Instituto Tecnológico y de Estudios Superiores de Monterrey
Escuela de Ingeniería y Ciencias
Ingeniería en Ciencia de Datos y Matemáticas

Análisis de criptografía y seguridad

Auditoría de Seguridad y Plan de Mitigación: SUQRO

Leonardo Laureles Olmedo A01659241
Manuel Andrés Rodríguez Rivera A01659819
Mariana Rincón Flores A01654973
Carlos Mateos Pérez A01654085
Daniel Núñez López A01654137
Mariano Luna Tress A01734509

Socio Formador: IPC Services

Profesores: Alberto F. Martínez y Alejandro Parra Briones

6 de mayo de 2022, Monterrey, Nuevo León

Agenda

- Descripción de la PyME
- Inventario
- Plan de evaluación
- Plan de mitigación
- Conclusiones
- Referencias

Pinturas SUQRO

Micro-empresa de pinturas OSEL en Querétaro, Qro.

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

- 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.

- Presupuesto para TI (mensaul): $15,000 MXN

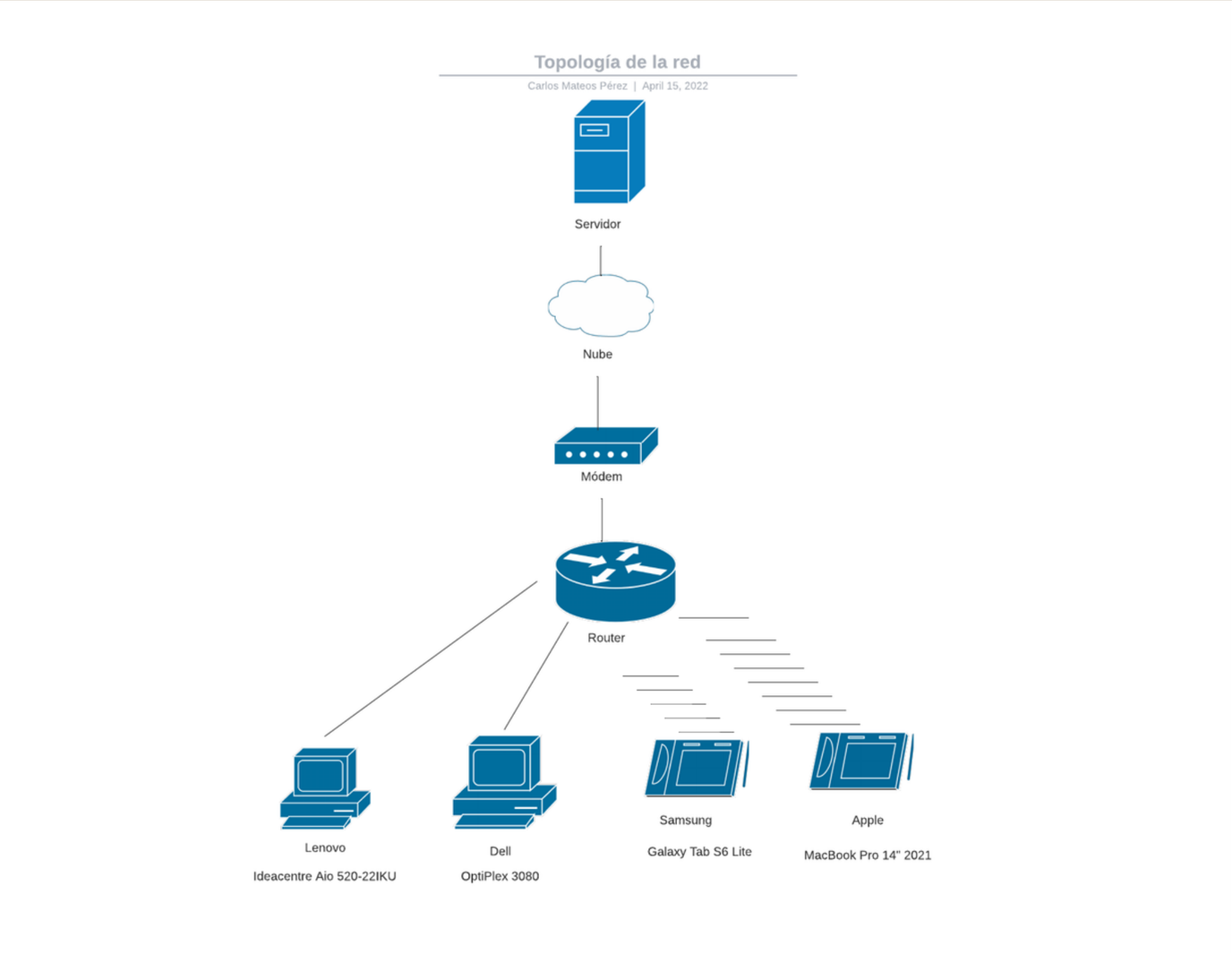
Inventario

- Marca: LENOVO
- Modelo: Ideacentre Aio 520-22IKU
- Colaboradores: Dirección, Ventas y Administración

- Marca: DELL
- Modelo: Optiplex 380
- Colaboradores: Dirección, Ventas y Administración

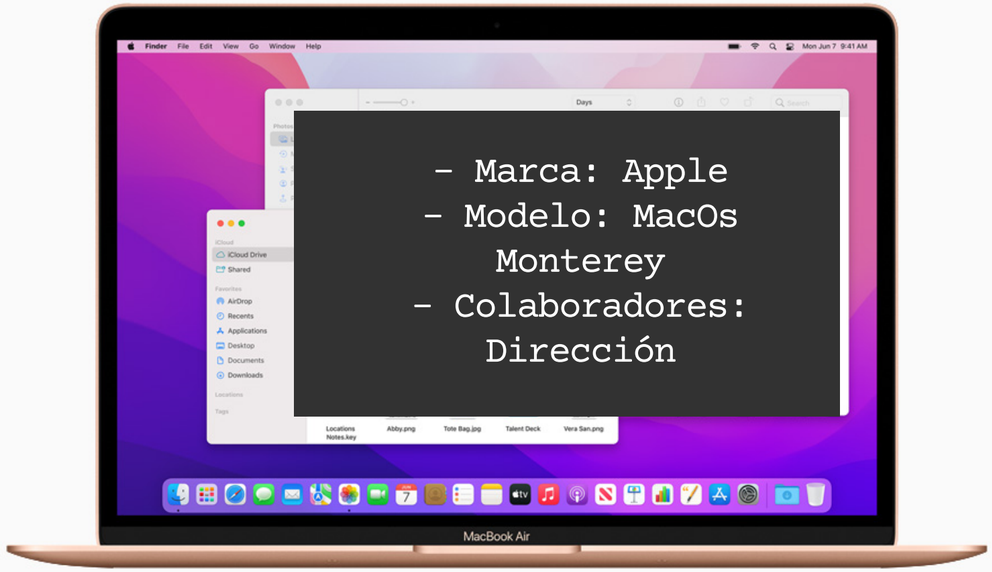
- Marca: Microsoft
- Modelo: 365 Business Basic
- Colaboradores: Dirección,Asistente, Ventas y Administración

Topología de la red

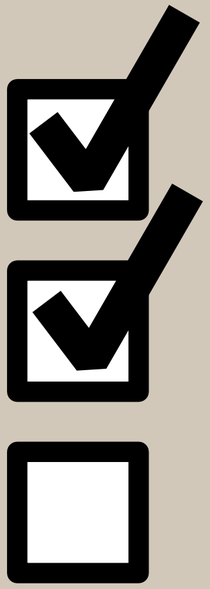


- Marca: Google
- Modelo: G Suite
- Colaboradores: Dirección, Ventas y Administración

- Marca: Bind
- Modelo: ERP + CrecimientO
- Colaboradores: Dirección, Asistente, Ventas y Administración



