así posibles ataques en un futuro. El plan de análisis se encuentra desglosado por grupos de fallas para facilitar el proceso de explicación, pero cada vulnerabilidad se tratará de forma individual al implementar la solución a la PyME. Dentro de la empresa se encontraron vulnerabilidades que oscilan entre simplemente actualizar sistemas operativos, hasta problemas más complejos como hacer actualizaciones a los TLS para parchear errores con los SSL. Las vulnerabilidades están desglosadas a continuación con sus respectivas soluciones.

1. **Vulnerabilidades referentes a una falta de actualización de aplicaciones y sistemas operativos: Microsoft Visual Studio Code, macOS 11.5.2, Windows 7, y Apache Httpd 2.4.49**

   Cuando se habla de los softwares de los equipos en una empresa, se está abordando un tema muy importante. Aunque probablemente no se le da la relevancia que realmente tiene, tener aplicaciones en desuso o software no actualizado es una situación de mucha vulnerabilidad [Schneier, 2000]. Como organización, se debe contar con un proceso de gestión de cambios eficaz, e implementarlo, para evitar daños que pueden llegar hasta pérdidas de sistemas y

datos. Aunque las principales compañías de software (como las de este caso) notifican sobre las nuevas actualizaciones, depende de nosotros el aceptarlas y darles continuidad, a menos que se tengan habilitadas las actualizaciones automáticas (altamente recomendado). Independientemente del mecanismo que se esté utilizando, es necesario seguir haciendo backups de los datos periódicamente y tenerlos almacenados en lugares distintos, pues nadie está exento de un ataque de este tipo [Laudon and Laudon, 2016]. Aunado a esto, es imprescindible que todos los empleados estén totalmente conscientes de su responsabilidad al utilizar alguno de estos dispositivos en materia de seguridad, pues muchas veces esta información no es divulgada, y al desconocer sobre el tema, se cae en el uso incorrecto de los servicios y en no darles mantenimiento. Una posible solución a este problema es tener un propio equipo de TI, que al tratarse de una PyME, no es necesario que sea muy grande, para que no sea necesario invertir tanto. Así habrá personal consciente de estos temas y encargados de darles el correcto seguimiento [Van der Aalst and Van Hee, 2002].

2. **IP Forwarding Enabled**

   Tener habilitada la opción de reenvío de IP puede ser un arma de doble filo. Esta herramienta permite que algún dispositivo remoto se conecte de forma directa a nuestro equipo, posibilitando la opción de transmitir información. Aunque parece un medio atractivo pues se puede tener acceso directo a otros dispositivos de la misma organización, también se le están dejando las puertas abiertas a atacantes que las pueden aprovechar para acceder a ellas [Hu et al., 2020]. De hecho, uno de los primeros pasos que realizan los ciberdelincuentes antes de atacar es analizar los puertos, pues así sabrán qué nivel de seguridad tienen, cuáles redes son las más vulnerables, entre otros. Para abordar este problema, existen analizadores de puertos que nos permiten saber exactamente qué puertos están abiertos, sus direcciones, sus niveles de seguridad y si pueden o no recibir datos 2018penetration

   Sin embargo, también es necesario remarcar que estos análisis los pueden llevar a cabo personas de TI con buenas intenciones, o también atacantes, para encontrar puertas abiertas y explotarlas. Existen diferentes técnicas para llevar a cabo este análisis de puertos, como por ejemplo: 'Análisis de ping', que se encarga de mostrar si un paquete puede distribuirse a una dirección IP sin presentar errores, 'Análisis semiabiertos', que sirven para saber el estado de un puerto sin completar la conexión, y, finalmente, 'Análisis XMAS', un análisis sumamente silencioso para conocer la protección y cortafuegos de una red [Tan et al., 2020]. Después de que la PyME lleve a cabo este análisis de puertos, se podrá definir si es necesario deshabilitar alguno de ellos o bloquear su acceso a externos instalando cortafuegos, sin dejar de minimizar al máximo la cantidad de puertos abiertos para reforzar su propia seguridad.

