Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencia de Datos y Matemáticas

Auditoría de Seguridad y Plan de Mitigación: Caso Pinturas SUQRO

Análisis de Criptografía y Seguridad

Mariana Ivette Rincón Flores A01654973

Leonardo Laureles Olmedo A01659241

Carlos Mateos Pérez A01654085

Mariano Luna Tress A01734509

Daniel Isaac Núñez López A01654137

Manuel Rodríguez Rivera A01659819

en conjunto con: IPC Services

supervisado por
Alberto F. Martínez
Alejandro Parra Briones

Monterrey, Nuevo León. Fecha, 6 de mayo de 2022

1. Introducción

Como breve introducción al reto "Auditoría de Seguridad y Plan de Mitigación", se plantea que las PyMEs representan una parte importante del producto interno bruto del país y por lo tanto juegan un gran rol en la economía del país. Un ataque cibernético masivo puede en gran medida afectar en corto plazo al PIB, es por ello, que para este reto trabajaremos con la micro empresa o PYME SUQRO, a la cual se busca hacerle un plan de prevención contra este tipo de ataques mediante y como el nombre lo indica, una auditoría de seguridad y un plan de mitigación.

Pinturas SUQRO: Tienda de pinturas OSEL en Querétaro, Qro.

Misión:Comercializar y distribuir pinturas y recubrimientos de excelente calidad. Brindar el mejor servicio de atención personalizada a cada uno de nuestros clientes para ofrecerle la mejor y más rápida solución que se adapte a sus necesidades. Ofrecer la solución económica para los proyectos de nuestros clientes, ofreciendo productos de la más alta calidad en el mercado.

Visión: Romper paradigmas en la industria de la construcción y ser reconocidos como una empresa líder en la comercialización y distribución de pinturas y recubrimientos de excelente calidad.

Dueño/director: Salvador Ugalde Jiménez - Año en el que se creó: 2018

El tipo de PyME a analizar en este caso de estudio puede ser ubicada en el conjunto de microempresa, de acuerdo al INEGI y la Secretaria de Economía. Recordemos que, de acuerdo con [13], el número de colaboradores con los que cuenta una PyME cae en el rango de 1 colaborador a 5 colaboradores.

De acuerdo con el sondeo *Combatir el cibercrimen en la nueva realidad* realizado en junio de 2020 por KPMG [1] en México, los ataques a las empresas han aumentado.

"Tras la pandemia, 79 % de las organizaciones enfrentó un mayor número de ciberataques en México. Asimismo, 97 % de las empresas mencionó incrementos de entre 6 % y más de 15 % de los ciberataques bajo la coyuntura actual.
Seis de cada diez (60 %) organizaciones han experimentado ataques de phishing en el último año, siendo la amenaza más común. Los virus y ransomware son el segundo más frecuente: 43 % de las empresas recibieron este tipo de ataques" [KMPG, 2020].

De lo que indica la PyME, ellos estan dispuestos a invertir una cantidad que no supere el presupuesto para TI. De acuerdo con [16], el autor hace una recomendación de presupuesto entre 800-1200 USD ya que " Es importante entender que todo incidente de seguridad va a costarle dinero a la empresa y, dependiendo de la magnitud, en la mayoría de los casos este costo es muchísimo mayor a lo que cuesta prevenirlo",[Pastoriano,2020]

Colaboradores (5 colaboradores):

- Director: Toma de decisiones estratégicas, financieras y comerciales de la empresa
- Asistente: Asistente administrativo general y de compras

- Ventas: Hace ventas, inventarios, controles de caja
- Administración: Conciliación de cuentas
- Mantenimeinto: Limpieza

Presupuesto para TI (mensual): $15,000 MXN

2. Inventario

2.1. Tabla-Inventario

Inventario			
#	Marca	Modelo	No.Serie
1	Lenovo	Ideacentre Aio 520-22IKU	MP1F3BFF
2	Dell	OptiPlex 3080	CTYG8A00
3	Samsung	Galaxy Tab S6 Lite	R52R4080YLW
4	Microsoft	365 Business Basic	NA
5	Google	G Suite	NA
6	Bind	ERP + CrecimientO	NA
7	Apple	MacBook PRO 14" 2021	NXTYQUEBEC6JIQF

Cuadro 1: Tabla de Inventario con Marca, Modelo y No. de Serie

En esta tabla podemos observar el inventario de la PyME, el cual cuenta con 4 dispositvios, 3 computadoras y 1 tablet. El cual cuenta con la marca, modelo y el no.serie.

2.2. Tabla-Inventario

Inventario			
#	CPU	Capacidad de almacenamiento	T. Video
1	Intel Pentium 4415	1 TB HDD	Integrada
2	Intel Core il5-10500T	256 GB SSD	Integrada
3	Exynos 9611	64 GB SSD	No
4	NA	NA	NA
5	NA	NA	NA
6	NA	NA	NA
7	M1 pro	1 TB SSD	Integrada

Cuadro 2: Tabla de Inventario con Almacenamiento y GPU

En esta tabla se ven los procesadores de cada dispositivo, los primeros dos son Intel Core's, que utilizan las computadoras de escritorio, luego sigue un procesador exynos que utiliza una tablet, y por último, se muestra el procesador de la laptop.

2.3. Tabla-Inventario

Inventario			
#	OS	Colab. con acceso.	Uso
1	Windows 10	1,3,4	Venta, inventarios, compras
2	Windows 10	1,3,4	Venta, inventarios,compras
3	Android 10	1,2,3,4	Ventas móviles
4	NA	1,2,3,4	Administración general
5	NA	1,3,4	Administración general
6	NA	1,2,3,4	Administración general
7	MacOs Monterey	1	Administración general

Cuadro 3: Tabla de Inventario con OS, Colaborador y Uso

En esta tabla se muestran los sistemas operativos de los dispositivos, las primeras dos cuentan con Windows, la tablet con Android y la laptop con MacOS.

