Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

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 19 de junio del 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 $25,000 (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

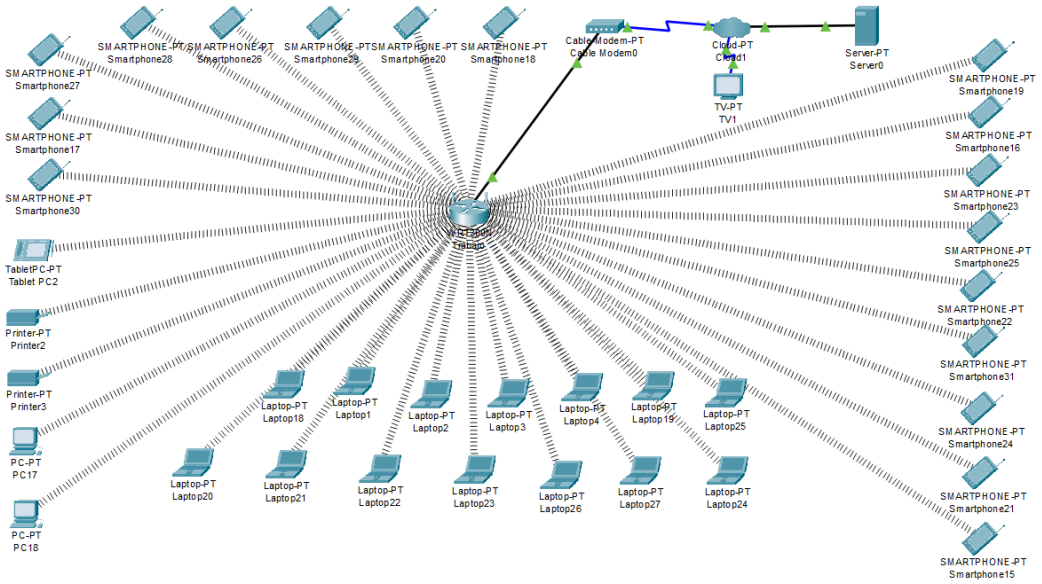

Figura 1. Topología original de la red inventariada para Pogen.

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:

Plugins de Severidad Media			
Plugin	**Nombre**	**CVSS**	**Descripción**
11213	HTTP TRACE / TRACK Methods Allowed	5.3	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. Los atacantes pueden aprovechar esto mediante la creación de una cadena de certificados maliciosos que desencadena un uso exponencial de recursos computacionales.
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.
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.
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	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.
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, 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.

Tabla 1: Inventario de vulnerabilidades de Severidad Media, Fuente: Tenable (2023)

Plugins de Severidad Baja			
Plugin	**Nombre**	**CVSS**	**Descripción**
11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	3.3	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.

Tabla 2: Inventario de vulnerabilidades de Severidad Baja, Fuente: Tenable (2023)

Plugins de Severidad Alta			
Plugin	**Nombre**	**CVSS**	**Descripción**
35291	SSL Certificate Signed Using Weak Hashing Algorithm	7.5	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 3: Inventario de vulnerabilidades de Severidad Alta, 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 y 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 redirijen 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 sensores reportaron datos erróneos el 1 y 2 de abril del año en curso. La falla no fue causada por un ataque, ni filtración de los datos, lo que sucedió fue que el servicio Legacy utilizado tiene un software y hardware obsoleto, se saturó de datos y empezó a subir valores erróneos a la base de datos. Ante esta falla se optó por migrar el servidor a otra plataforma y 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.

No obstante, Pogen si ha tenido buenas prácticas de ciberseguridad que le permiten mantenerse en un nivel no tan propenso a que sufran malas consecuencias, tales como:

Buenas prácticas de ciberseguridad	Malas prácticas de ciberseguridad
Utilizan certificados respaldados para su página web	No tienen Firewall
Sus datos son encriptados por AWS	Todos utilizan la misma red (no hay subredes dedicadas)
Sólo gente autorizada tiene acceso a los datos Utilizan el protocolo DNSSEC ofrecido por IONOS	Contraseñas inseguras
Saben identificar correos de spam y phishing	Contraseñas inseguras

Tabla 4: Buenas y malas prácticas de ciberseguridad en Pogen. Fuente: Elaboración Propia.

