APLICACIÓN DE CONTROLES DEL ESTÁNDAR ISO 27001:2013 PARA EL MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA CLÍNICA MAGIA Y ESPERANZA.

FREDDY JOSE MORALES MARTINEZ
JAVIER ALBERTO GALVIS TÁMARA

UNIVERSDAD COOPERATIVA DE COLOMBIA
CAMPUS MONTERÍA
SEMINARIO ADMINISTRACION, SEGURIDAD Y GESTION DE REDES

MARVIN LUIS PEREZ CABRERA
RUBEN ENRIQUE BAENA NAVARRO
JUAN MANUEL TORREZ TOVIO
ANGEL DARIO PINTO MANGONES

ASESORADO POR :
ONALVIS JOSE ESCUDERO OLASCUAGA

15 DE DICIEMBRE DE 2020

TABLA DE CONTENIDO

Titulo

Aplicación de controles del estándar ISO 27001:2013 para el mejoramiento de las políticas de seguridad de la información en la Clínica Magia y Esperanza.

Introducción

La digitalización de casi todo lo que nos rodea es evidente, a nivel general todo lo que se maneja es información, esta se mueve por la red de forma constante y es de vital importancia protegerla para que no sea robada ni usada con fines maliciosos. Las empresas deben contar siempre con los controles respectivos en pro de la seguridad de esta información, justo como lo estipulan las organizaciones rectoras. Estos controles se ven reflejados en las políticas de seguridad con las que cuentan, siempre fundamentadas en los estándares internacionales, como por ejemplo el ISO 27001. El objetivo principal es brindar y garantizar la debida protección a todos los datos.

Muchas empresas logran conformarse de una forma óptima, otras no, quizás por falta de recursos o incluso por desconocimiento sobre los lineamientos que deben seguir, es decir, cumplen a medias y no realizan un control riguroso sobre cómo se gestiona el manejo de la información de la que hacen uso en el día a día. Incluso existen empresas que no tienen en cuenta dichos controles, como lo es este caso de estudio.

Para la Clínica Magia y Esperanza, el punto clave es la seguridad de la información, por lo cual busca cuales son las estrategias, técnicas y herramientas disponibles que le permitan mitigar los posibles riesgos que atenten contra los datos que manejan. A través de estas estrategias, técnicas y herramientas se busca apoyar a la Clínica realizando una evaluación de sus políticas.

El propósito es saber en qué punto se encuentra la Clínica para tomar los correctivos necesarios, cuyo beneficio será la conformación de políticas fortalecidas que garanticen la seguridad de la información y la debida protección de los datos que se fundamenten en las normas y estándares pertinentes.

Resumen

La Clínica Magia y Esperanza se encuentra en un punto crítico debido a que desconoce por completo si está en el debido cumplimiento con respecto a las políticas de seguridad de la información, por lo tal deciden buscar ayuda profesional para evaluar su situación actual, para conocer en detalle lo que sucede y de esa forma poder tomar los correctivos necesarios.

Esto debe llevarse a cabo para que la empresa pueda garantizar la integridad de la información que se maneja a nivel interno, tal como lo menciona la Ley de Protección de Datos, apoyada por el Decreto 1377 de 2013.

Para llegar a una solución deben cumplirse tres fases, la fase de análisis, la fase de diseño y la fase de propuesta. Es decir, se van a analizar las condiciones en las que se encuentra la Clínica, tanto de parte física como lógica con respecto a la infraestructura que tienen en su red, a partir de los resultados de este análisis se procede a diseñar una estructura adecuada y posteriormente se realiza la debida propuesta para que se cumpla con todos los requerimientos y normativas pertinentes; cada una de estas fases van fundamentadas por el estándar ISO 27001:2013 dedicado a los Sistemas Gestión de la Seguridad de la Información.

Los resultados obtenidos no fueron alentadores, a partir del análisis se evidencia que no existen políticas de seguridad, no hay documentación alguna sobre estas, además de otros detalles referentes a los dispositivos y configuraciones de estos mismos, que no son las adecuadas. Por lo tanto, es un incumplimiento claro de la normativa y es necesario plasmar todo esto en la propuesta de mejoramiento.