3. **DHCP Server Detection**

   El protocolo de configuración dinámica de host sirve para proporcionar una dirección IP a

cada participante en la red, simplificando la administración de la misma, sin embargo, al hacer esto se le abre el acceso a la red a los atacantes. Esta vulnerabilidad se conoce como 'DHCP Spoofing'. Básicamente, este protocolo no utiliza ningún método de autenticación, permitiendo que cualquier dispositivo pueda tener acceso. Así, se pueden enviar mensajes con direcciones falsificadas engañando a otros clientes en la red [Al-Dulaimi et al., 2017].

Un método para combatir esta vulnerabilidad es el 'DHCP Snooping', que aunque no bloquea totalmente al DHCP Spoofing, sí bloquea los servidores de DHCP malicioso o no autorizados, y protege la red mitigando el impacto de los ataques de suplantación de identidad [Nguyen et al., 2017]. Para configurar el DHCP Snooping y empezar a utilizarlo es necesario habilitar esta opción en el switch y configurar las interfaces de red que aceptan tráfico DHCP, razones por las cuales ésto no representaría un costo a la PyME, sólo es necesario contar con personal capacitado en el tema.

4. **SSL Version 2 and 3 Protocol Detection**

   De igual forma, en el reporte anterior describimos otra vulnerabilidad encontrada, la de SSL Version 2 and 3 Protocol Detection, mencionamos que la variante del Secure Sockets Layer (SSL) que se utiliza para establecer una conexión cifrada entre la escuela y sus clientes emplea un protocolo con debilidades conocidas en su cifrado, lo que lo hace vulnerable a un posible ataque de intermediario [Al Faresi and Al Zubaidi, 2021]. Es de vital importancia que el colegio priorice la solución de la vulnerabilidad, ya que a través de él se puede transmitir una gran cantidad de información privada y sensible de los clientes, en este caso de los alumnos, desde detalles sobre sus datos personales hasta información confidencial como contraseñas o datos sobre tarjetas bancarias. Algunas de las propuestas que encontramos para darle solución a esta vulnerabilidad es la de proponerle al colegio que deshabilite estas versiones editando la configuración del servidor web, debido a que estas versiones corren mayores riesgos de ser atacadas. Es necesario hacer una actualización a TLS, que es la versión más reciente y segura de SSL, y el cual es conocido como uno de los protocolos criptográficos más implementados en la práctica y protege numerosas comunicaciones de Internet todos los días. La herramienta genera completamente las puntuaciones de prueba que verifican que el protocolo disfruta de las propiedades deseadas [Tran, 2022]. Se recomienda instalar la versión 1.2 o superior para que de esta forma el sitio esté protegido. Igualmente, es necesario realizar constantes pruebas de vulnerabilidad para asegurarse que la información se encuentra protegida y no se haya registrado algún ataque o una vulnerabilidad en la información y datos confidenciales.

5. **SSL Certificate Signed Using Weak Algorithm**

   Se encontró que las instalaciones utilizan un algoritmo de Hash débil, a pesar de que el certificado SSL asegura una conexión encriptada y segura entre un servidor web y el navegador