Plan de evaluación



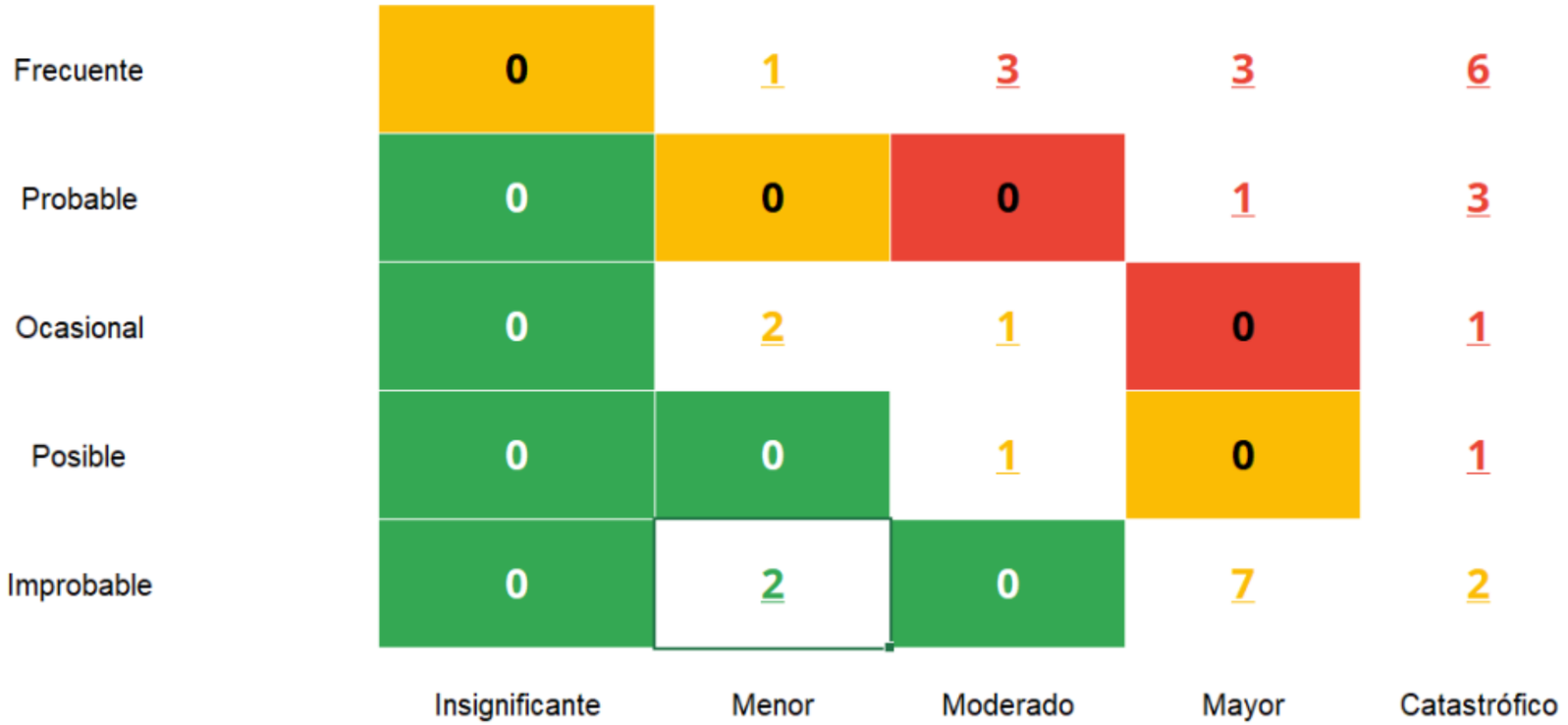
Anomalía o vulnerabilidad	Localización
Utilización de WPA2 en el router	Router
Contraseñas inseguras	Inicio de sesión a las aplicaciones web, computadoras y servicios externos
Depender de Bind para la facturación	Página web
Uso de dispositivos ajenos a la empresa en el mismo router	Infraestructura de la red
Solo contar con un proveedor de Internet	Infraestructura de la red
Solo contar con un router	Infraestructura de la red