A continuación, se presentarán las vulnerabilidades de forma más detallada.

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 5: Anomalías o vulnerabilidades y su localización. Fuente: Elaboración Propia.

Plan de mitigación

I. Solución de vulnerabilidades

A. Propuestas de solución

Como se mencionó con anterioridad, el router WiFi cuenta con el protocolo WEP, el cual entre los protocolos de seguridad es el más vulnerable, por lo tanto una buena solución sería cambiar este protocolo por uno más reciente que pueda ser compatible con el router, como WPA2 o WPA3. WPA2 asegura que los datos enviados o recibidos sobre tu red inalámbrica estén encriptados, y sólo las personas con la contraseña de la red puedan tener acceso a ella. Para Pogen, le convendría más el modo empresarial: WPA2-EAP (Okta, 2022). WPA3 puede ser un caso un poco más complejo. Si bien es el protocolo más nuevo y ofrece mayor seguridad (diseñada para encriptar datos usando un frecuente y automático tipo de encriptación llamado Perfect Forward Secrecy) no ha sido adoptado ampliamente aún. No todo el hardware soporta WPA3 automáticamente, y usar este protocolo requiere de vez en cuando actualizaciones costosas (Ghimiray, D., 2022).

Una implementación de firewall sería esencial, más que nada por la falta de uno en la topología de red, para la prevención de tráfico que pueda ser malicioso o simplemente sospechoso. De acuerdo con el RFC proporcionado por IETF escrito por Freed, N. (2000), los firewalls pueden actuar como punto final y reenvío de protocolos (por ejemplo, un cliente/servidor SMTP o un agente proxy web), como filtro de paquetes, o una combinación de ambos. Su uso dependería de los intereses de la empresa.

Actualmente en Pogen cuentan con dispositivos que no han sido actualizados, sus ordenadores cuentan con sistemas operativos tales como MacOS, Windows y Linux. Dependiendo del área es el sistema operativo utilizado, Data y Sistemas utilizan Linux y las demás áreas utilizan Windows o MacOS. Para sus smartphones, hay una variedad tanto de

iPhones (con iOS) y dispositivos Android. Finalmente, la tablet en cuestión que se usa es un iPad, utilizada por el dueño para hacer anotaciones en juntas.

Estas son las versiones actuales de cada sistema operativo, y que se recomienda tenga cada dispositivo para su funcionamiento óptimo:

- MacOS Ventura 13.4 para ordenadores de la marca Apple (Apple Support, 2023).
- Windows 11, versión 22H2 (Windows Support, 2023)
- Linux con distribución Ubuntu versión 22.04.2 LTS o 23.04 (Ubuntu, 2023)
- iOS 16.5 y iPad OS 16.5 para iPhone 8 en adelante, todos los iPad Pro, iPad Air (tercera generación y posteriores), iPad (quinta generación y posteriores) y y iPad mini (quinta generación y posteriores) (Apple Support, 2023).
- Android 12 para dispositivos Android (Android, 2023).

Se detectó que las contraseñas eran débiles. Por ende se eleva el nivel de vulnerabilidad para ataques. Para evitar este problema, puede haber una solución tan sencilla como elaborar contraseñas que sean distintas y a su vez más difíciles de descifrar, recursos pueden ser la alteración de mayúsculas y minúsculas. Pero también el uso de palabras no tan correlacionadas o bien algún método de cifrado que no sea lo suficientemente predecible. Pero otro método más técnico en caso de no querer cambiar contraseñas o tenerlas lo más simples posible, sea mediante un autentificador de 2 o multifactores. Por definición, una autentificación es el uso de uno o más mecanismos que prueban que eres quien dices ser. Una vez que se valida la identidad de una persona o una máquina, el acceso es otorgado. Dos tipos de autentificadores más utilizados son los biométricos, el de 2-factores y el uso de Tokens (Aloul, F., Zahidi, S., El-Hajj, W., 2009).

