Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Auditoría de Seguridad y Plan de Mitigación:

Caso Pogen

Profesores:

Alberto Francisco Martınez Herrera

Oscar Eduardo Labrada Gómez

Integrantes:

Avril Michelle Ruiz Martínez	A00833018
María Fernanda Lee Ponce	A009830974
Luis Fernando Navarro Saucedo	A00833148
Axel Quiroga Caldera	A00832676
Juan Ángel Lucio Rojas	A00833112

Nombre del Socio Formador:

IPC Services

Monterrey, Nuevo León, a 30 de Mayo de 2023.

Auditoría de Seguridad y Plan de Mitigación

Inventario de Pogen

I. Introducción

La PyME en México es una micro, pequeña y mediana empresa que forma un segmento importante de la economía a nivel nacional, pues genera un gran aporte en cuanto a productos y servicios. Las PyMEs promueven el desarrollo económico, la expansión del mercado, la generación de empleos y una distribución de riqueza más equitativa (Lizarazo, C., 2023).

En el presente caso de estudio, se analiza a Pogen, una pequeña empresa que opera en el sector de venta minorista al ofrecer soluciones de conteo de personas. Dichas soluciones implican rastrear e interpretar el flujo de personas en establecimientos comerciales, que es posible al utilizar sensores infrarrojos que detectan la entrada y salida de personas con más de un 95% de confiabilidad de acuerdo con Pogen (s.f.). También ofrece servicios relacionados al GeoMarketing, una técnica de análisis de mercados y planificación estratégica que combina información espacial con variables de marketing y de negocio. (Cliquet, G., 2011).

Pogen cuenta con dos servicios principales: flujo de personas y GeoMarketing. En colaboración, permite a sus clientes, centros comerciales, plazas y tiendas, tener una visión más profunda y minuciosa sobre el comportamiento de los consumidores, y por ende dar soporte a la toma de decisiones de una manera más precisa.

Considerando las clasificaciones del INEGI y la Secretaría de Economía, Pogen se clasifica como una PyME al contar con 33 colaboradores. Esto según la estratificación de empresas propuesta por la Secretaría de Economía (2009), la cual señala que una pequeña empresa del sector de servicios tiene desde 11 hasta 50 empleados y una mediana desde 51 hasta 100.

Las pymes no pueden permitirse el lujo de retrasar su inversión en ciberseguridad (Benz & Chatterjee, 2020), ya que en la actualidad son el objetivo de la gran mayoría de ataques cibernéticos (Ponsard et al., 2019). En este sentido, Pogen reconoce la importancia de realizar una auditoría de seguridad exhaustiva para evaluar la postura actual de seguridad de la empresa y detectar posibles vulnerabilidades y riesgos, por este motivo ellos están

dispuestos a invertir $15,000 (MXN), un presupuesto limitado; por este motivo las soluciones tienen que ser asequibles y concisas.

De acuerdo con Dávalos (2013):

> La Auditoría de Seguridad de la Información cobra importancia como medio de detección de desviaciones de las políticas y procedimientos implantados por medio de herramientas de aplicación aceptadas a nivel mundial (Estándares, prácticas, etc.) y permiten la retroalimentación para las correcciones o cambios oportunos con el fin de lograr mejorar la Seguridad de la Información y salvaguardar la misma.

La ciberseguridad ha aumentado en relevancia a distintas empresas, sin embargo aún se ha observado que no en su gran mayoría se han puesto en práctica las medidas de seguridad que requieren. Mauricio Benavides (2022), director ejecutivo de Metabase Q, explicó que una de las amenazas más comunes es el phishing a través de redes sociales, email o mensajes y el ransomware. Además, agregó:

> “Cada 11 segundos en América Latina está pasando un ataque de ransomware, para las PyMEs aumentarán 424% los ataques de este tipo en 2020”.

87% de las empresas en 19 países incluido México sufrieron de un ciberataque, generando pérdidas de hasta 1 millón de dólares (Fortinet, 2022) . Muchas de las empresas afectadas son pymes, la base de la economía nacional que de acuerdo con IDefender, el 86% de las empresas no está preparada para amenazas y 8 de cada 10 no cuenta con las herramientas necesarias de protección (López, E., 2022)

Keith Collins Storms (2022), director de Tecnología de IDefender, firma de seguridad cibernética, detalló que de los 156,000 millones de ataques cibernéticos sufridos en América Latina durante el primer semestre del 2022, 80,000 millones ocurrieron en México, siendo este de los mayores países afectados en la región del lado de las pymes.