del cliente. El uso del algoritmo Hash débil puede llevar a que los atacantes puedan violentar el sistema y crear un sistema falso que parezca real y de esta forma obtener la información confidencial [Schneier, 2000]. Un certificado SSL asegura una conexión encriptada y segura entre un servidor web y el navegador del cliente. La información que contiene incluye el dominio del sitio web, la clave pública del servidor y la firma digital de la Autoridad de Certificación que lo emitió. Sin embargo, si se usa un algoritmo de Hash débil, esto puede llevar a debilidades que los atacantes pueden aprovechar para comprometer la integridad del certificado y crear uno falso que parezca legítimo [Al-Hazaimeh et al., 2020]. Esto permitiría la interceptación de información confidencial que se transmite entre el servidor y el cliente. Para solucionarlo, como se mencionó anteriormente, es necesario hacer la actualización de las versiones de SSL 2 y 3, ya que esto trae como consecuencia muchos riesgos, entre ellos dos vulnerabilidades, la 5 y la 6 de este documento. También se necesita hacer un nuevo certificado SSL que utilice un algoritmo más fuerte asegurándose de que el proveedor de certificación sea confiable, hay muchos en el mercado como DigiCert, la cual es una de las empresas más grandes y respetadas en el mercado de certificados SSL [DigiCert, nd], así como Symantec [Symantec, nd], GlobalSign, etc. También puede utilizar un servidor de clave pública de alta seguridad para almacenar las claves de cifrado para que de esta forma se pueda proteger el certificado SSL.

6. **SMB NULL Session Authentication**

   Se encontró que en un equipo de la PyME se está utilizando una versión del sistema operativo que permite acceder a ciertas operaciones o archivos sin requerir autenticación mediante usuario y contraseña [Li et al., 2018]. El protocolo de intercambio de archivos o dispositivos periféricos conocido como SMB ha sido identificado como el origen de esta vulnerabilidad, ya que se ha comprobado que es posible autenticarse en una instancia de este protocolo sin la necesidad de proporcionar credenciales [Yang et al., 2019]. Para solucionar este problema es necesario implementar una autenticación de red para evitar el acceso no autorizado, algunas empresas ofrecen soluciones de autenticación en la red para evitar esto, como Cisco, Fortinet, Azure por parte de Microsoft, Okta, etc. También es conveniente limitar los permisos de acceso sólo a los usuarios necesarios para evitar cualquier tipo de filtración de información [Microsoft, 2021]. Es importante mantener los sistemas operativos actualizados como lo mencionamos en puntos anteriores. Limitar el acceso a la red también puede ayudar a prevenir el acceso no autorizado, y puedes limitar este acceso mediante la implementación de firewalls, VPN o segmentando la red. Para garantizar que todo se encuentre en orden, sin algún tipo de vulnerabilidad también es recomendable monitorear la actividad de red constantemente para poder darse cuenta de posibles intentos de accesos no autorizados o de actividades sospechosas [Wu and Hsu, 2016].

VI Plan de Mitigación

6.1 Propuesta de seguridad informática

Considerando que la PyME no cuenta con un equipo de informática presente en las instalaciones, es necesario considerar que las soluciones deben de ser asequibles y replicables, así como mantenerse actualizadas con el paso del tiempo.

Solución Propuesta	Precio
Plática a empleados	
Primero, el equipo pretende dar una charla corta platicando sobre la importancia de mantener dispositivos y aplicaciones actualizados. Así, además de crear un entorno consciente y mejorar su cultura de seguridad, se podría reducir el riesgo y, a su vez, aumentar la productividad. Este último es importante porque si los empleados conocieran las mejores prácticas de seguridad, podrían trabajar de una manera más eficiente y efectiva (Adams, 2021). **Pros:** • Una plática es suficiente, no necesita una atención continua. • Mejora la cultura general de los empleados. • Además de ayudar a la empresa, signifcaría también una ayuda a la seguridad de sus cuentas personales. • Servicio gratuito. **Contras:** • Puede ser que los empleados presenten una falta de interés y, por lo tanto, alcanzaríamos un menor impacto. • No es una solución completa, faltarían otras medidas de seguridad. • Puede ser que las personas tengan una comprensión limitada de los temas de seguridad, por lo que sería complicado implementar las soluciones.	$0

Figura 3: Solución 1 - Plática a empleados

Esta solución es gratuita porque el curso sería impartido por nosostros, con conceptos básicos sobre seguridad informática. El curso constaría de 2 sesiones, cada una de una hora y podríamos resolver sus dudas y preocupaciones. De tal manera, no solo mejoraría la seguridad de la empresa, sino de la vida personal de cada empleado.