Finalmente se procede a realizar la propuesta a la Clínica, donde se lista todo lo necesario para desarrollar políticas de seguridad en toda su regla, que cumplan con la norma y que le permitan mitigar todas las vulnerabilidades encontradas para mejorar la seguridad y la protección de la información.

Planteamiento Del Problema

La Clínica Magia y Esperanza considera necesario evaluar sus condiciones actuales en políticas de seguridad de la información, esto debido a que son conscientes de que no cuentan con un departamento de TI, que es la dependencia que se encarga de estas labores. Esto genera preocupación, teniendo en cuenta que la razón social de la Clínica Magia y Esperanza corresponde al sector de la salud.

Es de vital importancia que se pueda garantizar y asegurar la protección de toda la información sensible que se maneja de forma interna, desde datos personales básicos hasta diagnósticos e historias clínicas. El hecho de que no existe un departamento de TI es una muestra clara de que no se da la debida gestión a los procesos estipulados en la Ley de Protección de Datos, la cual está apoyada por el Decreto 1377 de 2013 y manifiesta:

> Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas. (MinTIC, 2013)

Dicho esto, la Clínica Magia y Esperanza debe procurar mantenerse al día con los requisitos y estándares legales de operación a nivel tecnológico y de sistemas. A raíz de esto, ha iniciado un proceso de convocatoria con el cual buscan ayuda profesional en pro de conocer en detalle su situación actual y realizar los correctivos necesarios.

Formulación Del Problema

¿Cómo es posible aplicar los controles del estándar ISO 27001:2013 en el fortalecimiento de las políticas de seguridad de la información en la Clínica Magia y Esperanza?

Objetivo General

Analizar las políticas, diseñar una estructura y proponer un plan de mejora para el fortalecimiento de seguridad de la información de Clínica Magia y Esperanza.

Objetivos Específicos

- Analizar las políticas de seguridad de la información existentes en la Clínica Magia y Esperanza aplicando el estándar ISO 27001:2013 para identificar vulnerabilidades e incumplimiento en normatividad.

- Diseñar una estructura de seguridad de la información que le permita a la Clínica Magia y Esperanza cumplir con los requerimientos estipulados en el estándar ISO 27001:2013 para establecer políticas que ayuden a la protección de la información.

- Proponer un plan de fortalecimiento para las políticas y controles de seguridad de la Clínica Magia y Esperanza que cumplan con lo estipulado en el estándar ISO 27001:2013 para mitigar los riesgos existentes.

Antecedentes

Reseña Histórica

La Clínica Magia y Esperanza es una institución sin ánimo de lucro, perteneciente al sector privado de la salud; en el año 2012 nace la Clínica Magia y Esperanza, a partir de un estudio del Doctor Omar García Banda, en el cual encontró la necesidad de crear una entidad prestadora de salud en una zona carente de ella y así, ofrecerle a la comunidad servicios de salud accesible y estos sean atendidos a tiempo, siempre y cuando su emergencia sea para tratamientos en casa. Esta institución inicia con una capacidad de atención de 6 camas para brindar los servicios básicos de salud, donde su objetivo es brindarle atención oportuna y estable al paciente y a su familia, donde la atención se caracterizará por el trato amable y humano. En sus inicios, la Clínica Magia y Esperanza, inaugura las salas colectivas para la atención de medicina general y de medicina interna. Es una institución que cuenta con una planta física actualizada y agradable, localizada estratégicamente y con fácil acceso para los pacientes. Es prestadora de servicios de salud de III nivel hospitalario con la infraestructura física, humana y administrativa necesaria para satisfacer las expectativas para la recuperación de la salud en el III nivel de atención. Nuestros procesos en las diferentes áreas se destacan en los siguientes aspectos:

- La eficiencia en la prestación de los servicios de la institución;
- El cumplimiento de altos estándares de calidad en un proceso continuo de aprendizaje y mejora;
- El aseguramiento de la sostenibilidad económica.

Basamos nuestros procesos en la orientación hacia el usuario a través del compromiso de su personal competente. Contamos con Talento Humano idóneo, en todas sus áreas: Médicos de Planta, Auditoría Médica, Coordinación Médica, Auxiliares de Enfermería, Coordinador de Atención al Usuario, Vigilante, Orientador, Auxiliares de Servicios Generales.