2.4. Tabla-Colaboradores

Colaboradores		
#	Puesto	Acción
1	dirección	tomar decisiones estratégicas, financieras y comerciales de la empresa
2	asistente	asistente administrativo general y compras
3	ventas	hace ventas, inventarios, controles de caja
4	administración	conciliación de cuentas
5	mantenimiento	limpieza

Cuadro 4: Tabla de Colaboradores con su Puesto y Acción

En esta tabla, podemos observar los colaboradores que trabajan actualmente con la PyME, existen 5 puestos..., dirección, asistente, ventas, administración, mantenimiento; lo mas importante de esta tabla, es que están enumerados para la identificación del uso de los dispositivos en las tablas anteriores.

3. Topología de la red

En la Figura 1 se tiene la topología de red de la PyME Pinturas SUQRO, donde se muestran los equipos de cada uno de los colaboradores, siendo el equipo Lenovo utilizado por el director, el colaborador de ventas y administración, la cual se conecta de manera alámbrica al módem, de igual manera, el equipo Dell se conecta de manera alámbrica al módem el cuál es utilizado por los mismos colaboradores del equipo Lenovo. También encontramos dispositivos inalámbricos que se conectan al módem en una red inalámbrica abierta, es decir, sin que se use una contraseña de acceso. El dispositivo Samsung es utilizado por el director, el asistente y los colaboradores de ventas y administración, el equipo Apple pertenece al director que es el encargado de tomar decisiones estratégicas, financieras y comerciales de la empresa, se conecta de manera inalámbrica, y finalmente, el módem se conecta a un Proveedor de Servicios de Internet que ofrece su servicio vía cable coaxial, donde cada colaborador conectado al router puede hacer sus actividades en Internet.

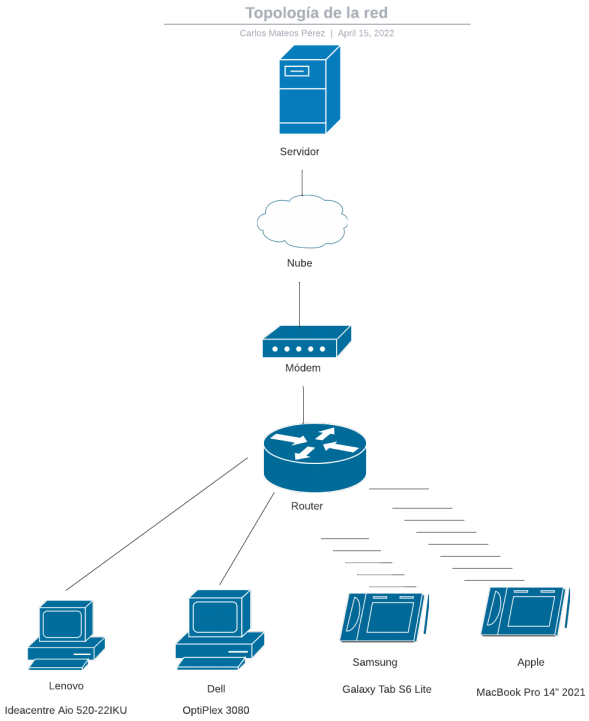

Figura 1: Topología original de la red inventariada para la PyME Pinturas SUQRO

En el tipo de información que maneja la PyME, se encuentran los datos de facturación, que reflejan toda la información de las operaciones de compraventa de la empresa. Dentro de los datos de facturación se encuentran:

- Datos bancarios.
- Direcciones fiscales y no fiscales (para hacer entregas).
- Datos fiscales del emisor y del cliente.
- Concepto.
- Tipo impositivo.
- Información del Registro Mercantil (licencias que acreditan su calidad de comerciante)

4. Plan de evaluación

4.1. Herramientas para el plan de evaluación

- Netsparker es una aplicación web que encuentra e informa de las vulnerabilidades de una aplicación web, como la inyección de SQL y de cross-site scripting (XSS) en todos los tipos de aplicaciones web, independientemente de la plataforma y de la tecnología con la que están construidos. [17]

- Acunetix es una herramienta de seguridad de aplicaciones web automatizada. Es capaz de escanear cualquier sitio web o aplicación web que es accesible a través del protocolo HTTP / HTTPS. Proporciona herramientas de penetración manuales para pruebas particulares, ya que no puede realizar todas las pruebas de manera automática. [11]

- Intruder es un scanner online de vulnerabilidades que encuentra debilidades de ciberseguridad en la infraestructura individual del cliente, para evitar costosas infracciones de datos. [14]

- Nexpose es un software creado y mantenido por la compañía RAPID7, que permite detectar y evaluar las vulnerabilidades que existen dentro de una infraestructura de red. Se instala en las instalaciones de la compañía en la que se adquiere. [3]

- Tripwire.- Tripwire es un software encargado de detectar intrusiones al sistema del equipo en el que está instalado. Basado en Open Source y desarrollado por la empresa que lleva el mismo nombre, Tripwire se encarga de monitorear y alertar al usuario de los cambios que se llevan a cabo en los ficheros de un sistema. Esto lo logra comparando la forma de archivos y directorios con una base de datos tomada al momento de su instalación. [21]

- Aircrack.- Aircrack es una suite de software de seguridad inalámbrica, este fue desarrollado por Thomas d'Otreppe, este software protege nuestro sistema de tráfico inusual analizando paquetes de redes, recupera contraseñas WEP y WPA/WPA2-PSK. Este software trabaja con Linux, preferentemente, aunque hay una versión para Windows, esta NO es recomendada, ya que presenta varios problemas de optimización. [12]

- Microsoft Baseline Security Analyzer (MBSA).- Esta es una herramienta de seguridad discontinuada (es decir, no funciona con sistemas operativos actuales, pero si con sistemas operativos hasta antes de 2012). Ayuda a pequeños y medianos negocios a determinar su estado de seguridad por medio de actualizaciones de seguridad, en la que la versión de turno era evaluada y corregida de manera periódica. Las actualizaciones de seguridad están determinadas por la versión de MBSA que utilizara el Agente de actualización de Windows, presente en las computadoras con Windows desde Windows 2000 Service Pack 3. [18]

