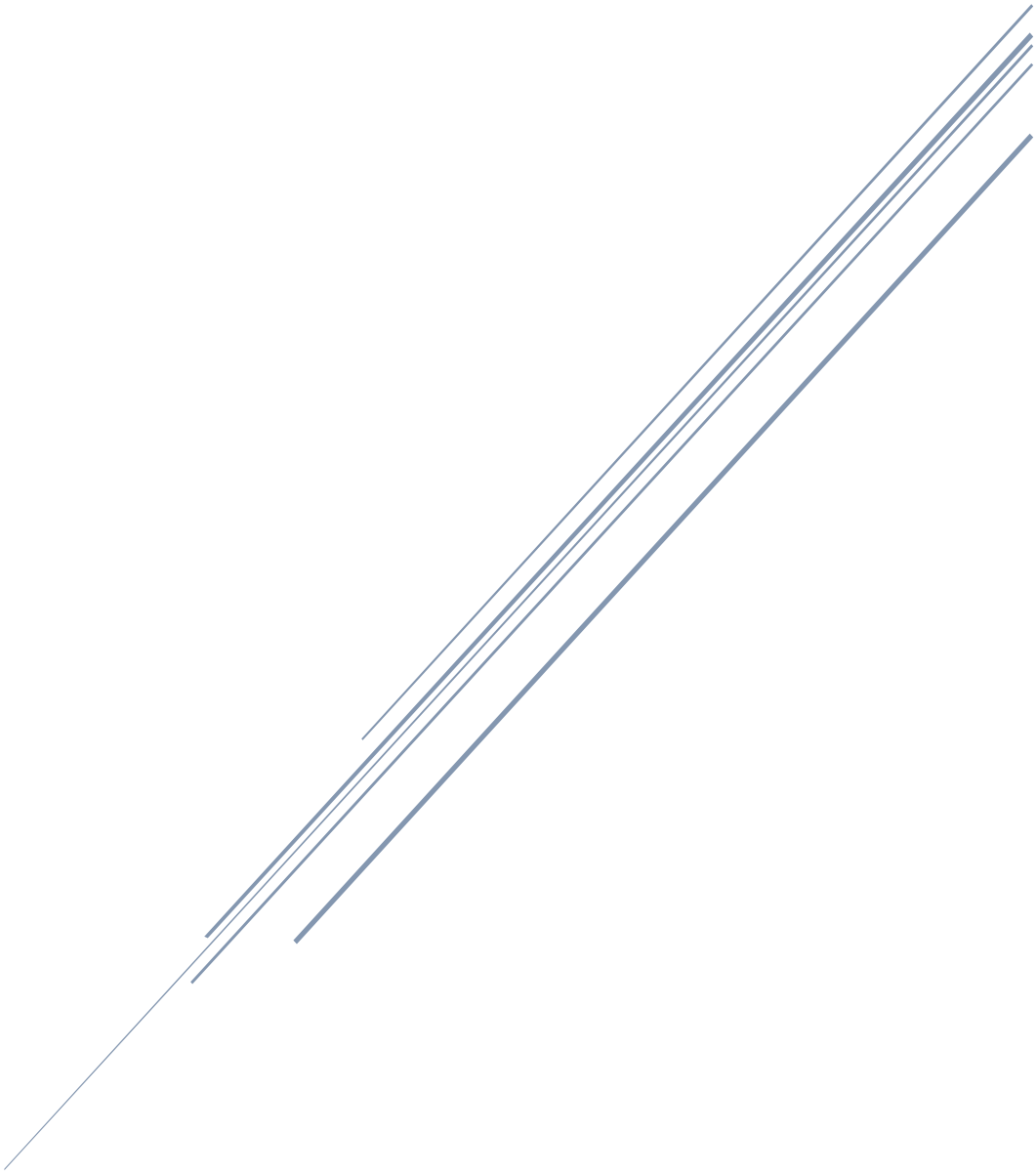
AUDITORIA INFORMATICA

EMPRESA AUDITADA: CENTRO MEDICO QUIRURGICO JUAN PABLO II E.I.R.L

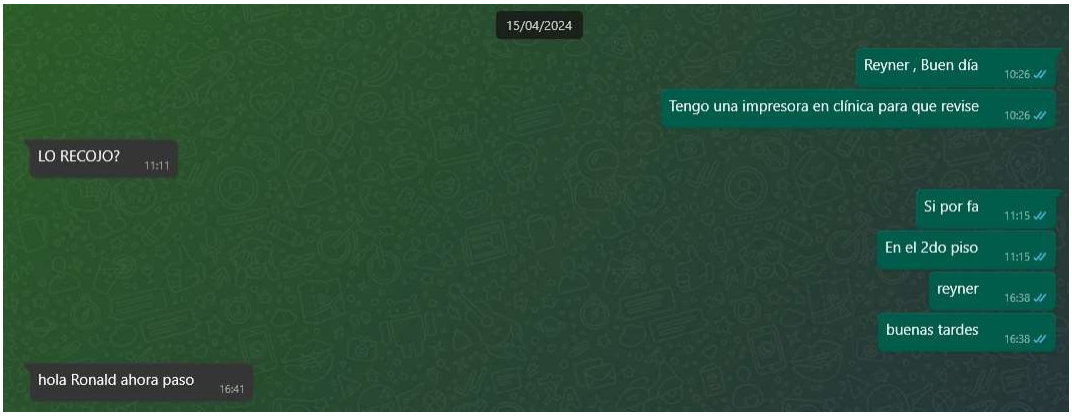


Asesor: Kael Jesús Torre Pérez
Estudiante de Ingeniería de Sistemas

1) Área diagnosticada: Outsourcing	
Descripción: La clínica recurre a los servicios de empresas desarrolladoras de software y empresas de servicios de mantenimiento de equipos de cómputo y otros.	
Pros: ▪ De estos servicios se obtiene softwares desarrollados a medida y con servicio de soporte técnico activo constantemente. ▪ Se permite la delegación de procesos de mantenimiento cuando la situación es crítica o cuando no se puede atender en el momento.	Contras: ▪ Algunos de estos servicios adquiridos no son de carácter formal, carecen de contrato fijo. ▪ No se cuenta con tasas fijas de pago por los servicios. ▪ No se cuenta con tiempos establecidos para la realización de los servicios. ▪ No se cuenta con estándares de calidad para los servicios adquiridos.
Sugerencias: ▪ Lograr formalizar todos sus servicios adquiridos de terceros por medio de contrato fijo. Estableciendo tasas fijas de pago por los servicios, tiempos de atención y estándares de calidad.	

Evidencias:

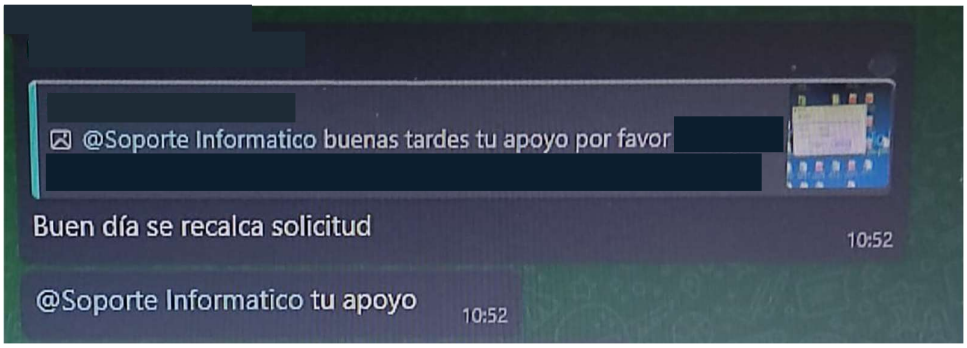