Misión

Somos una empresa prestadora de servicios de salud, socialmente responsable que brinda servicios de excelente calidad, en el departamento de Córdoba, respaldados por un talento humano competente en las áreas de medicina general y medicina interna, donde priorizamos en brindar una atención segura y con afectividad humana hacia el paciente y su núcleo familiar, en el cual nuestras políticas institucionales sean de excelencia, enmarcadas en talento humano, infraestructura adecuada, sistema de información veraz, oportuno y confiable; teniendo procesos de mejora continua y administración incluyente, garantizando la sostenibilidad social y financiera de la institución.

Visión

Para el año 2025, la clínica ampliará su cobertura en: laboratorio clínico y urgencias, y ofreciendo servicios de alta complejidad y altos estándares de calidad, asegurando la satisfacción del paciente y su familia; logrando impactar las condiciones de salud y ser distinguidos en el departamento de Córdoba y sus alrededores, siendo destacados como una entidad que ofrece excelentes servicios de salud.

Estructura Física

La Clínica solo tiene una sede y a nivel estructural cuenta con un solo piso para realizar sus labores y operaciones.

Internamente a grandes rasgos existe un área de recepción, una sala de espera, siete consultorios, un área de tratamiento de pacientes y dos pasillos.

Existen dieciocho computadores, de los cuales siete se distribuyen en los consultorios, cuatro se ubican en el área de atención de pacientes, tres están en la recepción, dos en la sala de estar para médicos, dos en el área de preparación; solo hay un servidor que se encuentra en un consultorio. Al fondo de un pasillo esta un rack donde se encuentra montado un switch administrable y al lado está el modem es provisto por el operador de servicio. Hay tres impresoras, una en la recepción y dos en el consultorio donde está el servidor. Adicional a eso se tienen dos routers Wi-Fi, uno de ellos está en el área de atención de pacientes y el otro en la recepción.

A nivel de cableado, el que se está usando es UTP categoría 4 ponchado sin bota protectora para los conectores RJ45. Todos los dispositivos tienen conexión cableada, es decir, desde el switch ubicado en el rack van los cables hasta cada equipo. Los demás dispositivos, como teléfonos móviles, se conectan a internet vía Wi-Fi.

Para una mejor ilustración se anexan los planos UNIDAD MEDICA CLINICA MIAGIA Y ESPERANZA 001 y UNIDAD MEDICA CLINICA MIAGIA Y ESPERANZA 002.

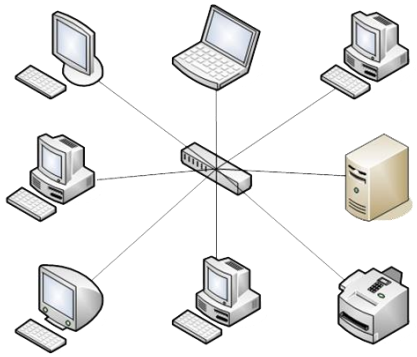
Topología De La Red

La topología de la red es lo que determina la forma en que están conectados o deben conectarse todos los dispositivos existentes entre sí para lograr la debida comunicación entre estos y así mismo un excelente funcionamiento de la red.

Para decidir cuál es la mejor topología que supla los requerimientos y necesidades se deben tener en cuenta varios factores como:

- Ubicación de los equipos;
- Software que se va a usar;
- Presupuesto;
- Cantidad de tráfico a soportar.

Topología Física



Fuente: (lifeder.com, https://www.lifeder.com/topologia-en-estrella/)

La topología que se maneja en la Clínica Magia y Esperanza es de tipo estrella, tal como se muestra en el esquema anterior, donde todo el tráfico se redirecciona mediante un switch administrable al que se conectan todos los dispositivos, computadores, servidor, routers e impresoras.

Dispositivos Y Especificaciones

Al realizar el inventario de los equipos se encuentra que todos están funcionales, pero se denotan algunos detalles.