El plan de mitigación busca minimizar los riesgos e impactos negativos. Diseñado en base a la auditoría de seguridad, proporcionará a Pogen una estrategia integral para fortalecer su postura de seguridad y proteger sus activos, tanto físicos como digitales. Esto no solo ayudará a salvaguardar la confidencialidad, integridad y disponibilidad de la información de

la empresa, sino que también reducirá el riesgo de sufrir brechas de seguridad y posibles repercusiones financieras y reputacionales.

II. Inventario de Pogen

La empresa no tiene como tal una lista con todos los dispositivos conectados a su red, por este motivo se optó por utilizar Advanced IP Scanner, un software gratuito para analizar todos los dispositivos conectados a la red y te devuelve el el nombre del dispositivo, IP, MAC. Tras correr el análisis, el software encontró 98 dispositivos conectados a la red. El resultado con todos los dispositivos conectados se puede ver en el *Anexo 1*. Tabla de dispositivos conectados.

Además de utilizar el software, se realizó una encuesta para conocer los dispositivos de los empleados, marca, tipo, propietario, sistema, para conocer qué tipo de laptops y celulares estaban conectados a la red.

Con estos datos, se pudo realizar un inventario con los dispositivos conocidos y el uso que se les da a los mismos, el inventario se compone de 34 dispositivos que están tanto en el análisis de Advanced IP Scanner y en la encuesta realizada, el inventario se puede ver en el *Anexo 2*. Tabla de inventario.

III. Topología de la red inventariada

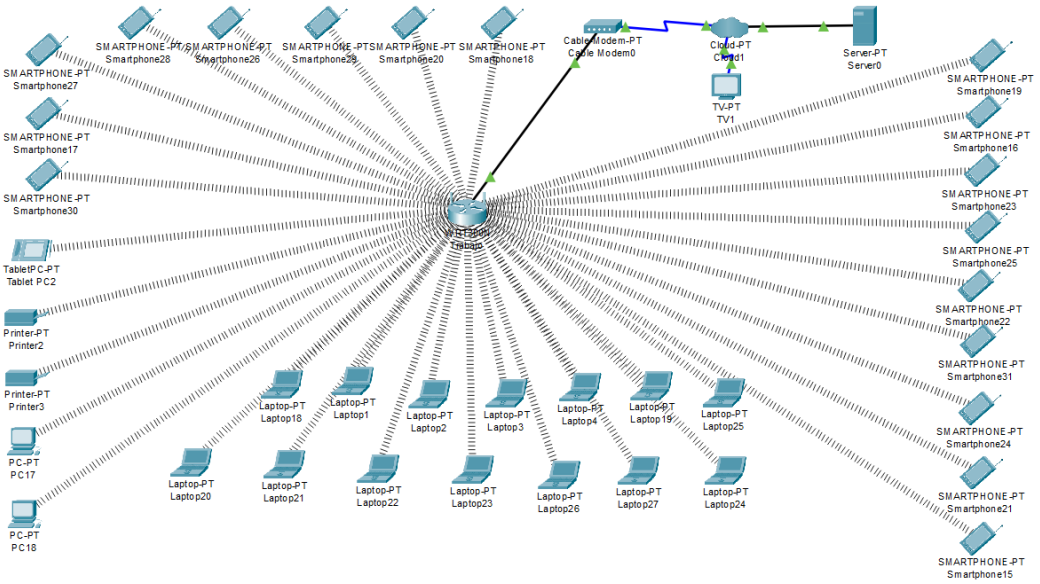

Figura 1. Topología original de la red inventariada para Pogen.