4.2. Tabla de evaluación

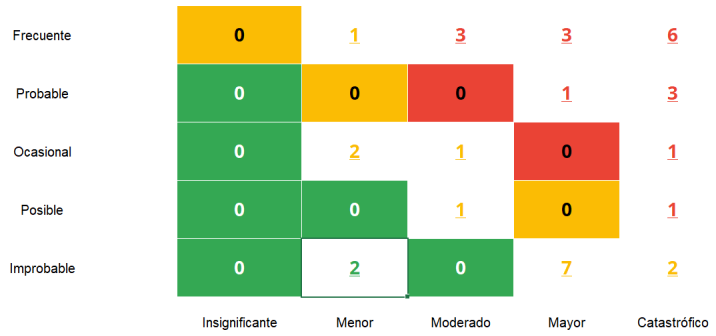

Figura 2: Matriz de riesgos de la PyME

Esta matriz está compuesta por 33 riesgos, los cuales están organizados de la siguiente forma:

1. Robo de contraseñas: Riesgo medio
2. Contraseñas inseguras: Riesgo alto
3. Contraseñas sin periodicidad de caducidad: Riesgo alto
4. Permitir intentos ilimitados de contraseñas: Riesgo alto
5. Usuarios comparten contraseñas: Riesgo alto
6. No tener bloqueo automático por inactividad: Riesgo alto
7. Interrupción en los servidores de Bind (software de facturación): Riesgo medio
8. Falla en el firewall de OneDrive: Riesgo medio
9. Computadoras con conexiones remotas permitidas: Riesgo medio
10. No tener una política zero trust: Riesgo alto
11. Usar celulares personales: Riesgo alto
12. Conectar dispositivos a la red: Riesgo alto
13. Riesgo de que alguien externo esté monitoreando paquetes del WiFi: Riesgo medio
14. Caída del servicio del proveedor de internet: Riesgo alto
15. Saturación de la banda ancha del internet: Riesgo alto
16. Utilizar WPA2: Riesgo alto
17. Capturación errónea de datos: Riesgo medio

18. Router a la vista de cualquier persona: Riesgo alto
19. Cables conectados a las computadoras no señalizados: Riesgo alto
20. Se descompone el router: Riesgo bajo
21. Se pierde un teléfono: Riesgo alto
22. No tener activas las actualizaciones del antivirus: Riesgo medio
23. No pagar el antivirus: Riesgo medio
24. No contar con seguro de reparación de dispositivos: Riesgo medio
25. No tener un sistema de monitoreo en los principales procesos: Riesgo medio
26. No tener encendidas todas las auditorías: Riesgo medio
27. No tener los parches de seguridad: Riesgo medio
28. No tener cifrado el disco duro: Riesgo medio
29. No hay respaldos periódicos: Riesgo alto
30. No tener los datos cifrados en la nube: Riesgo alto
31. Tener las llaves de encriptación a la vista: Riesgo alto
32. No tener inhabilitados puertos de USB: Riesgo alto
33. Compartir archivos por el router sin usar internet: Riesgo alto

4.3. Vulnerabilidades en el inventario

En la empresa se ocupan diversos softwares y sistemas operativos, a continuación...

- En algunas de las computadoras inventariadas se ocupa Office, el cual tiene una vulnerabilidad debido a su versión Windows 10 21h2, que de acuerdo con el CVE-2022-26903, tiene una vulnerabilidad dentro del Windows Graphics Component Remote Code Execution, reportada con un nivel de peligrosidad de 9.3 (alto). [19].
- En algunos de los dispositivos inventariados se ocupa Android, versión 10, el cual de acuerdo con el CVE-2022-27572, tiene una vulnerabilidad dentro de la función parser ipma de la librería libsima, reportada con un nivel de peligrosidad de 10 (alto) [9].
- En algunas de las computadoras inventariadas se ocupa Office, el cual tiene una vulnerabilidad debido a su versión Windows 10 21h2, el cual de acuerdo con el CVE-2022-26903, tiene una vulnerabilidad dentro del Windows Graphics Component Remote Code Execution, reportada con un nivel de peligrosidad de 9.3 (alto) [10].
- Los equipos Windows cuentan con el antivirus McAfee versión 5.7.5, de acuerdo con el CVE-2021-31854, tiene una vulnerabilidad dentro del Injection Vulnerability in McAfee Agent (MA), reportada con un nivel de peligrosidad de 9.3 (alto) [6].
- En algunos de los dispositivos inventariados se ocupa SAS, un ERP en el cuál se guardan los datos de los clientes, el cual de acuerdo con el CVE-2021-41569, tiene una vulnerabilidad dentro del SAS/Intrnet 9.4 build 1520, reportada con un nivel de peligrosidad de 5 (medio) [7].
- Los pagos en efectivo se reciben a través de MercadoPago (Mercadolibre), el cual de acuerdo con el CVE-2014-5658, tiene una vulnerabilidad dentro de la aplicación de MercadoLibre 3.8.7 para Android , reportada con un nivel de peligrosidad de 5.4 (medio) [5].
- Como backup para los pagos en efectivo se cuenta con terminal de Zettle (PayPal), el cual de acuerdo con el CVE-2013-7202, tiene una vulnerabilidad dentro de la clase WebHybridClient en PayPal 5.3, reportada con un nivel de peligrosidad de 6.8 (medio) [4].
- Se cuenta con información en la nube de OneDrive, el cual de acuerdo con el CVE-2022-23255, tiene una vulnerabilidad dentro de la Microsoft OneDrive for Android Security Feature Bypass Vulnerabilty, reportada con un nivel de peligrosidad de 4.6 (bajo-medio) [2].
- Se cuenta con información en la nube de ERP Bind, el cual de acuerdo con el CVE-2022-0635, tiene una vulnerabilidad dentro de la versión Bind (software de facturación) 9.18.0, reportada con un nivel de peligrosidad de 5 (alto) [8].