Los computadores no cuentan con licencia del sistema operativo, están hacktivados y no tienen suite de antivirus debidamente instalada y configurada. El servidor empresarial cuenta con un sistema operativo bastante antiguo que no está licenciado y no cuenta la debida protección a nivel de antivirus, está conectado para acceso público en la WAN, es decir se puede acceder a este desde cualquier escritorio remoto.

En el único Rack, que no tiene ningún tipo de seguridad, está montado el switch administrable. El modem es provisto por el operador de Internet está configurado con una IP fija, hay tres impresoras multifuncionales y los routers Wi-Fi ofrecen conexión de Internet a los pacientes, pero no existe ningún tipo de segmentación, es decir, se conectan en el mismo entorno de red del servidor.

Equipos De Computo

Fabricante: Lenovo
Equipo: IDEACENTRE 700 AIO (24", INTEL)
Tamaño de memoria: 8GB
Modelo CPU: Core i5
Fabricante modelo CPU: Intel
Velocidad CPU: 2.7 GHz
Tamaño de pantalla: 23.8”
Coprocesador Gráfico: GTX 950A
Descripción de Gráficos: dedicados
Capacidad de almacenamiento: 1000 GB
Tipo de plataforma de hardware: Desktop

Servidor

Fabricante: HP (Hewlett Packard Enterprise)

Equipo: HP PROLIANT ML110 G7

Tamaño de memoria: 2GB

Modelo CPU: Xeon E3 – 1220

Fabricante modelo CPU: Intel

Velocidad CPU: 3.1 GHz

Capacidad de almacenamiento: 250 GB

Tipo de plataforma de hardware: Server.

Rack

Altura: 80 cm

Modem

Fabricante: Technicolor

Equipo: TC8305C

Puertos: 4 Ethernet, 2 de Telefonía, 1 USB

Acceso Wi-Fi: Si

Conexión de energía: 100-240VCA, 50/60Hz

Consumo de energía: ≤ 15.5 W

Switch

Fabricante: TP-Link

Equipo: TL-SG1024D

Estándares y protocolos: IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x

Interfaz: 10/100/1000 Mbps

Puertos: 24 RJ 45

Medios de red: Cable 3, 4 5, 10BASE-T: categoría UTP (máximo 100m)

100BASE-TX/1000BASE-T: Categoría 5 UTP, 5e o sobre cable (máximo 100m)

Montaje: Kit para Rack

Fuente de alimentación: 100-240VAC, 50/60Hz

Routers

Fabricante: TP-Link

Equipo: TL-WR940N

Estándares y protocolos: IEEE 802.11n/b/g 2.4 GHz

Interfaz: 2.4 GHz: 450 Mbps (802.11n)

Puertos: 1× 10/100 Mbps WAN; 4x 10/100 Mbps LAN

Fuente de alimentación: Adaptador Externo (Salida: 9VDC / 0.6A)

Impresoras

Fabricante: EPSON

Equipo: EcoTank L210

Sistema: EcoTank (tinta continua)

Tipo: Multifuncional (impresora, escáner, fotocopiadora)

RESUMEN DE DISPOSITIVOS		
TIPO	**MARCA Y MODELO**	**CANTIDAD**
PC desktop	Lenovo IDEACENTRE 700 AIO	18
Servidor	HP PROLIANT ML110 G7	1
Modem	Technicolor TC8305C	1
Swtich	TP-Link TL-SG1024D	1
Router	TP-Link TL-WR940N	2
Impresora	EPSON EcoTank L210	3

Consideraciones Sobre Software

Windows Server 2008

Windows Server 2008 (algunas veces abreviado como "Win2K8" o "W2K8") es el nombre de un sistema operativo de Microsoft diseñado para servidores.

Es el sucesor de Windows Server 2003, distribuido al público casi cinco años después. Al igual que Windows Vista, Windows Server 2008 se basa en el núcleo Windows NT 6.0 Service Pack 1. Entre las mejoras de esta edición, se destacan nuevas funcionalidades para el Active Directory, nuevas prestaciones de virtualización y administración de sistemas, la inclusión de IIS 7.5 y el soporte para más de 256 procesadores. Hay siete ediciones diferentes: Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server y para Procesadores Itanium.