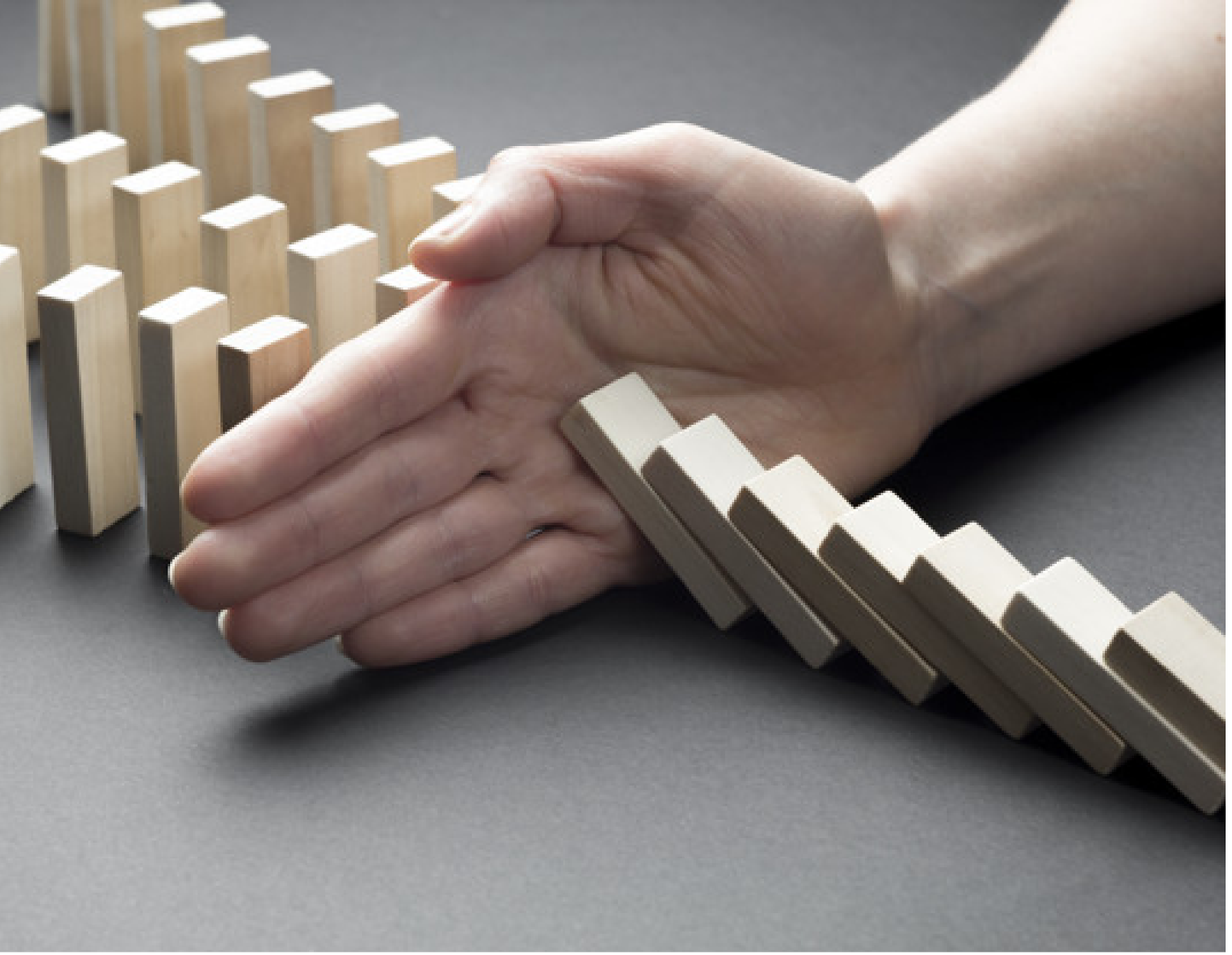
Anomalía o vulnerabilidad	Localización
Usar el teléfono personal como de trabajo	Infraestructura de la red
No tener cifrado el HDD	Hardware de los dispositivos
Firewall mal configurado	Software de la nube
Puertos de red no utilizados abiertos	Dispositivos electrónicos
Intentos ilimitados de las contraseñas	Inicio de sesión
Usuarios comparten contraseñas	Inicio de sesión

Anomalía o vulnerabilidad	Localización
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

Anomalía o vulnerabilidad	Localización
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 auditorias (monitoreo de logins)	Inicio de sesión y software
Conectar dispositivos personales a la red	Infraestructura de la red