En la *Figura 1* se tiene la topología de red de la PyME Pogen, la cual muestra cómo se conectaba la red de dispositivos durante el análisis de vulnerabilidades. Esta incluye los equipos de cada uno de los colaboradores, siendo las PC17 y PC18 equipos de la empresa destinados exclusivamente al área de Sistemas. Asimismo, se muestran un total de 14 Laptops, de las cuales 10 pertenecen a Pogen y son usadas en distintas áreas, como Sistemas, Recursos Humanos, Customer Services y el área de Data. Dentro de la misma red está conectado el equipo del Director de la PyME. También hay 4 Laptops que además de ser de uso personal, pertenecen a miembros del área de Data, Sistemas y Marketing. Al igual que estas existen 14 SmartPhones, todos de uso personal conectados a la red de la empresa. Además de los SmartPhones, hay una Tablet del director para tomar notas. Por último, la PyME cuenta con otros dispositivos que pueden ser usados por cualquier colaborador, como 2 impresoras y una SmartTV. Es importante mencionar que cada uno de los dispositivos mencionados están conectados de forma inalámbrica al enrutador mediante una contraseña de acceso, ya que es la manera en que trabaja la PyME, y este a su vez se conecta por cable al Módem que va conectado a un Proveedor de Servicios de Internet.

Plan de evaluación

I. Herramientas de Evaluación

La evaluación de vulnerabilidades se efectuó a 29 dispositivos conectados a la red, del tipo SmartPhones, Laptops y una Tablet. Para obtener esta información, se usó la plataforma de Tenable Nessus Expert.

Nessus Expert ofrece el servicio 'Vulnerability Scans' (Escaneo de Vulnerabilidades), que permite encontrar las vulnerabilidades alrededor de las IT (Tecnologías de Información) y la infraestructura de la nube (Tenable, 2023).

Tenable (2023) tiene productos que ayudan a identificar, investigar y priorizar vulnerabilidades de forma preciosa. Asegura tu nube, contenedores, dispositivos OT (Tecnología de Operación) y activos IT tradicionales.

> "Nessus es el estándar de oro para la evaluación de vulnerabilidad. Hemos mejorado las capacidades de abordar instancias en la nube que se actualizan constantemente y se conectan a varias fuentes. Estamos subiendo la apuesta con Nessus Expert." (Pendley, G., 2022)

Desde 1998, Nessus ha ayudado a los equipos de seguridad a ir un paso adelante. Proporciona la visibilidad, precisión y velocidad que necesita para proteger a su organización contra los riesgos inaceptables (DTE, 2023). Debido al prestigio que maneja esta plataforma, se decidió y a su vez se destinó a utilizarla, y los resultados fueron satisfactoriamente identificables.

II. Inventariado de vulnerabilidades

En los dispositivos inventariados como anteriormente se mencionó, se usó la herramienta de Tenable Nessus Expert. Las vulnerabilidades detectadas llegaron a ser variadas, puesto a la extensa cantidad de dispositivos conectados a la red. A continuación, se expone el tipo de plugin (error) que ocurre en cada uno, de los cuales hay tres niveles de severidad: baja, media y alta. También se especifica el CVSS (Common Vulnerability Scoring System). En su totalidad esta información es proporcionada por la base de datos de Tenable (2023), que recopila los plugins correspondientes:

Plugin	Nombre	CVSS	Severidad	Descripción
11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	3.3	Baja	Esta vulnerabilidad provoca pérdida de memoria de red en un host remoto. Esto sucede cuando un dispositivo de red usa datos variables en las tramas de ethernet. Esto puede provocar que un atacante recopile información del host afectado si se encuentra en la misma subred física, como solución se recomienda contactar al proveedor del controlador de los dispositivos en cuestión y obtener una solución.
83875	SSL Certificate Expiry (SSL/TLS Diffie-Hellman Modulus)	3.7		El host remoto conlleva una vulnerabilidad ya que permite conexiones SSL/TLS con módulos menores o iguales a 1024 bits. Esto mismo abre la posibilidad que sea más sencillo para una persona de fuera hacer un criptoanálisis y robar información sensible. Para la solución de esta vulnerabilidad se recomienda re-configurar el servicio para usar módulos Diffie-Hellman de al menos 2048 bits.
11213	HTTP TRACE / TRACK Methods Allowed	5.3	Media	El servidor web remoto admite los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web. La solución es deshabilitar estos métodos HTTP.
173260	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities	5.3		La versión de OpenSSL instalada en el host remoto es anterior a 1.1.1u. Por lo tanto, está afectada por múltiples vulnerabilidades mencionadas en el aviso 1.1.1u. Se ha identificado una vulnerabilidad de seguridad en todas las versiones admitidas de OpenSSL relacionada con la verificación de cadenas de certificados X.509 que incluyen restricciones de políticas. Los atacantes pueden aprovechar esta vulnerabilidad mediante la creación de una cadena de certificados maliciosos que desencadena un uso exponencial de recursos computacionales, lo que resulta en un ataque de denegación de servicio (DoS) en los sistemas afectados.
15901	SSL Certificate Expiry	5.3		Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el objetivo e informa si alguno de ellos ya ha caducado. La solución es adquirir o generar un nuevo certificado SSL para reemplazar el