Actualmente este sistema no tiene soporte por parte de Microsoft desde el 14 de enero de 2020. (Wikipedia, 2020)

Este sistema operativo fue el que vino de fabrica al comprar el servidor, fue formateado y omitieron la activación con la licencia, además de que no contemplaron realizar una actualización.

Windows 10

Windows 10 es el actual sistema operativo desarrollado por Microsoft como parte de la familia de sistemas operativos Windows NT. Fue dado a conocer oficialmente en septiembre de 2014, seguido por una breve presentación de demostración en la conferencia Build 2014. Entró en fase beta de prueba en octubre de 2014 y fue lanzado al público en general el 29 de julio de 2015.

Para animar su adopción, Microsoft anunció su descarga gratuita por un año desde su fecha de lanzamiento, para los usuarios que contasen con copias genuinas de Windows 7 (SP1) o Windows 8.1 Update. En julio de 2015 se habilitó una herramienta que permitía reservar esta actualización; dicha herramienta notificaba a cada usuario el momento en el que estaría lista la descarga de la actualización para su dispositivo, para así instalar la compilación 10240, la primera versión estable liberada. Los participantes en el programa Windows Insider podían recibir una licencia de Windows 10, pero con ciertas condiciones, entre ellas que su sistema operativo instalado (7, 8 u 8.1) fuese legítimo. (Wikipedia, 2020)

Los computadores vinieron de fabrica con este sistema operativo, pero tal como el servidor fueron formateados y omitieron la activación con la licencia, no se tuvo en cuenta realizar las debidas actualizaciones.

Office 2016

> Microsoft Office 2016 (nombre clave Office 16) es una versión de la suite de oficina Microsoft Office, sucesora de Office 2013 y de Office para Mac 2011 y predecesora de Office 2019. Fue lanzado en MacOS el 9 de julio de 2015 y en Microsoft Windows el 22 de septiembre de 2015 para suscriptores de Office 365. El soporte principal terminó el 13 de octubre de 2020 y el soporte extendido finaliza el 14 de octubre de 2025, al mismo tiempo que Windows 10. La versión con licencia perpetua en MacOS y Windows se publicó el 22 de septiembre de 2015. Office 2016 es la última versión oficialmente compatible con Windows 7 y Windows 8.1. (Wikipedia, 2020)

Esta versión de office venia preinstalada en los equipos, se venció en 60 días, luego fue hacktivado.

GoDaddy

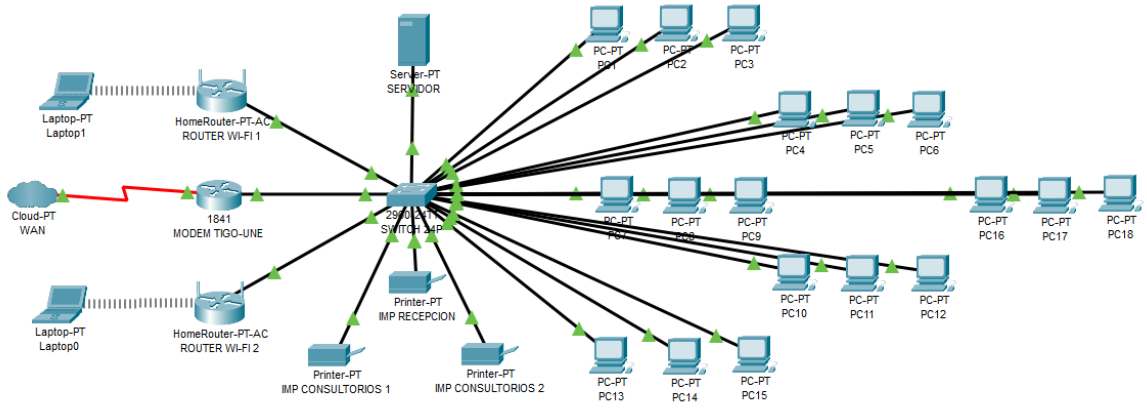
> Es una empresa registradora de dominios de Internet y de alojamiento web. En 2010 superó la cifra de más de 40 millones de dominios de Internet bajo su gestión. GoDaddy es actualmente la organización registradora de dominios más grande del mundo acreditada por ICANN. (Wikipedia, 2020)

En la Clínica Magia y Esperanza utilizan GoDaddy, la url del sitio web es https://clinicamagiayesperanza.com y para servicio de correo Microsoft 365.