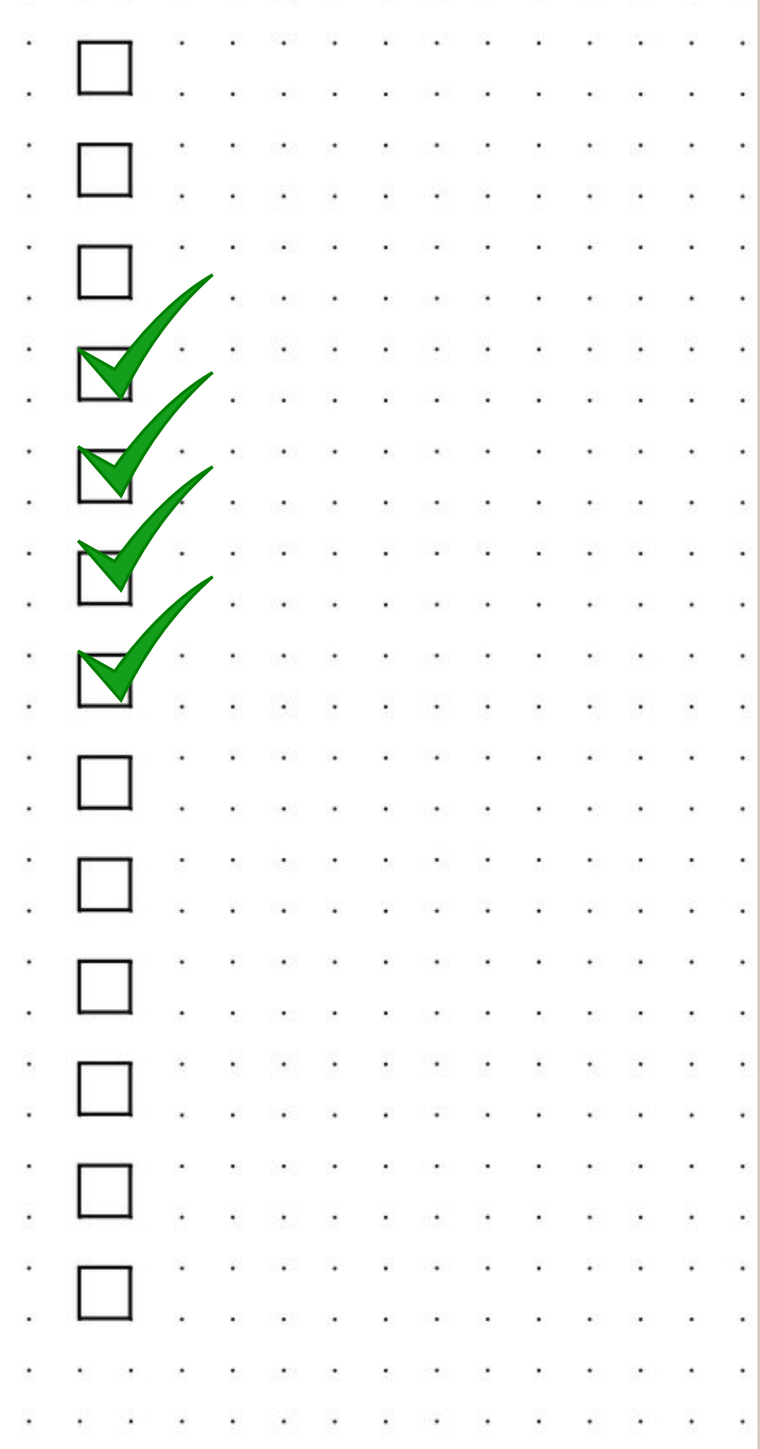
Matriz de riesgos





Plan de Mitigación

- Puntos del plan de mitigación
- Enfoques
- Costos

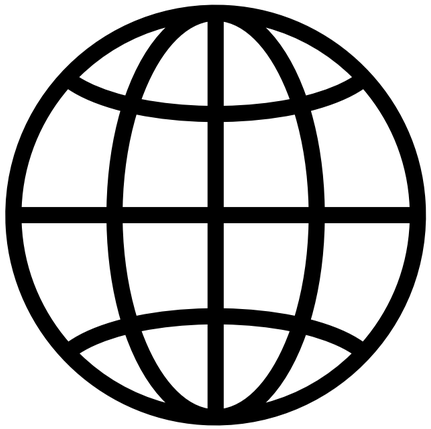


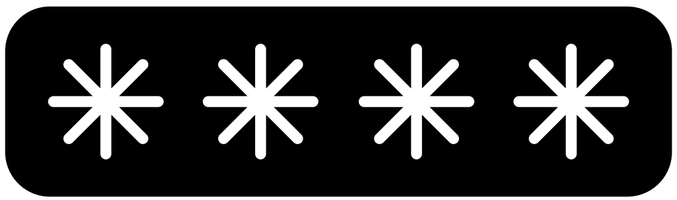
Puntos del Plan de Mitigación

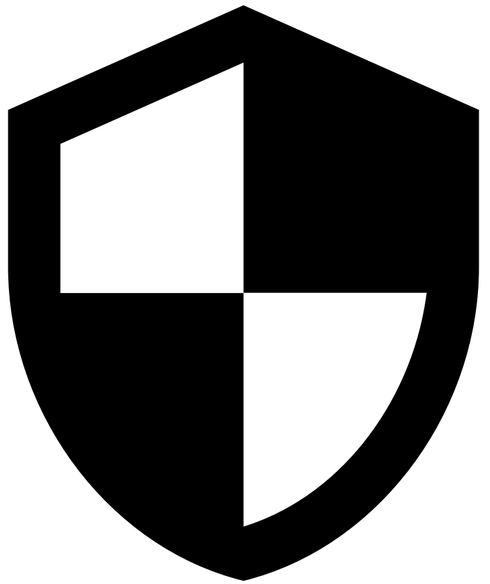
1. Inicio de sesión
2. Conectividad