4.4. Vulnerabilidades en la topología de la red

Entre las vulnerabilidades que se encontraron al analizar la PyME se encuentra el riesgo que alguien externo este monitoreando paquetes del WiFi, este riesgo se encuentra asociado a la conexión de red. La caída de servicio del proveedor del Internet es otro riesgo asociado a la conexión de red que podría afectar el funcionamiento de la PyME, sucede varias veces al mes y debido al uso que tiene el Internet dentro de la organización podría llegar a generar pérdidas significativas. La saturación de la banda ancha del Internet es otro riesgo que se podría llegar a presentar, está relacionado con el proceso de conexión de red, sucede varias veces al mes y al estar relacionado con el Internet al igual que el riesgo anterior, podría tener afectaciones económicas. El no tener inhabilitados puertos de USB es un riesgo relacionado a la conectividad de red, se presenta varias veces al mes y puede llegar a ser muy costoso ya que puede ocasionar brechas fuertes de información sensible. Compartir archivos por el router sin usar Internet es otro riesgo relacionado a la conectividad de red, sucede varias veces por mes y ya que se estarían dejando puertos abiertos pudiendo provocar algún ataque que podría llegar a ser en extremadamente costoso.

Al momento de revisar la configuración del router, nos percatamos de que se está ocupando el protocolo WPA2, el cual de acuerdo a Terol y Chavarri [20] hace más evidentes las vulnerabilidades de este al ser comparado con el nuevo protocolo WPA3, el cual ofrece un mayor nivel de seguridad incluso cuando la clave de conexión no lo es.

4.5. Procesos en el flujo y control de la información

En nuestra PyME el flujo de información empieza desde que el usuario entra a la página web y tiene la intención de realizar una compra, para esto debe proporcionar información personal así como datos bancarios, sin embargo estos datos son procesados o por Mercadopago o PayPal, es decir la empresa no se queda con los datos bancarios mas que con el número de autorización, esto significa que la PyME no corre riesgo de robo de información bancaria de los clientes; esto es gracias a que ambas empresas cuentan con un sistema de fraude robusto y soluciones compatibles con el PCI DSS lo cual significa que tienen un nivel base de protección para los tarjetahabientes y ayuda a reducir el fraude y la la filtración de datos, esto se logra gracias a que se transmite de forma segura la información, se almacenan los datos de acuerdo a los 12 requisitos normativos del estandar PCI, se validan anualmente el cumplimiento de los controles de seguridad.

4.6. Planes de contigencia

Respecto a un plan de contingencia, en caso de un filtrado de información no se tiene un plan preestablecido en cuanto ataques cibernéticos, aunque si se trata de un filtrado por parte de un empleado existen NDA (non disclosure agreements). Un filtrado de información o pérdida de información comúnmente ocurre o por error humano o por algún desastre natural; en cuanto a error humano, este puede ser responsable hasta del 32 % para la pérdida de datos, englobando corrupción de software, virus, y fallas en el hardware (siendo este el principal problema); en cuanto a desastres naturales, este solamente es responsable por 3 % para la pérdida de datos, sin embargo, vale la pena prevenir la posibilidad de perder toda la información debido a incendios, inundaciones, descargas eléctricas, terremotos, caídas de estructuras, etc.

Nuestro equipo de trabajo recomienda un plan de contingencia simple que implica tener un sistema de respaldos y restauraciones para los datos, esto se debe a que la empresa que estamos trabajando solamente tiene los datos en ONEDRIVE y ERP, por lo que si fallan estos servicios, no se tienen copias propias de la información en físico, esto es un problema, ya que, al depender de servicios externos también dependes de la buena/mala seguridad de los mismos.

En caso de caída de servicios externos, sí se tiene un plan, puesto que se pueden utilizar todas las aplicaciones que se requieren para una venta a través de una tablet con datos celulares. Igualmente, se tienen procesos manuales que permiten realizar las mismas tareas que Saas (software relacionado con ventas) en lo que se restablece el servicio nuevamente.

Se cuenta con respaldo de datos en caso de algún fallo de disco duro de la empresa; en caso de documentos generales, publicidad, registros de estados de cuenta, cotizaciones, listas de precios, imagen de marca, etc. En OneDrive, y en cuanto a información de clientes, información de proveedores, inventario, precios, movimientos, control de gastos, facturación, etc. en la nube de ERP Bind. Consideramos que contar con este tipo de respaldo no es suficiente para la empresa, debido a que se está confiando plenamente en servicios externos, es decir, no cuentan con un respaldo propio, y se tiene confianza en la seguridad de servicios externos (OneDrive, ERP), por lo que un error implicaría la pérdida total de la información, y tener los datos dentro de la empresa significaría mayor seguridad y confianza.

4.7. Nociones

Hablando de cultura de ciberseguridad, la PyME tiene las nociones básicas. Sin embargo, hay varios aspectos que podría mejorar, los de mayor urgencia son enumerados a continuación:

- El primer ejemplo es que solo los equipos que utilizan Windows cuentan con un antivirus (McAffe), sin embargo, todos los equipos tienen permitido compartir información mediante router.
- Otro ejemplo de su falta de cultura de la ciberseguridad es que nuestra empresa NO cuenta con un respaldo de sus datos, ni cuenta con una certificación ISO de ningún tipo.
- Los empleados únicamente tienen una ligera noción acerca de que es el phishing y las extorsiones, acerca de algún otro tipo de malware no se tiene conocimiento.
- No se tienen planes de contingencia en caso de un filtrado de información, en caso de una caída de los servicios externos se cuenta con procesos manuales para realizar sus procesos y una tablet.

Podemos observar que, el punto que tienen en común la mayoría de los puntos mencionados anteriormente, es que estos podrían ser fácilmente solucionados con una inversión mínima en ciberseguridad: se podría descargar un antivirus a todas las computadoras, se podría capacitar a los empleados en temas de ciberseguridad, esto no representaría mayor problema, ya que en la actualidad existen una gran cantidad de cursos gratuitos en línea.

Probablemente, la instalación de servidores propios sería el gasto más significativo de nuestra PyME. Sin embargo, este se podría arreglar de dos maneras posibles: seguir utilizando un servidor ajeno a la empresa, o bien, contactar con nuestro socio formador para la instalación de servidores, así como la protección de estos (antivirus, temas de seguridad y capacitación de empleados, etc).