1) Solicitud de servicio a empresa “System Ram”, para mantenimiento de equipos de impresión en clínica. Al llamado.

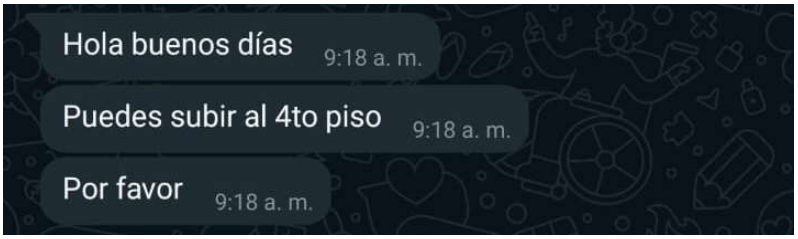


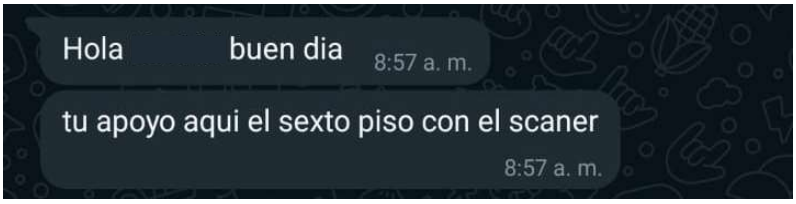
<table>
<tr><td colspan="2">2) Área diagnosticada: Técnica de sistemas (Soporte técnico)</td></tr>
<tr><td colspan="2">Descripción: El área de TI de la clínica esta encargada de realizar el soporte técnico necesario en el día a día.</td></tr>
<tr><td>Pros:
Personal capacitado en el área de trabajo.
Herramientas especiales para brindar soporte técnico en el área.
Se puede evitar los gastos extras por contratar servicios de terceros.</td><td>Contras:
Todo soporte es informado por medio de mensaje vía WhatsApp o por medio de llamada telefónica.
En ocasiones se puede confundir o pasar por alto algún servicio técnico pendiente.</td></tr>
<tr><td colspan="2">Sugerencias:
Gestionar adquisición o desarrollo de un sistema de tickets para soporte técnico. Sugerencia de sistema, FreshService de FreshWorks.
Establecer una cultura de responsabilidad compartida en la que el personal, mediante capacitación y acceso a equipos de limpieza básicos, se encargue de mantener sus áreas de trabajo limpias.</td></tr>
</table>

Evidencias:

1) Solicitudes de soporte por medio del servicio de mensajería WhatsApp







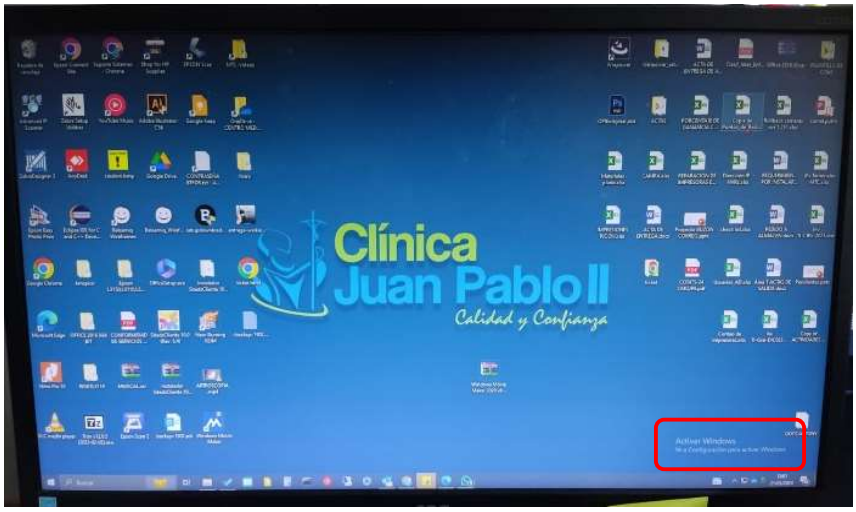
2) Inventario de equipos disponibles en el área de TI

N°	Equipo	Cantidad	Marca	Modelo	Estado	Uso
1	Computadora Desktop	1	Compatible	Genérico	Bueno	Computadora Principal en TI
2	Monitor	3	HP	Compaq la2006x	Bueno	Monitor estandar usado en TI
3	Teclado	1	Genius	KB-116	Bueno	Teclado usado en computadora principal
4	Teclado	2	Logitech	K120	Bueno	Teclados usados en otros equipos de TI
5	Mouse	3	Logitech	M90	Bueno	Mouse estandar usado en TI
6	Tablet	1	Samsung	TAB A7	Bueno	Usado en procesos de inventariado
7	Impresora de Stickers	1	Zebra	ZD220t	Bueno	Impresora usada para la generación de etiquetas
8	Impresora de PVC	1	Zebra	ZC100	Bueno	Impresora usada para la generación de ID
9	Impresora Laser	1	HP	Laserjet Pro M12w	Bueno	Impresora de contingencia
10	Impresora monocromática	1	Epson	M1120	Bueno	Impresora de contingencia
11	Impresora multifuncional	3	Epson	L3110	Malagrado	Repuestos para impresoras compatibles
12	Impresora multifuncional	2	Epson	L355	Malagrado	Repuestos para impresoras compatibles
13	Proyector Multimedia	1	ViewSonic	PA503X	Bueno	Proyector usado para reuniones y capacitaciones
14	Installer Kit (1 Crimping Tool, 1 Pelador de cable, 1 Lan Teste, 1 Terminador para Jacks de 90°)	1	SATRA	FT_Intaller_Kit	Bueno	Usado en las instalaciones de red
15	Disco duro externo de 1 TB	1	ADATA	HD710	Bueno	Usado para almacenar backups y otros
16	Acces Point	1	Tp-Link	TL-WA901ND	Bueno	Acces Point dentro de área de TI
17	DVD Writer	7	LG	GP65NB60	Bueno	Usados para lectura y escritura de discos
18	Taladro	1	EINHELL	TC-CD 18/35 LI	Bueno	Usado en instalaciones de red

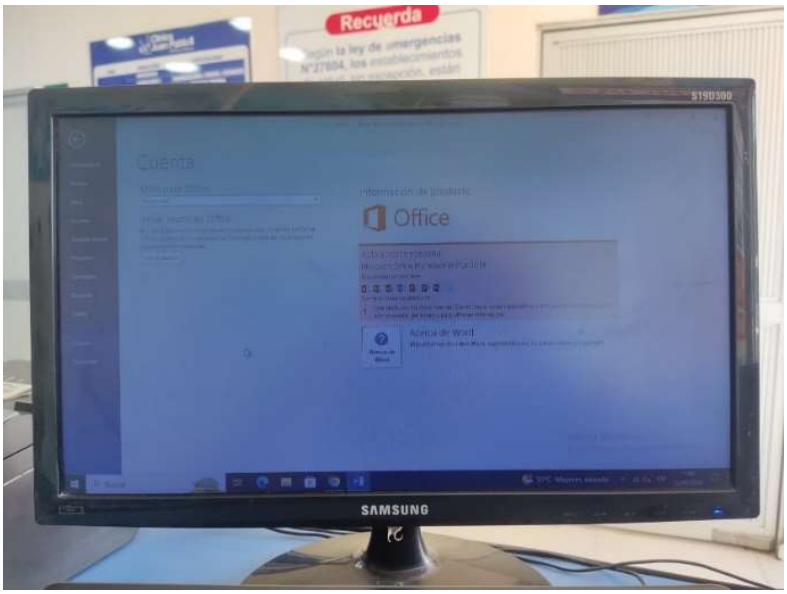
<table>
<tr><td colspan="2">3) Área diagnosticada: Aplicaciones</td></tr>
<tr><td colspan="2">Descripción: La clínica hace uso de servicios de Windows, Office, lectores de archivos y de software médico.</td></tr>
<tr><td>Pros:
Se cuenta con aplicaciones que facilitan y agilizan los procesos administrativos en la clínica.
Los softwares usados en clínica son fáciles de conseguir e implementar.</td><td>Contras:
Algunos sistemas operativos no cuentan licencia activa.
Algunos softwares no son licenciados.
Malfuncionamientos presentes debido a los softwares no licenciados.</td></tr>
<tr><td colspan="2">Sugerencias:
Activar licencias de sistema operativo a las máquinas que lo requieren.
Adquirir licencias para los softwares usados.
Evitar el uso de softwares pirateados o sin licencia.
Adquirir sistema para atención de tickets de soporte técnico.
Adquirir sistema para automatización de control de almacén.</td></tr>
</table>

Evidencias:

1) Equipos con sistemas operativos sin licencia activa.