Aun cuando Microsoft 365 ofrece el uso de Office en línea solo lo usan para las cuentas de correo, todo lo relacionado a ofimática se trabaja de forma local con Office 2016.

Conexión A Internet

De manera general se puede dar una muestra de cómo está conformada la red en la Clínica Magia y Esperanza con base a la visita realizada, cabe aclarar que al no contar con un departamento de TI que facilitase este esquema se tomó la decisión de simularlo en Cisco Packet Tracer, que es un programa que permite experimentar cómo se comporta una red en un entorno controlado. Se puede decir que “brinda una experiencia integral de Networking Academy, Packet Tracer, proporciona capacidades de simulación, visualización, autoría, evaluación y colaboración, y facilita la enseñanza y el aprendizaje de conceptos tecnológicos complejos.” (EcuRed, 2019)



Teniendo en cuenta el anterior esquema, se puede mencionar que la fuente de la conexión a internet está dada por el modem del proveedor de servicio, en este caso TIGO-UNE. Del modem va un cable hasta el switch que es el encargado de distribuir el tráfico a todos los demás dispositivos, incluyendo los routers Wi-Fi que se alimentan de cables UTP para reproducir la red de manera inalámbrica, permitiendo así que otros dispositivos se conecten.

Análisis De Riesgos

El análisis se lleva a cabo en base a lo estipulado en el estándar ISO 27001:2013 que se aplica para los Sistemas Gestión de la Seguridad de la Información, este instruye a las organizaciones en la realización de evaluaciones sobre posibles riesgos y la aplicación de controles necesario para mitigarlos.

Se decide usar este estándar teniendo en cuenta las preocupaciones expresadas por parte de la Clínica Magia y Esperanza, en cuanto a seguridad de la información el ISO 27001:2013 es el más pertinente. También cabe aclarar que este estándar ofrece la opción de que se genere una acreditación que en este caso no se aplicara ya que no es obligatoria. Según la documentación, para realizar la ejecución adecuada del análisis se debe tener en cuenta lo siguiente:

Anexo A

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN		
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información		
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.

Resultados Del Análisis

Después de haber realizado el debido análisis, es evidente que:

1. No existen políticas, no están debidamente documentadas.
2. No existe seguridad perimetral.
3. Los computadores están desactualizados y sin licencias.
4. El servidor esta desactualizado y sin licencias.
5. No existe una suite de antivirus debidamente instalada y configurada.
6. El modem del proveedor de servicio está configurado con una IP fija.
7. Se puede acceder al servidor desde cualquier equipo, incluso desde la WAN.
8. El cableado es categoría 4, por lo cual es bastante deficiente para transferencia de datos.

A partir de esta lista se puede decir que no existen políticas de seguridad, no hay documentación o evidencia alguna, esto deja a la Clínica Magia y Esperanza vulnerable a muchos tipos de ataque, como MiTM y Ransomware.

El MiTM (Man-in-the-Middle) “sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas entre el objetivo y la fuente” (Kaspersky, 2013) cuyo propósito es robar información. Por su parte se puede definir el ransomare como:

> Un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña. (Kaspersky, 2020)

Propuesta De Mejoramiento

Para mitigar los riesgos encontrados después de la revisión completa de las políticas, se propone:

1. Establecer políticas de seguridad ya que no existen.
2. Instalar y configurar un firewall que permita filtrar todo el tráfico que se distribuye en la red.
3. Activar las licencias del sistema operativo de los computadores y ejecutar las actualizaciones disponibles.
4. Instalar una versión de Windows Server más reciente en el servidor empresarial con su debida licencia de activación.
5. Comprar, instalar y configurar una suite de antivirus capaz de detectar la gran mayoría de amenazas y mantenerlo actualizado.
6. Realizar una nueva configuración del modem donde no se trabaje con IP fija, lo ideal sería usar IP dinámicas (DHCP).
7. Realizar una segmentación adecuada de la red para que solo el personal autorizado tenga acceso al mismo entorno que el servidor, los demás usuarios solo tendrán conexión a internet.
8. Cambiar todo el cableado a categoría 6 para mejorar la eficiencia del tráfico de datos.