Deshabilitar el IP Forwarding	
Deshabilitar el IP forwarding puede ser algo simple, siempre y cuando logremos reconocer los dispositivos que la sufren. La manera de hacerlo en windows es: 1. Abrir el "Editor del Registro". 2. Navegar a la ubicación: "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters". 3. Crear una nueva clave llamada "IPEnableRouter" y establecer su valor en "0" (cero). 4. Reiniciar el equipo para que los cambios surtan efecto. Con estos simples pasos, se puede eliminar la cantidad de riesgos y posibles ataques que la empresa podría sufrir, al tenerlo activado (Conran, 2014). **Pros:** • Puede evitar que los paquetes de red sean reenviados a una interfaz no autorizada. • Solución que no toma mucho tiempo. • Puede liberar recursos y mejorar el rendimiento general del sistema. **Contras:** • Se tendría que llamar al especialista en redes, para que lo haga. • Necesitaría auditorías de seguridad de una manera regular. • Presenta un costo extra a la empresa.	$600

Figura 4: Solución 2 - Deshabilitar el IP Forwarding

Aunque la PyME no tiene un equipo de TI en las instalaciones, cuentan con un empleado que, en casos especiales y urgentes, les ayuda a solucionar los problemas que presentan en su red. Recibe un sueldo de $600 por hora, pero, al ser una solución sencilla de hacer, el equipo consideró que una hora sería suficiente.

Gestor de Contraseñas	
Incitar que los empleados usen gestores de contraseñas al entrar a su correo empresarial, impulsando específicamente BitWarden. De esta manera, se evitaría el uso repetitivo de la misma contraseña en todas las cuentas que creen, evitando ser víctimas de un ataque de fuerza bruta (Trevino, 2022). **Pros:** • Gratuito • No necesita a un equipo de TI • No necesita auditorías de seguridad de una manera regular **Contras:** • Un hábito que sería difícil crear para las personas de edades más avanzadas. • Es un poco cansado tener que copiar y pegar la contraseña cada vez que ingresan a un sitio web.	$0

Figura 5: Solución 3 - Gestor de Contraseñas

Descargar antivirus	
Considerando que la mayoría de empleados tienen una edad mayor a 40, son más propensos a caer en ataques de tipo phishing (Schwind, 2022). Por lo tanto, se recomienda descargar un antivirus que cuente con este tipo de protección; la mejor opción es Norton. Este, cuenta con un plan para empresas pequeñas y 20 dispositivos cuestan 250 dólares (aproximadamente $5,000 mexicanos). **Pros:** • Poco esfuerzo por parte de los empleados. • Ofrece soporte técnico 24/7 para las personas. • Es aplicable para cualquier sistema operativo. **Contras:** • Tiene un costo relativamente elevado. • Tendría que capacitar a los empleados sobre su funcionamiento.	$5,000

Figura 6: Solución 4 - Descargar Antivirus

Usar USB	
Al investigar sobre la manera en que se envían los archivos, descubrimos que los estados de cuenta, documentos de Excel con las finanzas, de Word con información personal de sus clientes, son enviados por medio correo electrónico. Entonces, la siguiente propuesta es implementar el uso de USB's para transferir los datos, esto, porque pueden ser cifrados por contraseñas, garantizando la privacidad y seguridad de los datos. A diferencia de los enviados por correo electrónico que pueden ser interceptados o manipulados en tránsito, lo que los hace vulnerables a los hackers y virus informáticos (CMD, 2016). **Pros:** • Cifrado con contraseña, garantizando seguridad. • Mayor capacidad de almacenamiento, permitiendo transferir grandes cantidades de datos. • Transferencias de archivos más rápidas y fiables. **Contras:** • Si un USB es perdido o robado, la información puede ser comprometida. • Si es infectado con virus puede propagarse rápidamente a otros dispositivos. • Costo que, aunque no es muy grande, si es adicional. El costo que corresponde a un USB marca SanDisk de 256 GB es de 20 dólares, o $400 mexicanos y se puede encontrar en Amazon.	$400

Figura 7: Solución 5 - Uso de USB

Para está solución, es importante aclarar que se deberán implementar una serie de políticas que aseguren su correcta ejecución. Estas son:

- **Restricción de acceso**: El USB no puede salir de la oficina del Director General, quien cuidará que no se utilice para cosas indebidas.
- **Locación**: Está estrictamente prohibido que el USB salga de las instalaciones del Instituto Bilingüe la Silla.