2) Equipos con servicios de Office sin licencia activa.



3) Inventario de sistemas operativos en clínica

N°	Descripcion	Desarrollador	Maquinas	Licencias Activas
1	Windows 11 Pro	Microsoft	6	6
2	Windows 11 Home	Microsoft	2	2
3	Windows 10 Pro	Microsoft	48	36
4	Windows 10 Home	Microsoft	8	6
5	Windows 7 Pro	Microsoft	9	9
6	Windows 7 Home Premium	Microsoft	1	1
7	Windows 7 Ultimate	Microsoft	1	1
8	Windows Server 2019 Standard 64 bits	Microsoft	1	1

4) Inventario de aplicaciones usados en clínica.

N°	Descripción	Desarrollador	Licencia en máquina
1	Office 365	Microsoft	Todas
2	Office 2016	Microsoft	Algunas
3	BitDefender end point security	BitDefender	Todas
4	Google Drive	Google	No es necesario
5	Creative Cloud	Adobe	Todas
6	Siteds	SUSALUD	Todas
7	Windows Movie Maker	Microsoft	Todas (Licencia Free)
8	Google Chrome	Google	No es necesario
9	Micrososft Edge	Microsoft	No es necesario

5) Inventario de utilitarios usados en clínica.

N°	Descripción	Desarrollador	Licencia en máquina
1	Win Rar	Eugene Roshal	Todas (Licencia Free)
2	Nitro 16	Microsoft	Algunas
3	Formato DICOM (RadiAnt)	Medixant	Ninguna
4	Nero 7	Nero AG	Ninguna
5	Anydesk	AnyDesk Software GmbH	Todas (Licencia Free)
6	Zebra Utilities	Zebra	No es necesario
7	VLC media player	Video LAN	No es necesario
8	Epson Printer Utilities	Epson	No es necesario
7	Advance IP scanner	Famatech Corp	No es necesario

4) Área diagnosticada: Base de datos

Descripción: La clínica hace uso del gestor de base de datos SQL que está vinculado a su sistema médico “Mediweb”. Así mismo hace uso de archivos Excel para el almacenamiento de datos de otras operaciones.

Pros:	Contras:
▪ Gestor de base de datos con licencia ▪ Existencia de credenciales de acceso a la base de datos. ▪ Las credenciales son privadas y seguras. ▪ Permite el almacenamiento de datos críticos en clínica.	▪ Ausencia de logs de auditorías de base de datos. ▪ Archivos Excel almacenados en una sola maquina y con acceso libre a estas. ▪ Los procesos de respaldo de la data dentro de la base de datos no son frecuentes. ▪ Personal de TI no está completamente capacitado para la gestión de la base de datos.

Sugerencias:

- Generar un procedimiento de respaldo de datos periódico. Para así resguardar información crítica para la clínica.
- Realizar copia de los archivos Excel que contengan data crítica.
- Cifrar archivos Excel para resguardar los datos de copias o accesos no autorizados.
- Capacitar al personal de TI para correcta gestión de la base de datos.

5) Área diagnosticada: Redes e internet

Descripción: Se cuenta en clínica con red dedicada de internet. La red de clínica esta segmentada para mejor control de esta.

Pros:	Contras:
▪ Manejo ordenado de los equipos conectados a red gracias a las segmentaciones. ▪ Se evita la sobre carga en el flujo de datos entre equipos médicos, equipos de vigilancia y equipos de oficina. ▪ Puntos de red ubicados dentro de áreas de trabajo. ▪ Access Points ocultas y con contraseña privada. ▪ Cables de red respetan norma crimpado cable de red, T-568B ▪ DNS de red privada activa en todos los equipos conectados a red. ▪ Existencia de canaletas de piso y de pared, para la protección de los cables de red. ▪ Existencia de gabinetes donde se ubican los servidores y switches.	▪ Algunas conexiones están expuestas a pisadas del personal y no están correctamente ordenadas o etiquetadas. ▪ Algunos switches están mal ubicados o expuestos a ser golpeados. ▪ El diagrama de red no está actualizado. ▪ Se permite el conectar a red de clínica los equipos personales de los trabajadores. ▪ Existencia de canaletas, pero no hacen uso de algunas de estas. ▪ Gabinetes necesitan limpieza.