A.8 GESTIÓN DE ACTIVOS		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

A.9 CONTROL DE ACCESO		
A.9.1 Requisitos del negocio para control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.5 Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales.		
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.

A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

En las tablas se describen los puntos que soportan el listado de la propuesta.

La Clínica Magia y Esperanza es del sector salud y la Ley 1581 de 2012, en su Titulo 3 menciona que los datos relacionados a la salud se clasifican “como un tipo de dato destacado y que merece especial protección.” (Monroy, 2019)

A partir de esto, las políticas que se consideran pertinentes para desarrollar en la Clínica Magia y Esperanza son:

1. Establecer cultura de seguridad.
2. Establecer control de acceso a la información protegida.
3. Protección y mantenimiento de los dispositivos.
4. Mantener higiene cibernética.
5. Configurar debidamente un cortafuegos o “firewall”.
6. Instalar y mantener un software antivirus.
7. Realizar copias de seguridad de los datos.
8. Usar contraseñas seguras con cambios de forma regular.
9. Establecer controles de acceso físico.

La red no cuenta con ningún tipo de seguridad perimetral lógica o física, puesto que no existe firewall y la ubicación del Rack está al alcance de cualquier empleado o usuario que ingrese en las instalaciones de la Clínica. Para dar solución a la parte lógica se recomienda adquirir un nuevo dispositivo, el Qotom Mini Pc Q190g4, este es compatible con pfsense, una distribución libre que se emplea como firewall y enrutador. A nivel de configuración se asignan todas las reglas para el debido filtro del tráfico y acceso a la red, listas de control de acceso, así como la creación de una VPN que impulse el trabajo remoto y el uso de Snort, sistema para la detección de intrusos en la red. Todo esto se lleva a cabo entre el modem y el switch, así es como se establece el primer control. Para la parte física se recomienda cambiar el sitio de ubicación del rack, puede ser a un cuarto de servicio en donde solo el personal autorizado tenga acceso.

Adicional a esto, a nivel lógico se deben bloquear los puertos que se usan normalmente para el circuito cerrado de cámaras de seguridad, ya que al estar con acceso libre representan una vulnerabilidad latente y oportunidad para los atacantes.

A nivel de software, refiriéndose a los equipos de cómputo, se debe proceder a activarlos bajo licencias debidamente adquiridas y actualizar el sistema operativo a la última build, la ventaja es que ya los equipos cuentan con Windows 10.

En el caso del servidor, que tiene Windows Server 2008 se debe instalar una versión más reciente, se recomienda Windows Server 2016 R3 con su respectiva licencia y actualización a su última build.

Aun cuando Windows 10 y Windows Server 2016 R3 cuentan con Windows Defender como antivirus, es importante adquirir una suite más robusta, que sea capaz de detectar, malware, spyware y virus que pretendan ingresar en los equipos. La recomendación, para este caso y según lo analizado, es Kaspersky Endpoint Security, este mismo permite realizar todas las configuraciones desde el servidor, también se instala la parte de los clientes en los computadores.

Para la segmentación de la red se propone el uso de dos VLAN, una administrativa donde solo estarán los equipos del personal autorizado con acceso al servidor y una de servicio que es donde se conectaran agentes externos. Para la creación de estas VLAN será necesario realizar subnetting, así cada una tendrá su propio segmento, la distribución de las IP en los equipos se

hará por DHCP, pero no de forma normal, se hará de manera estricta usando pfsense, este ayudará a la asignación única de las IP a los equipos usados en la empresa.

Para garantizar la mejor eficiencia en transferencia de datos es importante adquirir e instalar cableado de categoría 6 debido a que el existente que es de categoría 4 no es muy fiable actualmente. Quizás es algo que no se considera mucho, pero al final un buen cableado puede hacer una gran diferencia.

A continuación, se ilustra de una forma gráfica la manera en que estaría constituida la red después de aplicar el plan de mejoramiento.