				existente.
10704	Apache Multiviews Arbitrary Directory Listing	5.3		El servidor web Apache en el host remoto tiene una vulnerabilidad de divulgación de información. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para obtener un listado de directorios remotos, incluso si existe un archivo de índice válido en el directorio.
10194	HTTP Proxy POST Request Relaying	5.3		El proxy permite a los usuarios realizar solicitudes POST sin etiqueta de Content-length, lo que puede dar a los atacantes la capacidad de tener sesiones interactivas. Esto también puede permitir que los atacantes eludan el firewall y se conectan a puertos sensibles, mientras que los usuarios internos pueden evadir las reglas del firewall y acceder a puertos no autorizados. Además, el proxy puede ser utilizado para llevar a cabo ataques contra otras redes.
57608	SMB Signing not required	5.3		No se requiere firma en el servidor SMB remoto, lo que significa que cualquier persona no autenticada y remota puede aprovechar esta falta de seguridad para realizar ataques de intermediario contra el servidor SMB.
134220	IP Forwarding Enabled (Information Disclosure)	5.3		El servidor web remoto se ve afectado por una vulnerabilidad de divulgación de información. La versión instalada de nginx es anterior a 1.17.7, por lo que se soluciona actualizando a una versión más nueva.
51192	SSL Certificate Cannot Be Trusted	6.5		El certificado X.509 utilizado por un servidor no es confiable, la autoridad del certificado no es reconocido, también puede contener un certificado inválido al momento de escaneo y otro motivo es que no coincide la firma del certificado o que esta no se puede verificar.
57582	SSL Self-Signed Certificate	6.5		El servicio en el host remoto no tiene una cadena de certificados X.509 firmada por una autoridad de certificación reconocida. Esto significa que si el host remoto es público y se encuentra en producción, el uso de SSL no tiene ningún efecto, ya que cualquier persona podría llevar a cabo un ataque de intermediario contra el host remoto.
104743	TLS Version 1.0 Protocol Detection	6.5		La versión TLS 1.0, esta versión del TLS tiene numerosas fallas de diseño criptográfico. La solución recomendada es

				habilitar la compatibilidad con TLS 1.2 y 1.3, esto implica deshabilitar la compatibilidad actual con TLS 1.0
157288	TLS Version 1.1 Protocol Deprecated	6.5		La versión TLS 1.1 representa una vulnerabilidad ya que esta acepta conexiones cifradas de TLS 1.1, por lo que no es compatible con los cifrados recomendados para mantener una seguridad adecuada. Por lo que la solución, similar a la vulnerabilidad anterior sería habilitar la compatibilidad con TLS 1.2 o 1.3 en su defecto, y con ello deshabilitar el TLS 1.1
42263	Unencrypted Telnet Server	6.5		El host remoto está utilizando un servidor Telnet que opera a través de un canal no cifrado. Esta configuración no es recomendable debido a que las credenciales de inicio de sesión, contraseñas y comandos se transmiten en texto plano, lo que permite que un atacante remoto pueda interceptar una sesión Telnet para obtener información confidencial o modificar el tráfico entre el cliente y el servidor.
50686	IP Forwarding Enabled	6.5		El reenvío de IP está habilitado en el host remoto, lo que permite a un atacante redirigir paquetes a través de él y posiblemente evadir algunos firewalls, enrutadores o filtros de NAC.
35291	SSL Certificate Signed Using Weak Hashing Algorithm	7.5	Alta	Se refiere a una vulnerabilidad de certificados SSL en un servicio remoto, el certificado SSL sirve para garantizar la seguridad entre cliente y servidor y se basa en la firma digital de un certificado. En este caso el servicio remoto está usando un algoritmo hash débil, un atacante puede generar otro certificado con la misma firma digital permitiendo que se haga pasar por el servicio al que se quiere comunicar el cliente.