Otra alternativa para las contraseñas, es implementar un gestor de contraseñas, incluir un gestor de contraseñas puede tener muchos beneficios, los gestores de contraseñas ayudarán a evaluar las contraseñas actuales y ofrecer recomendaciones para que sean más seguras, también utilizan cifrados AES-256 bits, disminuyendo los ciberataques (Terol, 2023).

Pogen utiliza OpenSSL, ya que este lo usan porque cuentan con un servidor local para hacer pruebas. Una solución podría ser cambiar de certificado TLS/SSL (Secure Sockets Layer/Transport Layer Security). De acuerdo con Amazon Web Services (2023), existen otras alternativas tal como EV SSL/TLS (usado por empresas para proteger a los usuarios contra terceros no autorizados), OV SSL/TLS (que contiene información empresarial verificada y puede ser inspeccionado por el navegador, además de tener un proceso de investigación menos estricto), para el caso de la PyME sería más recomendable el OV SSL/TLS ya que es más asequible y con autenticación menos rigurosa. En caso que el costo de los certificados sea muy elevado, se puede recurrir a un cambio de librería, como LibreSSL o wolfSSL.

Además, otra vulnerabilidad es la impresora utilizada por el director, la cual utiliza un servidor Telnet que transmite la información en texto plano, sin encriptar. La recomendación es cambiar a un servidor SSH, pero al ser una impresora EPSON, estas no cuentan con la opción de cambiarse a un servidor SSH. Ante esto, EPSON implementó Epson Email Print que funciona con modelos seleccionados manufacturados de 2013 en adelante, este es un servicio para enviar correos a la impresora y que está los imprima, este servicio cuenta con el protocolo Protocolo XMPP via puerto 5222 que utiliza conexiones encriptadas a través de TLS (ionos, s.f.).

B. Regulaciones y operativos involucrados

En México mediante el Código Penal Federal (2007), se monitorea aquellos delitos financieros, de seguridad de información y uso de la tecnología, como se muestra en el Artículo 211 bis 1, que dice:

- Artículo 211 bis 1: Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

La norma NMX-I-27001-NYCE-2015 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en el contexto de la organización. Esta Norma Mexicana también incluye requisitos para la valoración y tratamiento de riesgos de seguridad de la información a la medida de las necesidades de la organización. (NYCE, 2015). Esta norma coincide con la ISO/IEC 27001:2013 "Information Technology — Security Techniques — Information Security Management Systems — Requirements." En base a lo proporcionado por ISO (2022), esta norma proporciona a las empresas de cualquier tamaño y de todos los sectores de actividad orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

C. Topología renovada

La topología descrita durante la etapa de exploración de vulnerabilidades y dispositivos incluye los equipos que están conectados a la red de la empresa (computadoras portátiles, celulares, impresoras, televisores, etc). Como actualización a esta misma, se decidió colocar un firewall entre la conexión modem-router; esto con el propósito de actuar como una línea

de defensa y filtre la red entrante y saliente, lo cual permite identificar, filtrar e inspeccionar el tráfico de paquetes y esto proporciona protección ante amenazas externas previo a un intento de vulnerar la red de la PyME.