- **Contraseña**: Al tener documentos confidenciales, el USB deberá estar cifrado con una contraseña que solo sepa el Director General y que cambie de manera mensual.
- **Uso**: El uso del USB es exlusivo para facilitar la transferencia de archivos entre computadoras presentes en la oficina. Queda completamente prohibido su uso para cuestiones personales.

Certificado SSL	
Conociendo que se necesita un nuevo certificado SSL que utilice un algoritmo más fuerte, existen soluciones que brindan la posibilidad de que el consumidor se asegure que la certificación que otorga el proveedor sea confiable. DigiCert es la mejor opción en el mercado (Digicert, 2022), para evitar posibles vulnerabilidades al aprovecharse del Certificado SSL desactualizado. El costo se obtuvo de cotizar en la página de la empresa el plan básico. **Pros:** • Seguridad de la información • Protección contra el phishing • Servicio de ayuda 24/7 • Reemisiones y reemplazos gratuitos de por vida para el certificado. **Contras:** • Servicio costoso, pago por año • El certificado no garantiza al 100% que no se filtrarán datos, ha habido casos en el pasado en los que los certificados de Digicert han sido comprometidos.	$5, 400

Figura 8: Solución 6 - Compra de certificado

6.2 Precio Total

Finalmente, habiendo analizado las diferentes opciones que existen para atacar las vulnerabilidades presentes en la red, el plan de mitigación que se propone significaría un gasto de $11,400, cantidad que entra en el presupuesto de la PyME, que era de $15,000. En la figura 9 se muestra la gráfica del gasto que representa el 76% del presupuesto inicial. Cabe aclarar que estas soluciones son completamente asequibles y replicables por la PyME, y significan un aumento exponencial en la seguridad de la empresa.

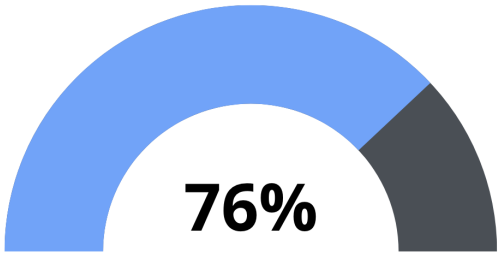

Figura 9: Gráfica de gasto respecto al presupuesto.
Hecha con la herramienta de Canva.

6.3 Riesgos de no implementarse

Hacer caso omiso a las vulnerabilidades que una empresa de este tipo presenta y no poner en práctica un plan de mitigación podría traer graves consecuencias. Éstas dependerán del tipo de empresa, el tipo del ataque y la información que esté en riesgo, sin embargo, independientemente de estos efectos, siempre se recomienda analizar qué tanto se puede perder (en todos los sentidos, no sólo económicamente) y de qué forma se puede evitar, y por ende, cuánto dinero se estaría ahorrando poniendo en práctica un plan, aunque al principio represente una inversión. Algunas de las posibles consecuencias para un caso como el de este análisis serían:

- **Pérdida económica:** Sufrir un ataque en una pequeña o mediana empresa podría significar una pérdida económica de poco más de 100,000 dólares, valor que dependerá de la magnitud del ataque. Además, una pérdida económica tiene más repercusión en una empresa pequeña que en una grande completamente establecida [Feagin, 2015].