Tabla 1: Inventariado de vulnerabilidades, Fuente: Tenable (2023)

III. Indicios de vulnerabilidades en la Topología.

La empresa utiliza el protocolo WEP (privacidad equivalente al cableado), el cual, si bien podría ser mejor que no usar ningún protocolo de seguridad, actualmente se considera obsoleto y se recomienda optar por uno mejor. Esto se debe a que contiene varias vulnerabilidades, pues de acuerdo con (WEP, WPA, WPA2 y WPA3: diferencias y explicación, 2023), WEP usa una clave estática de 128 bits, lo que significa que todo el

tráfico en la red se cifra con una sola clave. La cual además no se suele cambiar a menudo o siquiera una vez, lo que podría hacer que si el atacante captura suficiente tráfico de red cifrado, el cual es bastante débil , con facilidad podría descifrar la clave por tanto tener acceso a toda la red.

Asimismo, al indagar más en la topología de la red y consultarlo con los miembros de sistemas, nos dimos cuenta que no cuentan con un firewall o cortafuegos que limite el acceso a la red. Esto si bien podría no ser una llave que permita a cualquiera entrar, es muy importante considerar su implementación, en especial en las pequeñas y medianas empresas, pues según (Fernández, 2012), los cortafuegos son uno de los mejores modos de proteger una red de numerosos ataques provenientes del exterior. De estos existen una variedad, incluso los hay de uso doméstico, sin embargo, en el plan de mitigación se explorará este tema a mayor profundidad.

Como último punto, al hacer el inventario de los dispositivos que se encontraban dentro de la red, nos percatamos que aunque todos usan software diferentes, hay varios de ellos que no están actualizados. Por ejemplo, hay dispositivos con el sistema operativo Windows 10, cuando actualmente existe la versión 11, esto mismo ocurre con los dispositivos que usan iOS y Android, los cuales se encuentran una o hasta dos versiones anteriores a la más nueva. La actualización de los sistemas operativos es de suma importancia, ya que de acuerdo con (Alday, 2022), los desarrolladores de dichos sistemas a menudo lanzan nuevas versiones con el fin de corregir errores y fallas de seguridad que se encontraban en parches anteriores, por lo que actualizarlos constantemente permite disminuir la cantidad de vulnerabilidades a las que nos enfrentamos.

IV. Control y flujo de información

Pogen nos comentó que hace uso de Amazon Web Services (AWS, por sus siglas en inglés), que es una plataforma de servicios en la nube por parte de Amazon. Como las bases de datos de la empresa se encuentran en AWS, este servicio también se encarga de protegerlas.

Por medio de AWS Identity, según Amazon Web Services (s.f.), se administran los permisos de forma segura, esto se hace por medio de controles de acceso y administración de identidades, autenticación multifactor y cifrado de datos en reposo y en tránsito. Además, ofrece herramientas de monitoreo y detección de amenazas para proteger contra actividades maliciosas y garantizar la seguridad de los datos almacenados.

De acuerdo con Amazon Web Services (s.f.), se protegen a las redes y aplicaciones mediante políticas de seguridad detalladas, protección a nivel de host, red y aplicación, mitigación de ataques DDoS, filtrado de tráfico y visibilidad en tiempo real.

Como menciona Amazon Web Services (s.f.), AWS protege los datos según los clientes decidan, esto incluye la privacidad, el acceso y el cifrado de sus datos, respaldados por una infraestructura en la nube segura y flexible.

Aunque se desconoce las herramientas para la protección de datos que contrató Pogen, para proteger los datos se requieren herramientas para tratar con los permisos de acceso (como el AWS Identity and Access Management), para la detección de accesos no autorizados (como el AWS CloudTrail) y para la gestión de claves criptográficas (como el AWS Key Management Service).

La implementación de dichas herramientas se alinean con el enfoque de ISO 27001, uno de los estándares más conocidos a nivel mundial, que involucra proteger la confidencialidad, integridad y disponibilidad de la información en una empresa (Kosutic, s.f.).

Cabe agregar que su dominio y página web los provee IONOS, que es un proveedor de hosting y cloud para PyMEs. IONOS, (s.f.) brinda protección a los dominios mediante la defensa contra DNS hijacking, implementando la verificación de dos factores, seguridad con DNSSEC y proporcionando una prueba de propiedad del dominio.