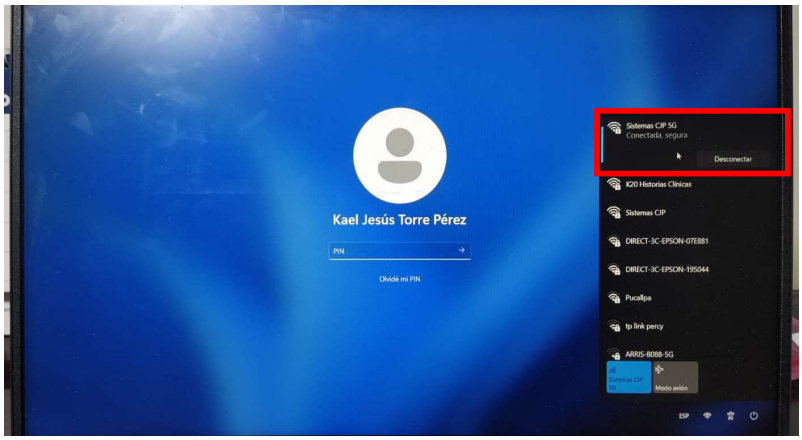
Sugerencias:

- Realizar mantenimiento preventivo periódico de las conexiones de red para evitar daños a los equipos y cables de red.
- Realizar revisión de canaletas de red periódicas.
- Realizar limpieza a los gabinetes de red periódicamente.
- Actualizar el diagrama de red de clínica.
- Brindar equipos de trabajo propios de la empresa a los trabajadores.

Evidencias:

1) Cables de red expuestos a pisadas del personal

2) Se permite equipos personales dentro de la red privada de clínica



6) Área diagnosticada: Videovigilancia

Descripción: En clínica se cuenta con una red CCTV compuesta por diversas cámaras de vigilancia y equipos NVR. Todos activos y cumpliendo su funcionamiento sin complicaciones.

Pros:	Contras:
▪ Dentro del segmentado de red dedicado a cámaras de vigilancia. ▪ La administración de las cámaras de vigilancia es únicamente realizada por el área de TI. ▪ Cámaras ubicadas en partes esenciales y con claro campo de visibilidad. ▪ Cámaras con visión infrarroja para las grabaciones nocturnas. ▪ Tiempo de almacenamiento de grabaciones de vigilancia de al menos un mes. ▪ Las cámaras son constantemente monitoreadas por medio de monitores en las áreas de administración.	▪ Algunas cámaras de vigilancia presentan suciedad acumulada. ▪ En algunas cámaras de vigilancia, la grabación nocturna, presenta imagen distorsionada o bloqueada.

Sugerencias:

- Realizar un mantenimiento detectivo a la red CCTV. Debido a indicios de factores que afectan la vida útil de los equipos de vigilancia.
- Gestionar un proceso de mantenimiento preventivo periódico a la red CCTV.

Evidencias:

1) Cámara con suciedad acumulada

2) Cámara con imagen nocturna bloqueada

3) Cámaras monitoreadas desde monitor en administración

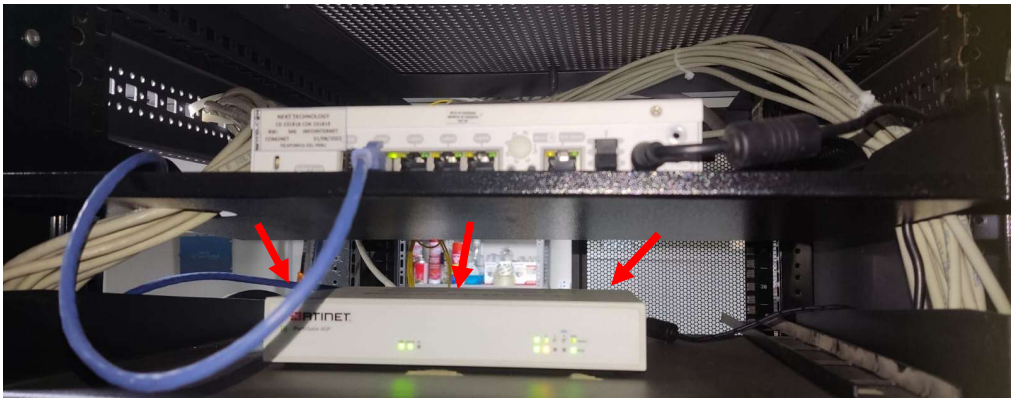
7) Área diagnosticada: Seguridad Física y Lógica
Descripción: En la clínica Juan Pablo II, por su propia naturaleza del negocio, sus ambientes son limpios y con las respectivas medidas de seguridad.

Pros – Seguridad Física:	Contras – Seguridad Física:
▪ La sala de servidores se encuentra en un ambiente de humedad controlada. ▪ Se cuenta con un firewall conectada a la red de clínica. ▪ Extintores y detectores de humo en cada piso y de fácil disposición. ▪ Luces de emergencia en puntos estratégicos. ▪ El acceso a las diferentes áreas críticas en la clínica está regulado por cerraduras con llave. ▪ Las computadoras y equipos en clínica están resguardadas ante cortes o bajones de corriente eléctrica por UPS y generadores de electricidad. ▪ Switches y servidores dentro de gabinetes. ▪ Cables de red y de electricidad protegidos por canaletas. ▪ Cables de periféricos de las computadoras protegidos y separados. ▪ Se realiza entrega de discos duros externos dedicados, a las áreas que almacenen exámenes y resultados de pacientes.	▪ Se presenta humedad en algunas partes de los techos por motivo de los conductos de sistema de drenado de los aires acondicionados. ▪ La humedad presenta un potencial riesgo a los cables de red y electricidad que se encuentran en los techos. ▪ No se cuenta con un plan de acción ante incidentes físicos o desastres en el área de TI.
Sugerencias: ▪ Brindar mantenimiento periódico a los conductos de sistemas de drenado de los aires acondicionados. ▪ Realizar revisión y removimiento de humedad en los techos de la clínica. ▪ Desarrollar un plan de acción ante incidentes físicos o desastres en el área de TI	