4.8. Vulnerabilidades o Anomalías y sus localizaciones

Anomalía o vulnerabilidad	**Localización**
Utilización de WPA2 en el router	Router.
Contraseñas inseguras	Inicio de sesión a las aplicaciones web, computadoras y servicios de externos.
Depender de Bind para la facturación	Página web.
Uso de dispositivos ajenos a la empresa en el mismo router	Infraestructura de la red.
Solo contar con un proveedor de internet	Infraestructura de la red.
Solo contar con un router	Infraestructura de la red.
Usar el teléfono personal como de trabajo	Infraestructura de la red.
No tener cifrado el HDD	Hardware de los dispositivos.
Firewall mal configurado	Software de la nube.
Puertos de red no utilizados abiertos	Dispositivos electrónicos.
Intentos ilimitados de las contraseñas	Inicio de sesión.
Usuarios comparten contraseñas	Inicio de sesión.
No hay respaldos periódicos de datos	Nube/Hardware.
No tener señalizados los cables conectados a las computadoras	Hardware.
Puertos USB habilitados	Hardware.
No cifrar los datos que se suben a la nube	Nube/OneDrive.
Tener las llaves de encriptación a la vista	Archivos en hardware o nube.
No actualizar el antivirus	Software.
No pagar el antivirus	Software.
No tener seguro de reparación para los dispositivos	Hardware.
No tener sistema de monitoreo de los principales procesos	Software.
No contar con auditorías (monitoreo de logins)	Inicio de sesión y software.
Conectar dispositivos personales a la red	Infraestructura de la red.

Cuadro 5: Se detallan las anomalías o vulnerabilidades actuales y posibles, y su respectiva localización

5. Plan de mitigación

5.1. Solución a los puntos evaluados

Identificamos 33 posibles riesgos o vulnerabilidades dentro de la PyME, los cuales, se asocian a diversos procesos/áreas como lo son: inicio de sesión, conectividad, conexión de red, proceso de compra, seguridad física, mantenimiento de infraestructura, almacenamiento de datos, seguridad tecnológica y conectividad de red. A continuación se dará una propuesta de solución para cada uno de ellos. (Los costos se mostratán en la Tabla 5.4)

Inicio de sesión

1. Robo de contraseñas: Dentro de este apartado encontramos que se puede solucionar utilizando una clave de autenticación de dos pasos, y mejorando la cultura de prevención de phishing, whaling y vishing.

2. Contraseñas inseguras: Encontramos que las contraseñas no tienen un protocolo de seguridad, tal como: contar con un mínimo de caracteres, uso de caracteres especiales, uso de números y letras, prohibir el uso sucesivo de números, uso de mayúsculas y minúsculas, no usar nombres, no relacionarla con el nombre de usuario o algún otro dato relacionado a la empresa.

3. Contraseñas sin periodicidad de caducidad: Es necesario realizar cambios periódicos debido a que esto puede prevenir un descuido de algún empleado, como anotar la contraseña en algún lugar o dársela a otro empleado, logrando así una mayor seguridad.

4. Permitir intentos ilimitados de contraseñas: El permitir muchos intentos sin sanción puede dar paso a un ataque de fuerza bruta, por lo que limitar los intentos posibles para el inicio de sesión (3 intentos) y después de los permitidos bloquear el acceso del usuario y forzar un reseteo de credenciales.

5. Usuarios comparten contraseñas: Tener una cultura de seguridad y tener estrictamente prohibido compartir las contraseñas, además que con el punto 3, este mal hábito se minimiza.

6. No tener bloqueo automático por inactividad: Definir un timer para que los dispositivos se bloqueen automáticamente.

Conectividad

7. Interrupción en los servidores de BIND: Contar con un aplicativo alterno para poder continuar con los servicios de facturación y que pueda usarse fuera de línea.

8. Falla en el firewall de OneDrive: Contar con una alternativa para el almacenamiento de datos, es decir en físico (discos duros), o en la nube (google drive).

9. Computadoras con conexiones remotas permitidas: No permitir el uso de programas de escritorio remoto, ya que se dejan abiertos puertos de las computadoras que pueden ser utilizados para un ataque.

10. No tener una política zero trust: El tener acceso a los dispositivos de la empresa no implica que los pueda ocupar esa persona ya que se debe dar de alta por el administrador para que tenga acceso.

11. Usar celulares personales: Prohibir el uso de celulares personales y brindarle a los empleados celulares exclusivamente para la empresa, donde solamente podrán usar sus cuentas de trabajo.

12. Conectar dispositivos a la red: Apoyarse en el punto 10, es decir que el administrador solamente dará acceso a dispositivos autorizados.

    Conexión de red

13. Riesgo de que alguien externo esté monitoreando paquetes del WiFi: No permitir la conexión a dispositivos no autorizados, tener un software de monitoreo que revise las nuevas conexiones.

14. Caída del servicio del proveedor de internet: Contar con otro proveedor, ya sea local o incluso satelital.

15. Saturación de la banda ancha del internet: Apoyarse del punto 14, así como contratar paquetes empresariales y no de hogar.

16. Utilizar WPA2: De acuerdo con las vulnerabilidades del WPA2, la recomendación es actualizar el router y los dispositivos a WPA3.

    Proceso de compra

17. Capturación errónea de datos: Verificar los datos antes de enviarlos pasando por varios filtros de revisión.

    Seguridad física

18. Router a la vista de cualquier persona: Resguardarlo en algún mueble con candado logrando así que ninguna persona más que el administrador tenga acceso a él.

19. Cables conectados a las computadoras no señalizados: Etiquetar todos los cables a la vista para una mejor organización y en caso de alguna modificación a la conexión saber que cable es el correcto.

    Mantenimiento de la infraestructura

20. Se descompone el router: Contar con un router de repuesto y siguiendo el punto 14

21. Se pierde un teléfono: Contar con un servicio de eliminación de datos a distancia automático, además de contar con rastreo GPS.

22. No tener activas las actualizaciones del antivirus: Revisar constantemente las actualizaciones del software

23. No pagar el antivirus: Tener un recordatorio anual de pagar la licencia

24. No contar con seguro de reparación de dispositivos: Contratar un servicio externo de servicio técnico para los dispositivos como lo puede ser Asurion

25. No tener un sistema de monitoreo en los principales procesos: Buscar un software que permita monitorear la página web, el sistema de facturación, nubes, además de la infraestructura para que el estado de todo equipo/servicio se pueda ver desde una aplicación.