La protección de dominio es crucial para prevenir que los piratas informáticos redirijan el dominio a páginas web fraudulentas. Esto evita la recopilación de datos como tarjetas de crédito de usuarios y protege la propiedad legal de tu dominio. Al utilizar DNSSEC, se asegura la integridad y autenticidad de la información almacenada en tus registros DNS, protegiendo la conexión y dirección IP de tu dominio (IONOS, s.f.).

V. Pérdida de información

Pogen tuvo pérdida de información hace aproximadamente 2 meses, por una falla general en los sensores en el sistema y todos los datos de los 1770 sensores reportaron datos erróneos el 1 y 2 de abril del año en curso, ante esta falla se optó por migrar el servidor a otra plataforma y en empezar a diseñar un protocolo de emergencias en el departamento de sistemas.

VI. Cultura de ciberseguridad

Los colaboradores y distintas áreas dentro de la PyME han mencionado que la misma empresa les proporciona los correos y cuentas para el acceso a la página, por lo que se descarta el posible uso de contraseñas dadas por información personal del empleado, sin embargo las contraseñas no son creadas de manera “aleatoria” o con un patrón difícilmente de identificar para alguien externo; a palabras de ellos se menciona que las contraseñas son muy similares entre sí y están elaboradas a partir de información interna de la empresa por lo que si un tercero descubriera una o un par de las claves de acceso a la página fácilmente podría encontrar relación entre las mismas y acceder a las cuentas de todos los colaboradores; lo que representa un riesgo inmenso ya que información sensible está a disposición de una única contraseña de correo que puede ser fácilmente vulnerable al está conformada por únicamente letras y números (sin símbolos) y ser muy similar a la clave del mismo router.

Es importante señalar que la red de dispositivos conectados a la red dentro de la PyME no está completamente aislada de amenazas externas, esto viene principalmente de los dispositivos personales que tienen acceso directo a la red y página de la empresa, como pueden ser las laptops y celulares personales utilizadas por ciertos colaboradores. Por lo que el acceso a la página (con una contraseña única y vulnerable para todo el personal) puede ser violado sin necesidad de atacar a la PyME directamente, sino con un malware a uno de estos dispositivos que entran y salen de la red; esto va de la mano a un nulo uso de un antivirus para los equipos de parte de la empresa, dado que cada empleado cuenta con uno propio que pueden o no tener la misma efectividad de mitigar algún ataque a la plataforma o que robe información a las cuentas y/o correos.

VII. Identificación de anomalías o vulnerabilidades

Anomalía o vulnerabilidad	**Localización**
WiFi con WEP	Router WiFi
Carencia de un cortafuegos	En toda la red
Poca actualización de SO	Sistema Operativo de los colaboradores de la PyME
Contraseñas débiles	Colaboradores de la PyME.
Certificados SSL débiles	Base de datos generada por un servidor.
TSL desactualizado	Servidor.

Tabla 2: Anomalías o vulnerabilidades y su localización. Fuente: Elaboración Propia.

Anexos

Anexo 1. Tabla de dispositivos conectados.

https://drive.google.com/file/d/1YwQFr8ZMAEt6XMW4TzpqOiHkvHGI_7Q2/view?usp=sharing

Anexo 2. Tabla de inventario.

https://docs.google.com/spreadsheets/d/1fJxH86vCe4vhEa5NdjGJFlOeQ3AVSqIK/edit?usp=sharing&ouid=106108270118132150303&rtpof=true&sd=true

Referencias

Amazon Web Services. (s.f.). *AWS Identity*. Amazon.com. Recuperado el 6 de junio de 2023, de https://aws.amazon.com/es/identity/

Amazon Web Services. (s.f.). *Protección de datos y privacidad en AWS*. Amazon.com. Recuperado el 6 de junio de 2023, de https://aws.amazon.com/es/compliance/data-protection/

Amazon Web Services. (s.f.). *Protección de redes y aplicaciones en AWS*. Amazon.com. Recuperado el 6 de junio de 2023, de https://aws.amazon.com/es/products/security/network-application-protection/

Pogen. (s.f.) pogen. Recuperado el 26 de mayo de 2023, de https://pogen.com

Lizarazo, C. (2023) Las PyMEs en México: Retos e Importancia. Conekta. https://www.conekta.com/blog/las-pymes-en-mexico-retos-e-importancia