<table>
<tr>
<td>Pros – Seguridad Lógica:
Las computadoras conectadas a red cuentan con antivirus dedicado.
Active Directory de Windows Server activo en clínica, permitiendo un dominio de usuarios para las computadoras.
Existe filtrado de páginas web que sean categorizadas como peligrosas.
Acceso a las diferentes computadoras regulado por usuario y contraseña de personal autorizado.
Las contraseñas son seguras y actualizadas periódicamente.
Solo usuarios administradores tienen permiso de realizar cambios en la configuración de las computadoras.
Acceso al software médico por medio de credenciales otorgados solo a personal autorizado.
La creación de nuevos usuarios o restablecimiento de contraseñas están administrados únicamente por el área de TI.
Se realiza backup de correos electrónicos de clínica y de archivos de las computadoras periódicamente.</td>
<td>Contras – Seguridad Lógica:
No todas las computadoras tienen activo el servicio de antivirus, faltante la instalación del servicio de endpoint.
No se cuenta con un procedimiento establecido para la evaluación y mitigación de vulnerabilidades en el software y hardware.</td>
</tr>
<tr>
<td colspan="2">Sugerencias:
Realizar instalación de servicio endpoint en las computadoras que no tengas BitDefender activado.
Desarrollar un procedimiento para la evaluación y mitigación de vulnerabilidades en el software y hardware.</td>
</tr>
</table>

Evidencias:

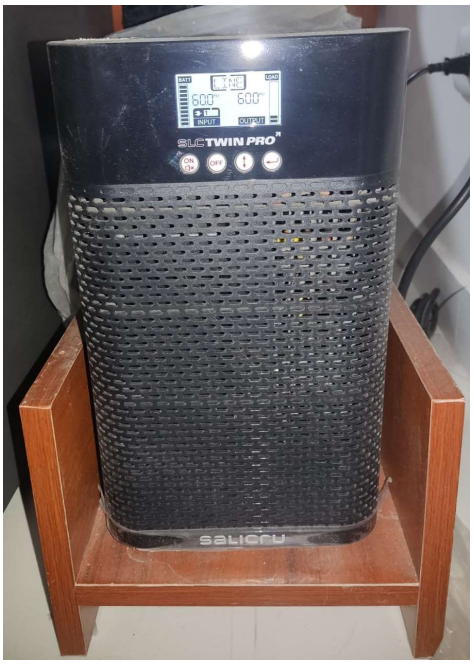
1) Firewall conectado a red de clínica.



2) Extintores, sensores de humo y luces de emergencia

3) Acceso a área criticas reguladas por puertas con llave.

4) UPS conectados a los equipos

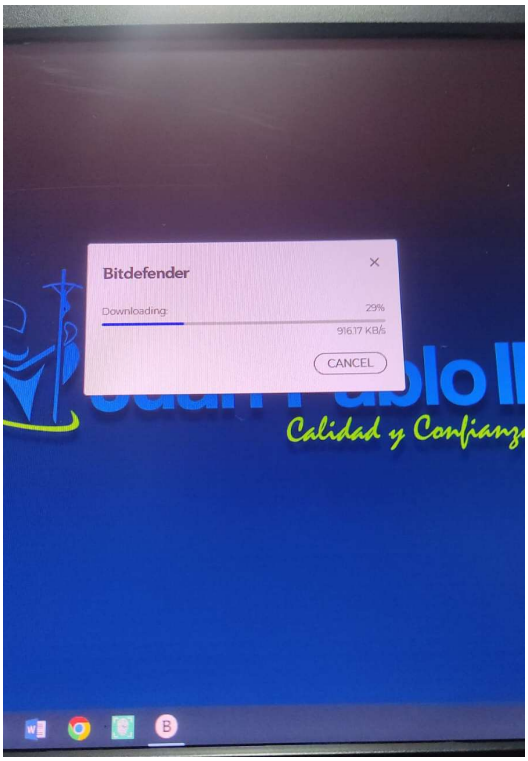


5) Switches y servidores dentro de gabinetes, rackeados.

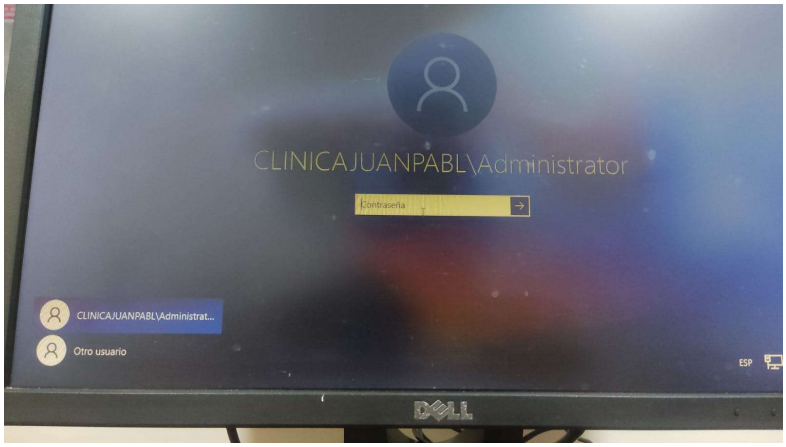
6) Cables de red y electricidad protegidos por canaleteas