- **Pérdida de clientes:** El que una empresa sufra un ataque informático da pie a que sus clientes pierdan la confianza en ella, lo que recae directamente en su reputación y en que futuros clientes se abstengan de trabajar con ella [Feagin, 2015]. Un informe de 2018 de la firma de seguridad digital Gemalto encontró que el 70% de los consumidores en todo el mundo afirmaron que dejarían de hacer negocios con una empresa si se enteraran de que había sufrido una violación de datos [Gemalto, 2018]. Otro estudio realizado en 2020 por la empresa de seguridad cibernética Kaspersky encontró que el 43% de las pequeñas y medianas empresas perdieron clientes después de sufrir una violación de datos, y que el 22% de estas empresas tuvieron que cerrar sus negocios debido al impacto financiero [Kaspersky, 2020].

- **Sanciones legales:** En muchos países, encluido México, existe una Legislación de Protección de Datos. Si se demuestra que una empresa no cumple con esta ley, se puede recurrir a multas por infracción [Huggett, 2022]. Las sanciones pueden ser de hasta 2% de los ingresos anuales del responsable que haya cometido la infracción, con un tope máximo de aproximadamente $4.4 millones

VII Conclusiones

En conclusión, es de vital importancia que las empresas estén conscientes de las vulnerabilidades de su red, pues el aumento de la tecnología y la conectividad de los negocios ha llevado a un aumento en los riesgos de seguridad, y las empresas deben tomar medidas proactivas para mitigar, o al menos reducir, estos riesgos. De lo contrario, se enfrentarían con riesgos y podrían sufrir consecuencias significativas.

Por lo tanto, es esencial que la PyME seleccionada sea capaz de implementar algunas de las medidas de seguridad propuestas anteriormente, para así lograr proteger sus datos valiosos y garantizar la continuidad de sus operaciones de una manera segura.

Finalmente, el trabajo en equipo mostró ser una pieza fundamental para el éxito en este tipo de proyectos, pues, cuando las personas trabajan juntas en un ambiente colaborativo y apoyándose mutuamente, pueden lograr objetivos que no podrían alcanzar individualmente. Está comprobado que este fomenta la productividad, la creatividad, la innovación y la construcción de relaciones positivas entre los miembros del equipo.

VIII Referencias Bibliográficas

[Adams, 2019] Adams, K. (2019). Help employees understand the importance of cybersecurity. *SHRM*.

[Al-Dulaimi et al., 2017] Al-Dulaimi, A., Al-Ataby, A., and Zohdy, M. (2017). Dhcp spoofing: attack techniques and countermeasures. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 9(3-11):39–44.

[Al Faresi and Al Zubaidi, 2021] Al Faresi, H. M. and Al Zubaidi, A. M. (2021). Ssl/tls protocol: Vulnerabilities, threats and solutions. *Journal of Information Security*, 12(1):41–53.

[Al-Hazaimeh et al., 2020] Al-Hazaimeh, M. M., Al-Naimat, A., and Abu-Awad, F. (2020). Secure hash algorithm (sha) performance analysis. *International Journal of Advanced Computer Science and Applications*, 11(5):422–429.

[ASEM, 2021] ASEM (2021). ¿qué es una pyme? `https://www.asem.mx/que-es-una-pyme/`.

[CANACO, 2021] CANACO (2021). Clasificación de empresas. `https://www.canacocdmx.com/clasificacion-de-empresas/`.

[Conran, 2014] Conran, M. (2014). Ip forwarding and packet forwarding. `https://network-insight.net/2014/08/10/ip-forwarding/`.

[Corporation, 2021] Corporation, T. M. (2021). Common Vulnerabilities and Exposures (CVE). *MITRE Corporation*.

[Digicert, 2022] Digicert (2022). Digicert marca una tasa de crecimiento sólida en 2022 y crea impulso para la visión de confianza digital. [comunicado de prensa]. pr newswire. https://www.prnewswire.com/news-releases/digicert-marks-strong-growth-rate-in-2022-and-builds-momentum-for-digital-trust-vision-3 html.