3. Conexión de red
4. Proceso de compra
5. Seguridad física
6. Mantenimiento de la infraestructura
7. Almacenamiento de datos
8. Seguridad tecnológica
9. Conectividad de red

- Costos
- Cuestiones operativas y de regulaciones
- Riesgos de no implementar el plan

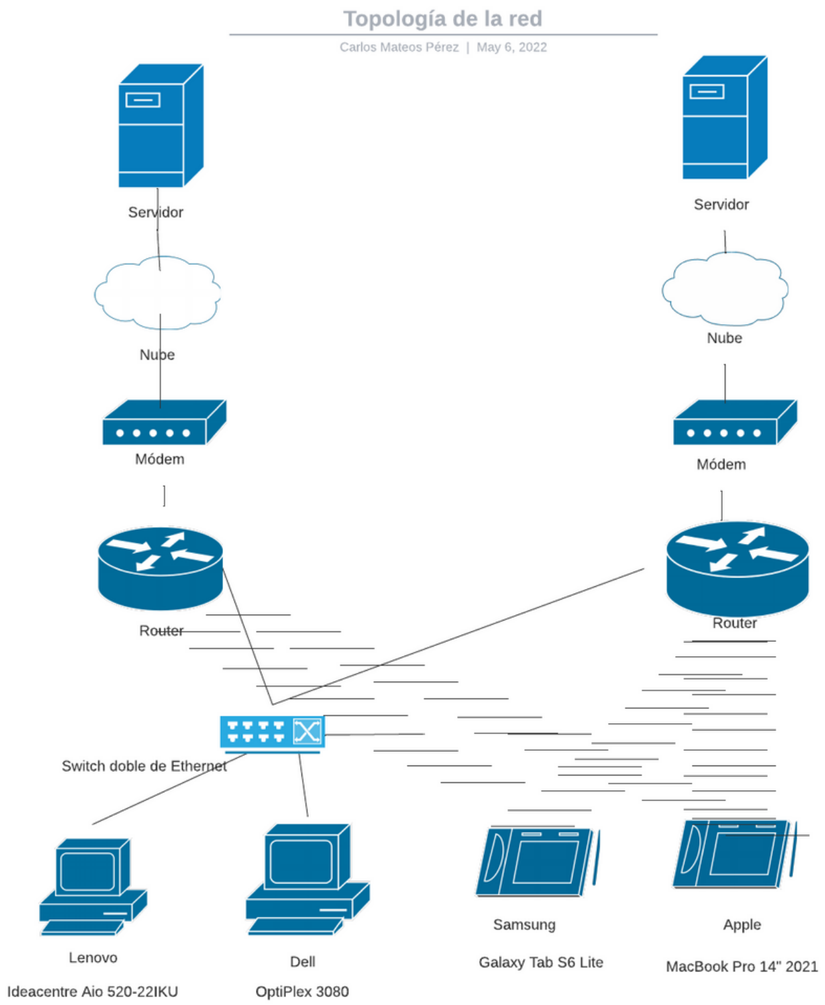
Enfoque (soluciones)