7) Cables de periféricos de las computadoras protegidos y separados

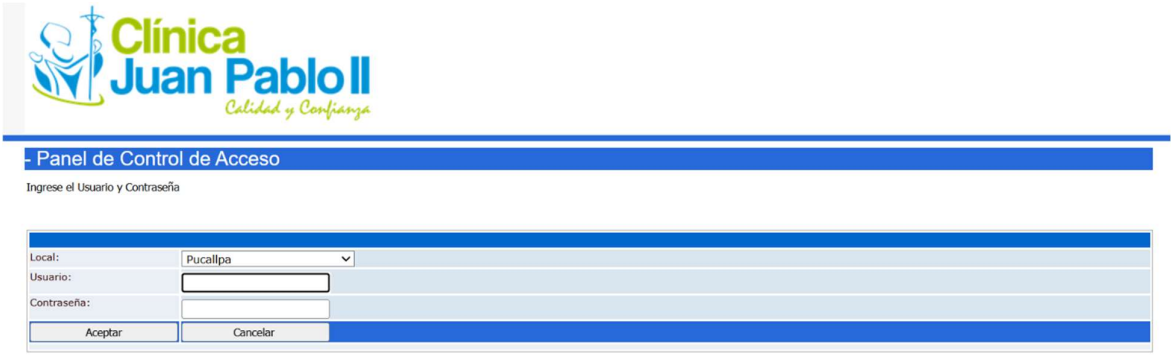
8) Computadoras con BitDefender



9) Acceso a las computadoras regulados por usuario y contraseña del dominio

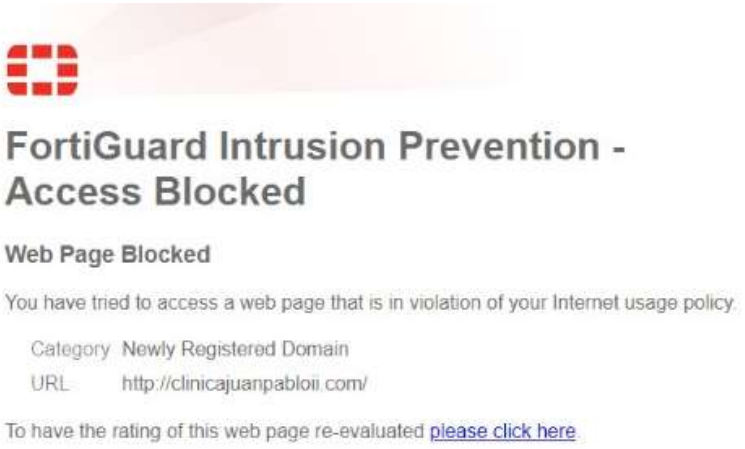


10) Acceso al software medico por medio de credenciales.



11) Presencia de humedad en los techos

12) Bloqueo de páginas que se categorizan peligrosas.



13) Lista de categorías afectadas por el filtro web.

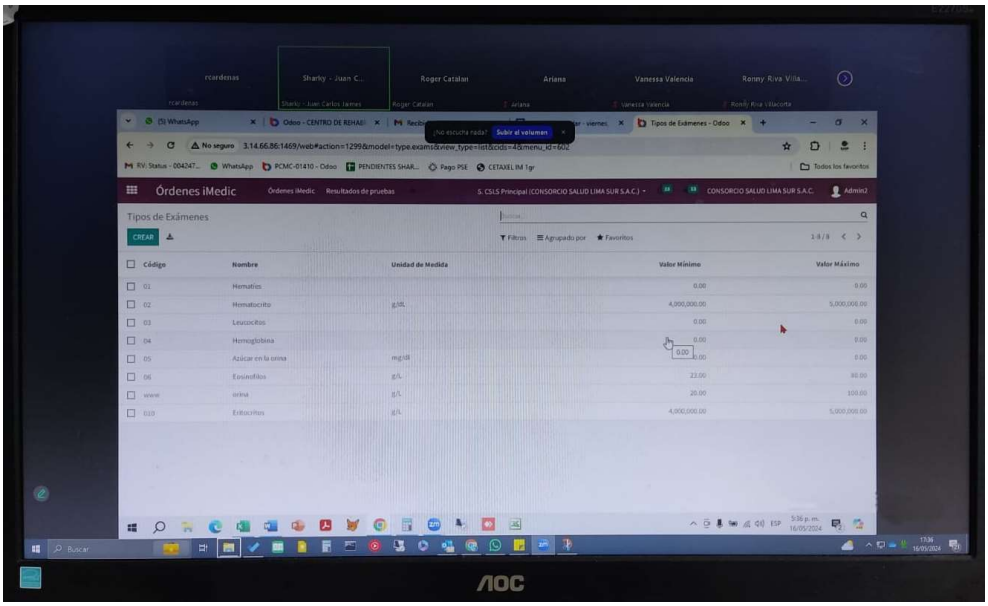
N°	Razón	Categorías
1	Contenido para adultos	• Aborto • Alcohol • Desnudez y subidas de tono • Lencería y trajes de baño • Pornografía • Otros materiales para adultos • Educación sexual • Ventas de armas • Otros
2	Interés General - Negocios	• Fuerzas armadas • Criptomoneda • Acortamiento de URL • Otros
3	Interés General - Personal	• Publicidad • Subasta • Trading • Diversión • Juegos • Viajar • Otros
4	Potencialmente responsable	• Abuso Sexual • Violencia infantil explícita • Hacking ilegal o poco ético • Terrorismo • Otros
5	Riesgo de seguridad	• Sitios web maliciosos • dominios recién registrados • phishing • Spam URLs • Otros

14) Back ups de correos electrónicos y archivos de computadoras.