26. No tener encendidas todas las auditorías: Tener activas las opciones del registro de datos, como registro de cuándo hay un login, cuando se abrió qué software, etc. Tener monitoreo exhaustivo en todos los dispositivos de la empresa para que en caso de una brecha, aislar la afectación.

27. No tener los parches de seguridad: Sin importar si se cuenta con la última versión del sistema operativo, es importante tener todos los parches de seguridad mensuales del mismo, hay que verificar que la versión del sistema operativo aún tenga soporte.

Almacenamiento de datos

28. No tener cifrado el disco duro: Cifrar el disco duro de la computadora con las mismas herramientas que provee windows, esto es importante ya que en caso de ransomware, el atacante no podrá cifrar el disco duro, ya que se encontraría cifrado previamente.

29. No hay respaldos periódicos: Configurar los dispositivos para que realicen respaldos de los datos importantes al finalizar las actividades diarias.

30. No tener los datos cifrados en la nube: Contratar servicios de compañías como Oracle que puedan cifrar los datos antes de subirlos a la nube, esto permite una mayor seguridad ante un posible ataque del proveedor de los servicios de la nube.

Seguridad tecnológica

31. Tener las llaves de encriptación a la vista: No guardar las llaves en el mismo lugar que los archivos, además de no digitalizarlas, sino que tenerlas en físico, incluso considerar comprar una cartera cifrada por blockchain para almacenar las llaves.

Conectividad de red

32. No tener inhabilitados puertos de USB: En línea con la política zero trust, deshabilitar todos los puertos no utilizados de la computadora, hasta ser autorizados y desbloqueados por el administrador.

33. Compartir archivos por el router sin usar internet: Desactivar esta opción y solamente permitir transferencia de archivos a través de conexiones seguras (utilizando la nube).

5.2. Aspectos normativos para las soluciones

Con base en las vulnerabilidades encontradas en la PyME y dadas nuestras soluciones, encontramos algunas certificaciones internacionales que pueden ser de utilidad para mitigar los riesgos, dentro de estas, la serie ISO 27000 la cual se creó para cumplir los requisitos de la norma ISO 27001, esta serie engloba las certificaciones 27000-27019, 27030-27044, y finalmente la 27799. En esta ocasión nos enfocaremos en la ISO 27001, esta certificación se creó para minimizar los riesgos y reducir el impacto de alguna brecha a la seguridad informática de las empresas, la implementación de esta certificación da 3 principales beneficios a la empresa:

- Comercial: Que la empresa cuente con un sistema de gestión de la información (SGSI, que es una guía de políticas de administración de la información) brinda seguridad a los clientes ya que se tendrán controles de seguridad y requisitos actualizados; asimismo cuando se intentan buscar alianzas con otras empresas, se podrá exigir contar con el mismo estándar de calidad con el que cuenta la PyME para mantener y aumentar los ingresos comerciales.

- Tranquilidad: Al manejar la PyME datos sensibles y contar con esta certificación se puede tener una mayor certeza que el manejo de la información estará debidamente controlando, sabiendo que se tiene políticas en marcha para prevenir interrupciones en sus servicios y tener el menor impacto ante una amenaza. Actualmente la información es el activo más importante de una empresa por lo que tener el ISO 27001 mejora la imagen de la empresa y mayor confianza.

- Operacional: Consideramos que este punto es el más importante para la PyME ya que aquí se considera tener una cultura de ciberseguridad para todos los procesos, esto quiere decir que todo aquel que trabaje para la PyME, deberá estar al tanto de las políticas existentes, esto ocasionará que al haber al haber un ataque, la PyME y sus empleados sabrán como reaccionar y las afectaciones se minimizan y se controlarán de formas eficiente.

El ISO 27001 tiene algunas características importantes, dentro de ellas se encuentran:

- Ciclo PHVA: Puede implementarse para el SGSI así como para cada elemento individual y proporcionar la mejora continua, este consiste en 4 pasos:

  - Planificar: Establecer objetivos, recursos, requisitos del cliente y accionistas, política organizativa e identificar riesgos y oportunidades.
  - Hacer: Implementar lo planificado
  - Verificar: Controlar y medir los procesos para establecer el rendimiento de la políticas, objetivos, requisitos y actividades planificadas e informas de los resultados
  - Actuar: Tomar acciones para mejorar el rendimiento, en la medida de lo necesario.

- Auditorías para riesgos: Permite un análisis sistemático y científico para evaluar el SGSI, son realizadas tanto de forma interna como externa para verificar su eficiencia. Estas auditorías garantizan una evaluación regular para controlar y mejorar procesos de forma continua, credibilidad del sistema para conseguir objetivos deseados, reducir riesgos e incertidumbre y aumentar las oportunidades de negocio, consistencia de los resultados diseñados para cumplir con las expectativas de las partes interesadas. [15]

- Auditorías para procesos: Permite detallar las actividades que tienen un proceso para lograr los objetivos planificados, comúnmente en las empresas, un proceso se convierte en la entrada de otro proceso, por lo que es importante mantenerlos todos en orden. Estas auditorías garantizan, resultados consistentes, predecibles y eficientes, ya que los procesos funcionan de forma coherente.

Finalmente, en el 2013 se adoptó en Anexo SL (ISO 83), el cual consiste de 10 cláusulas: alcance, referencias normativas, términos y definiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño, mejora; cada cláusula se puede ver detalladamente en la cita [[15]].