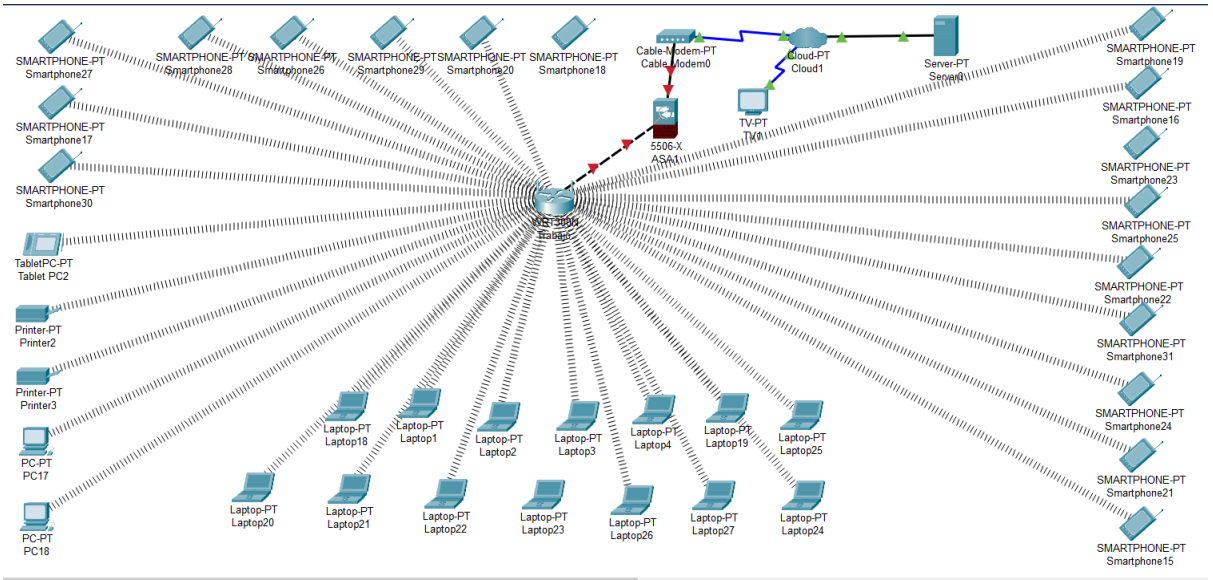

Figura 2. Topología cambiada de la red inventariada para Pogen.

En la Figura 2 se muestra la topología correspondiente, como se mencionó, únicamente se añadió un firewall previo al router de la empresa, se decidió modificar solo ésta sección de la red por la seguridad que provee su implementación dadas las condiciones con las que trabajan los colaboradores, en donde algunos usan computadoras personales y estos dispositivos son de los más vulnerables a posibles ataques o violaciones de privacidad. No se añade algún otro factor porque se considera que las propuestas van más dirigidas al apartado de logística/técnico interno como la creación de contraseñas confiables, la creación de correos y claves de manera aleatoria sin seguir un patrón en específico e incluso la implementación de una autentificación de dos factores que resguarde la información de la PyME, que es fundamental al trabajar con datos sensibles de otras empresas como es el caso de Pogen.

D. Controles CIS

Los Controles CIS (2022) son un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes.

A continuación, se implementarán los controles CIS que serían adecuados su implementación::

- *Control 1: Inventario de Dispositivos autorizados y no autorizados*

  Sólo se permite el acceso a aquellos dispositivos autorizados, y los que no estén autorizados sean detectados de tal manera podamos conocer un poco más sobre el atacante y sus propósitos con la red. Al inventariar, se contempla tener la noción de este hardware y por ende identificar alguna anomalía en caso de haber una.

- *Control 2: Inventario de Software autorizados y no autorizados*

  Similar al primer control, sólo que enfocado en el software. Esto quiere decir que se tiene un mayor control en la información y procesos a los que accede un dispositivo, tal que sólo pueda tenerse acceso al software autorizado, y en el mejor de los casos bloquear cualquier otro sitio o programa que pueda traer vulnerabilidades de red y posiblemente conlleve a un robo o espionaje de información.

- *Control 3: Gestión continua de vulnerabilidades*

  Mediante el programa de Tenable NESSUS Expert, se identificó el CVSS (Common Vulnerability Scoring System), por lo tanto se recomendaría tener un seguimiento cada determinado tiempo de este CVSS y sus Plugins proporcionados también por Tenable. Se espera a que conforme pase el tiempo estos disminuyan y se elimine en su mayoría o en su totalidad estos Plugins.