8) Área diagnosticada: Desarrollo y calidad de software	
Descripción: En clínica el área de TI no está encargada de desarrollar software para clínica. Pero, sí está encargada de administrar el correcto funcionamiento de los sistemas.	
Pros: ▪ El equipo de TI está presente en las demostraciones de nuevos sistemas a adquirir. ▪ Se realizan pruebas del funcionamiento de las interfaces de los sistemas para ver si cumple con los requerimientos necesarios. ▪ Se realizan capacitaciones al personal para el correcto uso de los sistemas de clínica. ▪ Se cuenta con contratos fijos con las empresas desarrolladoras de sistemas, incluyendo un plan de soporte técnico constante.	Contras: ▪ Las revisiones de calidad de software y gestión de defectos no son periódicas. ▪ Procesos repetitivos presentes en las diferentes áreas de la clínica. Posible implementación de sistemas que apoyen en la automatización de estas. Sugerencias: Sistema gestor de historias clínicas, Sistema gestor de tickets atención para soporte técnico, Sistema logístico WMS para la gestión de almacenes.
Sugerencias: ▪ Gestionar revisaciones periódicas de la calidad de los sistemas de clínica y gestionar los defectos encontrados. ▪ Realizar foros informativos o documentación que sirva como introducción a los diferentes sistemas en clínica. Esto para facilitar el proceso de capacitación de nuevo personal.	

Evidencias:

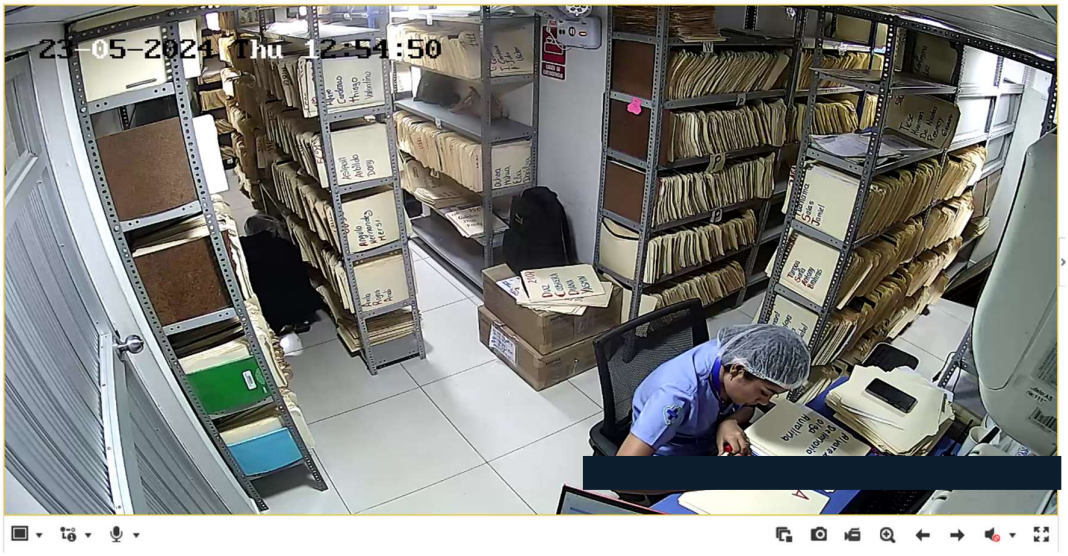
1) Participación en demostraciones de nuevos sistemas para clínica



<table>
<tr><td colspan="2">9) Área diagnosticada: Protección de datos de carácter personal (LOPD)</td></tr>
<tr><td colspan="2">Descripción: En clínica se trabaja con datos sensibles de los pacientes. Estos datos están guardados de manera física, en historiales médicos, como lógica, en base de datos.</td></tr>
<tr><td>Pros:
La recopilación de información privada es realizada únicamente por personal del equipo médico.
Almacenamiento correcto en ficheros físicos (historias médicas).
Sala de historiales médicos con acceso restringido por una puerta con llave y cámara de vigilancia en la habitación.
Determinación por parte del personal del equipo médico para resguardar la información privada de los pacientes.</td><td>Contras:
No se cuenta con documentación sobre protocolos de guardado y resguardado de datos personales de los pacientes.
Algunos datos recaudados de los pacientes no son exactos o no están actualizados.</td></tr>
<tr><td colspan="2">Sugerencias:
Establecer un protocolo estandarizado para el guardado y resguardado de datos personales de los pacientes, y documentarlo.
Realizar verificación y actualización de los datos de los pacientes, para así asegurar la calidad de estos.
Revisar la Ley N° 29733, Ley de protección de datos personales. Para así lograr un correcto tratado de los datos sensibles de lo pacientes y empleados de la clínica.</td></tr>
</table>

Evidencias:

1) Imagen de cámara de seguridad ubicada en sala de historias médicas. Visibilidad de correcto almacenamiento.



2) Acceso a sala de historias clínicas regulada por puerta con llave