[DigiCert, nd] DigiCert (n.d.). Ssl/tls certificates. https://www.digicert.com/ssl-tls-certificates/.

[Economia, 2021] Economia, S. D. (2021). Programa nacional de la micro, pequeña y mediana empresa. https://www.gob.mx/se/acciones-y-programas/programa-nacional-de-la-micro-pequena-y-mediana-empresa.

[Feagin, 2015] Feagin, R. D. (2015). The value of cyber security in small business.

[Gemalto, 2018] Gemalto (2018). Global customer data breach report. https://www.gemalto.com/press/Pages/Global-Customer-Data-Breach-Report.aspx/.

[Hu et al., 2020] Hu, Y., Kim, J., and Lee, H. (2020). Understanding and mitigating the security risks of port forwarding. *IEEE Communications Magazine*, 58(3):71–77.

[Huggett, 2022] Huggett, C. (2022). Going on the attack: Top five consequences of cyber security breaches. https://technative.io/going-on-the-attack-top-five-consequences-of-cyber-security-breaches/.

[Kaspersky, 2020] Kaspersky (2020). Small business it security risks 2020: Malware and financial threats report. https://www.kaspersky.com/small-business-security/it-security-risks-report-2020/.

[Laudon and Laudon, 2016] Laudon, K. C. and Laudon, J. P. (2016). *Management Information Systems: Managing the Digital Firm*. Pearson.

[Li et al., 2018] Li, S., Li, Z., Li, Y., and Huang, W. (2018). The development of smb vulnerability scanning tool based on python. In *Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–6. IEEE.

[Microsoft, 2021] Microsoft (2021). Smb security best practices. https://docs.microsoft.com/en-us/windows-server/administration/smb-security-best-practices. Accessed: 2023-03-19.

[Nguyen et al., 2017] Nguyen, T. A., Nguyen, P. H., Pham, T. L., and Pham, D. H. (2017). Enhancing dhcp snooping for mitigating dhcp spoofing attacks. In *2017 9th International Conference on Knowledge and Systems Engineering (KSE)*, pages 76–81. IEEE.

[Norton, 2020] Norton (2020). Informe de norton lifelock sobre ciberseguridad. https://es.norton.com/internetsecurity-emerging-threats-2020-data-breach-statistics-report.html.

[Schneier, 2000] Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Wiley.

[Schwind, 2022] Schwind, P. (2022). Norton malware protection. https://www.keepersecurity.com/blog/2022/10/24/why-organizations-need-a-business-password-manager/.

[Symantec, nd] Symantec (n.d.). Ssl/tls certificates. https://www.symantec.com/products/ssl-tls-certificates.

[Tan et al., 2020] Tan, K. C., Razak, A., and Ahmad, R. (2020). Network security and cybercrime prevention strategies. *Journal of Information Security*, 11(1):52–63.

[Tran, 2022] Tran, T. (2022). *Implementing SSL/TLS: Using Cryptography and PKI*. Packt Publishing Ltd.

[Trevino, 2022] Trevino, A. (2022). Why organizations need a business password manager. https://www.keepersecurity.com/blog/2022/10/24/why-organizations-need-a-business-password-manager/.

[Van der Aalst and Van Hee, 2002] Van der Aalst, W. M. P. and Van Hee, K. M. (2002). *Workflow Management: Models, Methods, and Systems*. MIT press.

[Wu and Hsu, 2016] Wu, C.-H. and Hsu, C.-W. (2016). A vulnerability analysis of smb protocol. *Journal of Information Hiding and Multimedia Signal Processing*, 7(2):403–412.

[Yang et al., 2019] Yang, Y., Xu, C., Zhang, X., and Wang, W. (2019). Security analysis of smb protocol based on wireshark. In *Proceedings of the 2019 5th International Conference on Control, Automation and Robotics (ICCAR)*, pages 145–149. IEEE.