- *Control 4: Uso controlado de privilegios administrativos*

Para una mayor seguridad, es vital mejorar la seguridad de accesos a la red, es por eso que se recomienda las contraseñas únicas o un método de dos factores o multifactor.

- *Control 9: Limitación y control de puertos de red, protocolos y servicios*

  Se implementa un firewall a modo de protocolo de tal manera que verifique y valide el tráfico en el servidor. Un tráfico desconocido se puede bloquear e inclusive registrar, lo cual puede ayudar mucho a entender los propósitos de algún potencial ataque cibernético.

- *Control 14:Control de acceso basado en la necesidad de conocer*

  Sería de manera relevante tener un plan de mitigación para la amenaza de filtración de datos. Se sabe que Pogen hace uso de Amazon Web Services para este propósito.

- *Control 17: Implementar un programa de concienciación y entrenamiento de seguridad*

  Este control se basa más en esparcir la cultura de ciberseguridad con el personal de la PyME, así como conocer los niveles de peligrosidad que pueden existir al entrar a algún sitio desconocido o la falta de mantenimiento de software en los dispositivos que conllevan a más vulnerabilidades de ciberseguridad.

- *Control 20: Pruebas de penetración y ejercicios de equipo rojo*

  Finalmente, un control que es de suma importancia es este, ya que permite comprobar qué tan exitosas fueron las implementaciones pasadas en relación a la ciberseguridad y la protección de redes y dispositivos de Pogen.

E. Coste de solución

La implementación de las soluciones propuestas conlleva algunos costos que deben ser considerados. A continuación, se proporciona una estimación de los posibles costos asociados a cada una de las soluciones:

1. Cambio del protocolo de seguridad del router WiFi:

Si el router es compatible con WPA2, el cambio del protocolo podría no implicar costos adicionales, ya que generalmente es una opción disponible en la configuración del router. No se considera WP3 pues es menos común y es más probable que su implementación sea más costosa.

En el caso de que el router no sea compatible con WPA2 y se requiera adquirir uno nuevo, el costo dependerá del modelo y la marca elegida. Los routers con soporte para WPA2 suelen tener precios que varían entre 400 y 900 pesos mexicanos, dependiendo de las características y capacidades adicionales. Sin embargo, a partir de 900 pesos es posible encontrar algunos routers compatibles con WP3.

2. Implementación de un firewall:

La opción de implementar un firewall puede tener distintos costos asociados dependiendo de la elección realizada. Si optan por un firewall de hardware, deberán adquirir el dispositivo, cuyos precios van desde los 8 mil pesos mexicanos hasta más de 20 mil, dependiendo de la marca. Un firewall recomendado para organizaciones pequeñas es el SonicWall TZ350 con un costo de $13,656.

También existe la posibilidad de utilizar un firewall de software, que puede ser más económico o incluso gratuito. Algunas opciones populares de software de firewall incluyen pfSense, IPFire y Untangle. Estos suelen requerir una computadora dedicada o un dispositivo compatible para su instalación. En el caso de Untangle, es gratuito y requiere de una arquitectura AMD64, la cual es bastante común. Por lo que su implementación sería gratuita.

3. Actualización de sistemas operativos en dispositivos:

Las actualizaciones de sistemas operativos generalmente son gratuitas, aunque pueden requerir tiempo y recursos para llevarlas a cabo. Se recomienda asignar tiempo para realizar las actualizaciones en los dispositivos existentes en la empresa, teniendo en cuenta la compatibilidad de hardware y los requisitos del sistema operativo.

4. Mejora de contraseñas y autenticación de dos factores:

La mejora de contraseñas puede ser una solución económica, ya que no implica costos adicionales. Sin embargo, se debe asignar tiempo y esfuerzo para educar a los empleados sobre la importancia de utilizar contraseñas seguras y establecer políticas de cambio periódico de contraseñas. Nosotros podemos ofrecer una pequeña charla de manos de una hora explicando la importancia de las contraseñas, así como nos ofrecemos a crear infografías para que los empleados puedan aprender al respecto.