5.3. Topología de red modificada

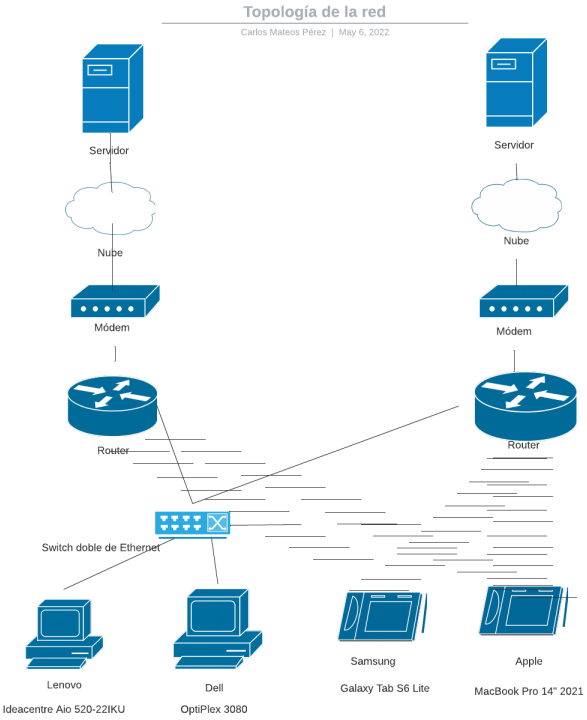

Figura 3: Topología modificada de la red inventariada para la PyME Pinturas SUQRO

En la Figura 3 se muestra la topología actualizada, en donde se pueden ver los cambios realizados, dentro de estos, se encuentra un router de respaldo con conexión a un segundo módem con conexión a un nuevo proveedor de internet, además, para simplificar las conexiones de las computadoras por ethernet se agregará el switch doble de ethernet (Es necesario buscar un switch con tecnología SDWan, la cual permite realizar fastswitches entre varios ISP), el cual contará con dos entradas LAN para ambos routers y salidas ethernet para las computadoras de escritorio.

5.4. Tabla-soluciones

Anomalía o vulnerabilidad	Localización	Solución	Costo
Utilización de WPA2 en el router	Router.	Comprar un router que cumpla	$1200 MXN una sola vez (Huawei AX3)
Contraseñas inseguras	Inicio de sesión a las aplicaciones web, computadoras y servicios de externos.	Contar con un protocolo de seguridad	$0
Depender de Bind para la facturación	Página web.	Contar con un aplicativo alterno para poder continuar con los servicios de facturación y que pueda usarse fuera de línea.	$500 USD / mes (NetSuite by Oracle)
Uso de dispositivos ajenos a la empresa en el mismo router	Infraestructura de la red.	Prohibir el uso de dispositivos ajenos, el administrador solamente dará acceso a dispositivos autorizados.	$0
Solo contar con un proveedor de internet	Infraestructura de la red.	Contar con otro proveedor, ya sea local o incluso satelital.	MXN al mes (Izzi Negocios 200, actualmente se cuenta con Telmex)
Solo contar con un router	Infraestructura de la red.	Contar con un router de repuesto	$1200 MXN una sola vez (Huawei AX3)
Usar el teléfono personal como de trabajo		Prohibir el uso de celulares personales y brindarle a los empleados celulares exclusivamente para la empresa, donde solamente podrán usar sus cuentas de trabajo.	$4500 MXN x celular, una sola vez (Samsung A13)
No tener cifrado el HDD	Hardware de los dispositivos.	Cifrar el disco duro de la computadora con las mismas herramientas que provee windows	$0 MXN
Firewall mal configurado	Software de la nube.	Contar con una alternativa para el almacenamiento de datos, es decir en físico (discos duros), o en la nube (google drive).	$210 MXN por usuario al mes (Google Drive for Enterprise)
Puertos de red no utilizados abiertos	Dispositivos electrónicos.	En línea con la política zero trust, deshabilitar todos los puertos no utilizados de la computadora, hasta ser autorizados y desbloqueados por el administrador.	$0 MXN
Intentos ilimitados de las contraseñas	Inicio de sesión.	Limitar los intentos posibles para el inicio de sesión (3 intentos) y después de los permitidos bloquear el acceso del usuario y forzar un reseteo de credenciales.	$0 MXN
Usuarios comparten contraseñas	Inicio de sesión.	Tener una cultura de seguridad y tener estrictamente prohibido compartir las contraseñas	$0 MXN

Anomalía o vulnerabilidad	Localización	Solución	Costo
No hay respaldos periódicos de datos	Nube/Hardware.	Configurar los dispositivos para que realicen respaldos de los datos importantes al finalizar las actividades diarias.	$0 MXN
No tener señalizados los cables conectados a las computadoras (material para señalizar)	Hardware.	Etiquetar todos los cables a la vista para una mejor orzación y en caso de alguna modificación a la conexión saber que cableis ? es el correcto.	$500 MXN, una sola vez
Puertos USB habilitados	Hardware.	En línea con la política zero trust, deshabilitar todos los puertos no utilizados de la computadora, hasta ser autorizados y desbloqueados por el administrador.	$0 MXN
No cifrar los datos que se suben a la nube	Nube/OneDrive.	Contratar servicios de compañías como Oracle que puedan cifrar los datos antes de subirlos a la nube	$10 USD por usuario y al mes (Boxcryptor)
Tener las llaves de encriptación a la vista	Archivos en hardware o nube.	No guardar las llaves en el mismo lugar que los archivos, además de no digitalizarlas, sino que tenerlas en físico	$0 MXN
No actualizar el antivirus	Software.	Revisar constantemente las actualizaciones del software	$0 MXN
No pagar el antivirus	Software.	Tener un recordatorio anual de pagar la licencia	$36 USD por dispositivo al año (McAffee endpoint security for enterprise)
No tener seguro de reparación para los dispositivos	Hardware.	Contratar un servicio externo de servicio técnico para los dispositivos como lo puede ser Asurion	$25 USD por usuario al mes (Asurion Home+: Incluye dispositivos de uso personal y de trabajo)
No tener sistema de monitoreo de los principales procesos	Software.	Buscar un software que permita monitorear la página web, el sistema de facturación, nubes, además de la infraestructura para que el estado de todo	$3.6 USD al mes (Sematext Monitoring)
No contar con auditorías (monitoreo de logins)	Inicio de sesión y software.	Tener activas las opciones del registro de datos, como registro de cuándo hay un login, cuando se abrió qué software, etc.	$0 MXN
Conectar dispositivos personales a la red	Infraestructura de la red.	Prohibir el uso de dispositivos personales, el administrador solamente dará acceso a dispositivos autorizados.	$0 MXN
Usuarios comparten contraseñas	Inicio de sesión.	Tener una cultura de seguridad y tener estrictamente prohibido compartir las contraseñas	$0 MXN

Cabe mencionar, que la suma total aproximada de los costos mensaules es igual a $13,959 MXN, por lo que entra perfectamente dentro del prespuesto de nuestra PyME. Sin embargo, este costo solo representa el costo del primer año, ya que en los años subsecuentes, se tendrá que hacer una

nueva auditoría para verificar el estado de los equipos y las actualizaciones que estos requieran, por lo que los costos podrían disminuir.