Canal Forbes México, (Febrero 9, 2022). *Estrategias de ciberseguridad para las PyMEs* https://www.youtube.com/watch?v=_MyjIWIJdBo&ab_channel=ForbesM%C3%A9xico

Kosutic, D. (s.f.). *What is ISO 27001? A detailed and straightforward guide*. 27001Academy. Recuperado el 6 de junio de 2023, de https://advisera.com/27001academy/what-is-iso-27001/

López, E. (2022), *Aumenta vulnerabilidad de pymes ante ciberataques; México el más afectado en Latinoamérica.* El Economista.

https://www.eleconomista.com.mx/el-empresario/Aumenta-vulnerabilidad-de-pymes-ante-ciberataques-Mexico-el-mas-afectado-en-Latinoamerica-20220901-0108.html

(2022), *Riesgo aumenta con brecha de habilidades en ciberseguridad, mientras que el 87% de las empresas latinoamericanas revela haber sido hackeadas en el último año.* Fortinet.

https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-2022-cybersecurity-skills-gap-survey

Secretaría de Economía. (2009, 30 de junio) *ACUERDO por el que se establece la estratificación de las micro, pequeñas y medianas empresas*. Diario Oficial de la Federación. Recuperado el 26 de mayo de 2023, de https://www.economia.gob.mx/files/marco_normativo/A539.pdf

Cliquet, G. (2013). *Geomarketing: Methods and Strategies in Spatial Marketing*. 10.1002/9781118614020. Recuperado el 26 de Mayo de 2023, de https://www.researchgate.net/publication/298082048_Geomarketing_Methods_and_Strategies_in_Spatial_Marketing

Benz, M., & Chatterjee, D. (2020). *Calculated risk? A cybersecurity evaluation tool for SMEs.* Business Horizons, 63(4), 531-540. https://doi.org/10.1016/j.bushor.2020.03.010

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). *Survey and lessons learned on raising SME awareness about cybersecurity*. Proceedings of the 5th International Conference on Information Systems Security and Privacy(ICISSP) (p. 558-563). https://doi.org/10.5220/0007574305580563

IONOS. (s.f.). *Protección de dominio de IONOS*.Ionos.mx. Recuperado el 6 de junio de 2023, de https://www.ionos.mx/dominios/domain-guard

Bustillos, O. & Rojas, J. (2022). *Protocolo básico de ciberseguridad para pymes* (p. 5). https://revistas.ulima.edu.pe/index.php/Interfases/article/view/6021

Dávalos, A. (2013). *Auditoría de seguridad de información.* Fides Et Ratio, 6(6), 19-30

Arcentales, D. & Caycedo, X. (2013). *Auditoría informática.* Fundación Dialnet (p. 157-163). https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

.(2023, 19 abril). *WEP, WPA, WPA2 y WPA3: diferencias y explicación* latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/wep-vs-wpa

Fernández, R. (2012, 5 diciembre). *Cortafuegos: entornos SoHo y PYMES.* IDG Communications S.A.U. https://www.dealerworld.es/pymes/cortafuegos-entornos-soho-y-pymes

Alday, J. (2022). *IMPORTANCIA DE LAS ACTUALIZACIONES DE TU SISTEMA OPERATIVO.* AS Sistemas. https://assistemas.net/importancia-de-las-actualizaciones-de-tu-sistema-operativo%EF%BB%BF/

(2023). *CLOSE YOUR CYBER EXPOSURE GAP WITH NESSUS.* Tenable Inc. https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{11596512476}-{116641138521}-{537515898224}_00026643_fy23&utm_promoter=tenable-hv-brand-00026643&utm_source=google&utm_term=nessus&utm_medium=cpc&utm_geo=latam&gclid=Cj0KCQjwsIejBhDOARIsANYqkD2OZ6w7ciFHmy_ZZojw9n1zgFOPaUhJkaRGE76GWqxhIl256Yop_yIaAjw7EALw_wcB

(2022). *Tenable Nessus Expert to provide complete visibility across modern attack surfaces.* Enterprise It World. https://www.enterpriseitworld.com/tenable-nessus-expert-to-provide-complete-visibility-across-modern-attack-surfaces/

(2023). *Plugins.* Tenable Inc. https://www.tenable.com/plugins

(2023). *EL CONOCIMIENTO ES PODER.* Desarrollo Tecnológico Empresarial https://detecemp.com/Tenable-Nessus.html