La implementación de la autenticación de dos factores puede requerir la adquisición de herramientas o servicios adicionales. Hay opciones gratuitas y de pago disponibles. Por ejemplo, el uso de aplicaciones móviles de autenticación de dos factores como Google Authenticator es gratuito, además de fácil de usar. Así como Slack, que cuenta con la opción de habilitar la autenticación de dos factores, que funciona también con Google Authenticator.

En caso de agregar una capa de seguridad extra a las contraseñas, se puede implementar un gestor de contraseñas, se recomienda NordPass Premium, una herramienta con funciones muy útiles para proteger las contraseñas dentro de una empresa; identifica contraseñas vulnerables, genera reportes y cuenta con un cifrado XChaCha20. Como tiene un costo por usuario se recomienda sólo contratarlo para aquellos empleados que tienen acceso a los datos e información más valiosa, que son 6 empleados en Pogen. Existe un plan familiar que incluye 6 usuarios, por lo que se puede optar por esta opción. Esto nos ayuda a disminuir los costos y quedarnos dentro del presupuesto establecido, ya que existe una versión Business

que es más costosa, sin embargo si Pogen decide ampliar su presupuesto, es recomendable contratarlo para todos sus colaboradores.

5. Cambio de certificado TLS/SSL

El cambio de certificado TLS/SSL puede tener costos asociados si se requiere adquirir un certificado diferente. El costo de los certificados varía dependiendo del tipo de certificado (EV SSL/TLS, OV SSL/TLS, etc.) y del proveedor. Uno de los mejores certificados tomando en cuenta la relación calidad-precio, es el SSL Starter de IONOS, que cuesta anualmente $500 (MXN). Otra alternativa es cambiar a otras librerías como LibreSSL, que son gratuitas.

6. Incremento de seguridad en la impresora:

En el caso de la impresora EPSON que no permite cambiar a un servidor SSH, la alternativa propuesta es utilizar Epson Email Print. Esta solución no implica costos adicionales, ya que se trata de un servicio proporcionado por Epson.

7. Capacitación y servicios de ciberseguridad

Se recomienda buscar capacitaciones en línea gratuitas que se ajusten a las necesidades de la empresa. Plataformas como Coursera, Udemy o LinkedIn Learning ofrecen una amplia variedad de cursos y tutoriales relacionados con la seguridad informática y las buenas prácticas en el uso de redes y sistemas.

En específico se recomienda el curso en Udemy: Essential Cybersecurity Practices for the Modern Age, que tiene una duración de menos de una hora. Se puede acceder al contenido de forma gratuita, más si se desea un certificado conlleva un costo adicional. Se considera que para Pogen es necesario que los colaboradores tengan las nociones más no necesitan el

certificado, por lo que este curso es una gran opción. Una gran ventaja de este tipo de cursos es que cada empleado puede tomarlo según su agenda.

Si se considera necesario contratar servicios de ciberseguridad, los costos asociados pueden variar significativamente dependiendo del alcance y la duración de los servicios requeridos. En México el precio promedio por servicios de ciberseguridad está entre los 8 mil y 22 mil pesos mexicanos (*¿Cuánto cuesta la ciberseguridad para empresas?, 2023*).

Se recomienda solicitar cotizaciones a diferentes proveedores y evaluar cuidadosamente los beneficios y costos de involucrar a consultores externos.