5.5. Riesgos en caso de no implementar el plan de mitigación

En caso de no implementar el plan de mitigación, la PyME queda vulnerable ante distintos tipos de ataque y por lo tanto expuesta a los riesgos que estos conlleva. Algunas de las consecuencias serían:

- Poner en riesgo la información propia de la PyME, sus colaboradores y clientes
- Perder la confianza de los clientes y posibles futuros socios
- Pérdida monetaria incluso mayor a la que se invertiría en ciberseguridad

5.6. Conclusiones

Al inicio de este proyecto, nos encontramos con una microempresa incursionando en los temas de pagos digitales, que avanzaba a paso seguro pero con una noción mínima sobre la ciberseguridad. Conforme este proyecto avanzó, más y más vulnerabilidades fueron encontradas, cosas que iban desde lo más sencillo como no tener un servidor propio, hasta temas mucho más preocupantes como el hecho de que el router permitiera el acceso de red a todas las computadoras. Poco a poco se fueron haciendo más descubrimientos y dando pequeñas y sencillas soluciones a cada uno de ellos. Con ayuda de nuestro socio formador, cada uno de estos problemas tiene una solución rápida, sencilla y asequible a las posibilidades de nuestra PyME. Por otro lado, la identificación de las vulnerabilidades por parte de nuestro equipo no fue una tarea sencilla, muchos aspectos que nos parecían normales en realidad representaban fallas de moderadas a graves dentro del campo de la ciberseguridad, aun así, con ayuda de los contenidos vistos en clase, así como el material y asesorías proporcionados por el socioformador nos fue posible diseñar un plan de acción y fortificación a los puntos débiles del software de nuestra PyME. Esto sin llegar a requerir una inversión exorbitante, como se creía en un principio: el gasto más significativo sería montar un servidor propio. Queda pendiente dar seguimiento a nuestra empresa asignada, ver si sigue nuestras recomendaciones y observar los resultados que estos cambios implementados arrojan.

Referencias

[1] CanalesTI. “PyME, en riesgo por ciber ataques”. En: *CanalesTI* 1 (1 2021).

[2] “CVE-2022-23255: Microsoft OneDrive for Android Security Feature Bypass Vulnerability.” En: *Intruder.io* 1 (1 2022).

[3] S. Daza. “Nexpose Escaneo de Vulnerabilidades - Behackerpro. BeHackerPro - Profesionales en Ciberseguridad - El elemento que le suma a tu conocimiento. Aprende Ciberseguridad”. En: *BeHackerPro* 1 (1 2021).

[4] CVE Details. “CVE-2013-7202 : The WebHybridClient class in PayPal 5.3 and earlier for Android allows remote attackers to execute arbitrary JavaScript.” En: *Intruder.io* 1 (1 2018).

[5] CVE Details. “CVE-2014-5658: The MercadoLibre (aka com.mercadolibre) application 3.8.7 for Android does not verify X.509 certificates from SSL server.” En: *Intruder.io* 1 (1 2014).

[6] CVE Details. “CVE-2021-31854: A command Injection Vulnerability in McAfee Agent (MA) for Windows prior to 5.7.5 allows local users to inject arbitrary.” En: *Intruder.io* 1 (1 2022).

[7] CVE Details. “CVE-2021-41569: SAS/Intrnet 9.4 build 1520 and earlier allows Local File Inclusion. The samples library (included by default) in the app.” En: *Intruder.io* 1 (1 2022).

[8] CVE Details. “CVE-2022-0635 : Versions affected: BIND 9.18.0 When a vulnerable version of named receives a series of specific queries, the named proce.” En: *Intruder.io* 1 (1 2022).

[9] CVE Details. “CVE-2022-26903 : Windows Graphics Component Remote Code Execution Vulnerability”. En: *Intruder.io* 1 (1 2022).

[10] CVE Details. “CVE-2022-27572 : Heap-based buffer overflow vulnerability in parser_ipma function of libsimba library prior to SMR Apr-2022”. En: *Intruder.io* 1 (1 2022).

[11] DSA. “Acunetix Web Vulnerability Scanner”. En: *DSA* 1 (1 2022).

[12] GeeksforGeeks. “Kali Linux - Aircrack-ng”. En: *GeekforGeeks* 1 (1 2020).

[13] INEGI. “Micro, Pequeña, Mediana y Gran empresa.” En: *INEGI* 1 (1 2009).

[14] Intruder.io. “Intruder — An Effortless Vulnerability Scanner”. En: *Intruder.io* 1 (1 2022).

[15] NQA. “ISO 27001:2013 GUÍA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN”. En: *NQA* 1 (1 2013).

[16] Granados Ó. "¿Cuánto hay que invertir en ciberseguridad para proteger un negocio? " En: *El Empresario* 1 (1 2021).

[17] QMA. "Netsparker Web Application Security Scanner . QMA MSS." En: *QMA* 1 (1 2020).

[18] T. Rains. "Microsoft Free Security Tools – Microsoft Baseline Security Analyzer". En: *Microsoft Security Blog* 1 (1 2020).

[19] Castro Rubén. " WPA3: Qué características y ventajas tiene". En: *Castro Rubén* 1 (1 2021).

[20] G. Terol G Chavarri. "¿Qué es y cómo funciona el protocolo WPA3?" En: *WPA3* 1 (1 2022).

[21] Tripwire. "About Us — Tripwire. Tripwire Enterprise." En: *Tripwire* 1 (1 2020).