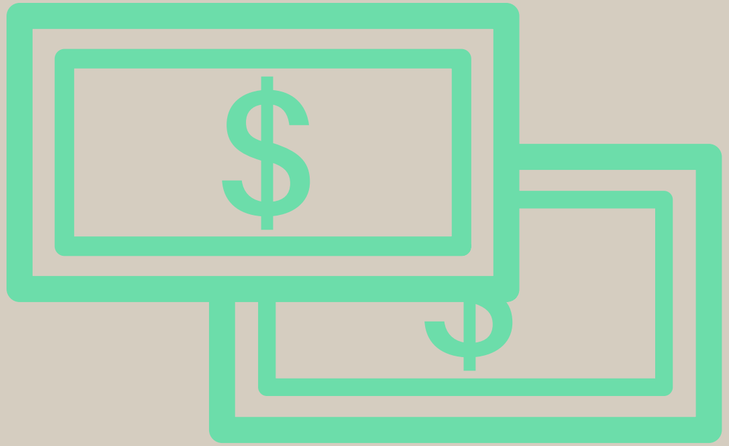


Topología de la red actualizada



Costos

Al analizar las soluciones a las vulnerabilidades presentadas, la inversión total mensual está estimada en $ 13,959 MXN lo que se encuentra dentro del presupuesto de la PyME.



Normativas

- Certificaciones Internacionales serie ISO 27000 que cumple con los requisitos de la norma ISO 27001, esta serie engloba las certificaciones 27000-27019, 27030-27044, 27799 y el Anexo SL (ISO 83).
- Brinda 3 principales beneficios:
    - Comercial
    - Tranquilidad
    - Operacional
- Caraterísticas de ISO 27001:
    - Ciclo PHVA
    - Auditoría para riesgos
    - Auditoría para procesos

Riesgos en caso de no implementar el plan de mitigación

- Vulnerable ante distintos ataques
- Pérdida monetaria
- Se pone en riesgo la información propia de la empresa, colaboradores y clientes
- Confianza en clientes

Conclusiones

Nos encontramos con una empresa con varios huecos de seguridad

Con ayuda del socio formador...

- Identificamos fallas, vulnerabilidades y áreas de mejora en su sistema.
- Diseñamos un plan que satisficiera las necesidades del negocio, tanto funcionales como de ciberseguridad.
- Fuimos instruidos acerca de temas de ciberseguridad y le transmitimos estos conocimientos a los trabajadores y deuños de nuestra PyME.
- Logramos todo esto sin requerir una inversión monetaria significativa por parte de los propietarios

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, Peque˜na, 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 GU´IA DE IMPLANTACION PARA LA SEGURIDAD DE LA IN- ´ FORMACION”. En: ´ NQA 1 (1 2013).
[[16] Granados O. “¿Cu´anto 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: Micro soft Security Blog 1 (1 2020).
[19] Castro Rub´en. “ WPA3: Qu´e caracter´ısticas y ventajas tiene”. En: Castro Rub´en 1 (1 2021).
[20] G. Terol G Chavarri. “¿Qu´e es y c´omo funciona el protocolo WPA3?” En: WPA3 1 (1 2022). [21] Tripwire. “About Us — Tripwire. Tripwire Enterprise.” En: Tripwire 1 (1 2020).