F. Análisis de costos para la solución de problemas detectados.

Solución	**Descripción**	**Costo**
1	Cambio de protocolo de seguridad del Router WiFi	Ninguno
2	Implementación del firewall	SonicWall TZ350: $13,656 Software: Ninguno
3	Actualización de sistemas operativos en dispositivos	Ninguno
4	Mejora de contraseñas y autenticación de dos factores	Mejora de contraseñas: Ninguno Autenticación (Google Authenticator): Ninguno
5	Gestor de contraseñas	NordPass Family: $682 (por 6 usuarios por año)
6	Cambio de certificado TLS/SSL	SSL Starter: $500 (un certificado por un año) Cambio de librería: Ninguno
7	Incremento de seguridad en la impresora	Ninguno
8	Desactivar reenvío de IP	Desactivarlo desde PC: Ninguno Actualizar nginx: Ninguno

9	Servicios especializados de ciberseguridad (instalación e implementación de propuestas)	$8,000 (mensual)
10	Capacitación a empleados de lo más básico de ciberseguridad	Curso en Udemy (Essential Cybersecurity Practices for the Modern Age): Ninguno
Total (aproximado):		$22,838 incluye: ● 1 certificado (1 año) ● Implementación de firewall ● Firewalls open source ● Cambio de librerías ● Cambio de contraseña ● Autenticación 2 factores ● Gestor de contraseñas (1 año a 6 usuarios) ● Servicios por parte de un profesional (1 mes)

Tabla 6: Análisis de presupuestos para cada solución a implementar.

II. Discusión de resultados

Dependiendo del nivel de seguridad al que se quiera llegar con la implementación de las soluciones propuestas, esta puede entrar en el presupuesto establecido por la PyME de $25,000 MXN. Sin embargo, es recomendable considerar las demás propuestas y sobre si valdría la pena aumentar el presupuesto establecido a fin de tener una mejor seguridad. En cuanto al tiempo de implementación, este sería de forma inmediata en su mayoría, al igual que el pago. Únicamente se considera un pago de forma anual para el certificado SSL.

Si bien, aplicar estas medidas podrían significar un costo no considerado antes por la empresa, es importante tomar en cuenta los riesgos que esto significa a mediano y largo plazo si no se realiza un cambio. De acuerdo con un estudio realizado por Kaspersky (2022), los ataques a PyMEs producen pérdidas económicas y de reputación, lo cual en conjunto

asciende hasta los 155 mil dólares en pérdidas. Y aunque pareciera que esto es difícil que ocurra, hay que considerar que las PyMEs son las que más se encuentran en riesgo, pues este mismo estudio demostró que México es el país con mayor número de ataques en América Latina, y un cuarto de las PyMEs en esta región han sido atacadas.

Asimismo, los cambios en cuanto a contraseñas y la cultura de ciberseguridad, aunque suene tedioso, también es de suma importancia, pues según la Encuesta Mundial sobre el Estado de la Seguridad de la Información (PricewaterhouseCoopers, 2018), las empresas pueden llegar a tener pérdidas de hasta 4.8 millones de dólares por incidentes de seguridad, muchos de ellos causados por métodos como la suplantación y robo de identidad y la falta de prevención. Casos que pueden ser erradicados si se mejora la cultura que se tiene.

III. Conclusiones

La elaboración de este reto ha traído consigo diversos aprendizajes que nos hacen analizar, comprender e informarnos de situaciones de riesgo dentro de una organización, empresa o uno como persona por medio de sus dispositivos, con ello se ha comprendido la importancia de un buen funcionamiento de red que incluya protocolos de seguridad, una gestión técnica en la elaboración de contraseñas/patrones y claves de acceso a correos en conjunto con lo vulnerable que resulta hoy en día la información privada de una empresa.

Con la solución propuesta en este reporte se espera que la PyME reconsidere sus estrategias y técnicas actuales en las que se encuentran trabajando y elaboren bajo su criterio un plan de acción al tomar en consideración las sugerencias de propuestas elaboradas de nuestra parte para mejorar la seguridad de su información; como tal las propuestas mencionadas son viables para su situación tanto de software/hardware como en el ámbito económico, dado que las observaciones realizadas fueron hechas a partir de vulnerabilidades que tienen una solución práctica en el mercado hoy en día y algunas incluso únicamente requieren acciones logísticas que no genera algún costo dentro de la empresa y mejoran altamente la protección de la misma red ante posibles ataques de terceros o algún filtrado de información interno.

Dado lo anterior, se estima que la máxima inversión tanto en tiempo y dinero de parte de la empresa Pogen sea aproximadamente dentro del rango $9,500 en un periodo de 4 a 6 meses por motivos de instalaciones, modificaciones internas y actualizaciones de software y hardware, además de considerar costos fijos de $500 pesos anuales por el certificado y un rango de $8,000 a $20,000 mensuales; lo cuál es una cifra que dado el tamaño de la empresa pueden permitirse invertir en ello dado el presupuesto inicial y generaría un beneficio mayormente preventivo que es lo que se busca conseguir con este plan de mitigación.

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

¿Cuánto cuesta la ciberseguridad para empresas? (2023, enero 21). cronoshare.

https://www.cronoshare.com.mx/cuanto-cuesta/servicio-ciberseguridad-empresas

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

¿Qué es XMPP? Resumen de sus funciones y ventajas. (s. f.). IONOS Digital Guide. https://www.ionos.mx/digitalguide/servidores/know-how/xmpp/#:~:text=XMPP%20son%20las%20siglas%20de,usado%20para%20la%20comunicaci%C3%B3n%20online.

(2023). *Wi-Fi Security: WEP vs WPA or WPA2*. Avast. https://www.avast.com/c-wep-vs-wpa-or-wpa2

Freed, N., (2000). *Behavior of and Requirements for Internet Firewalls*. Network Working Group. RFC 2979 (p. 1-2). https://www.ietf.org/rfc/rfc2979.txt

(2022). *Wired Equivalent Privacy (WEP): Definition & Risks*. Okta. https://www.okta.com/identity-101/wep/

(2023). *Android 12: More personal, safe and effortless than ever before*. Android. https://www.android.com/android-12/

(2023). *¿Qué versiones de macOS son las más recientes?*. Apple Support. https://support.apple.com/es-mx/HT201260

(2023). *Actualizaciones de seguridad de Apple*. Apple Support. https://support.apple.com/es-lamr/HT201222

(2023). *Obtener la actualización más reciente de Windows*. Microsoft Support. https://support.microsoft.com/es-es/windows/obtener-la-actualizaci%C3%B3n-m%C3%A1s-reciente-de-windows-7d20e88c-0568-483a-37bc-c3885390d212#:~:text=La%20actualizaci%C3%B3n%20m%C3%A1s%20reciente%20de%20Windows%20es%20Windows%2011%2C%20versi%C3%B3n,actualizaci%C3%B3n%20de%20Windows%2011%202022.

(2023). *Download Ubuntu Desktop*. Ubuntu. https://ubuntu.com/download/desktop

Aloul, F., Zahidi, S., El-Hajj, W., (2009). *Two Factor Authentication Using Mobile Phones.* IEEE. (p. 642)

Kaspersky Team. (2022, 27 junio). Las PyMEs de América Latina enfrentan un creciente número de ciberataques. *Kaspersky daily*. https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/

(Septiembre 25, 2007). *Gaceta del Senado.* Senado de México. https://www.senado.gob.mx/65/gaceta_del_senado/documento/13967

(2015). *NMX-I-27001-NYCE-2015 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-REQUISITOS (CANCELA A LA NMX-I-27001-NYCE-2009).* NYCE. https://nyce.org.mx/catalogodeestandaresnyce/producto/nmx-i-27001-nyce-2015-tecnologias-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-seguridad-de-la-informacion-requisitos-cancela-a-la-nmx-i-27001-nyce-2009/

(2022). *ISO/IEC 27001.* ISO. https://www.iso.org/standard/27001

(2022). *CIS Controls.* CIS. (p. 2-76). https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

PricewaterhouseCoopers. (2018). *Encuesta Mundial - Estado Seguridad de la Información 2018*. PwC. https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html