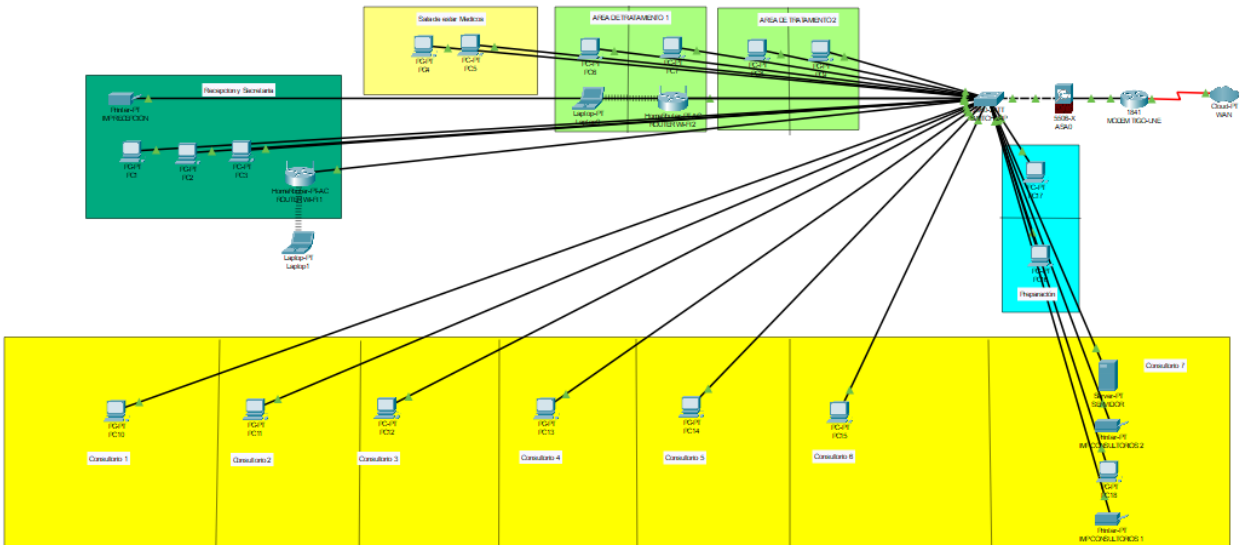


Tabla de enrutamiento

Nro.	SubRed	Mascara Subred	Broadcast	Primer Host	Ultimo Host
*1	192.168.10.0	255.255.255.224	192.168.10.28	192.168.10.1	192.168.10.28
2	192.168.10.29	255.255.255.224	192.168.10.61	192.168.10.30	192.168.10.60
3	192.168.10.61	255.255.255.128	192.168.10.181	192.168.10.62	192.168.10.180
*4	192.168.10.182	255.255.255.128	192.168.10.253	192.168.10.183	192.168.10.254

(Las direcciones marcadas con * no se tienen en cuenta para las asignaciones.

Conclusiones

Todo el proceso que requirió este informe permite adquirir un gran conocimiento en todo lo referente a la gestión de redes, para este caso de estudio se hace más énfasis en cuestiones de seguridad y a futuro este conocimiento queda para cualquier momento en que se desee aplicar en el debido análisis, diseño y propuesta de planes que mejoren este aspecto en las empresas.

Existen normativas establecidas, pero depende de las necesidades de cada empresa cuales son las que se deben aplicar, es necesario documentarse bien para realizar las evaluaciones y así obtener los resultados más precisos ya que de esto depende el desarrollo de las fases necesarias en el mejoramiento en cuanto a políticas de seguridad.

La escalabilidad futura de las políticas de seguridad depende enteramente de hacia donde quiera llegar la empresa, de cuanto vaya a expandirse y de las necesidades que surjan mediante esa expansión, aun así, siempre se deben tener todos los factores para realizar cada proceso con los mayores estándares de calidad, siempre teniendo en cuenta las normas y regulaciones planteadas por los organismos rectores Nacionales e Internacionales.

En cuanto a hardware y software, siempre es ideal optar por lo mejor que se pueda adquirir, ya que no se puede dejar de lado el presupuesto de la empresa. Es de mucha importancia adquirir siempre equipos nuevos, no de segunda mano, en el caso de hardware, a nivel de software existe mucha flexibilidad, ya que hay programas open source que facilitan un poco el manejo de las configuraciones y es amigable con los costos. Tampoco se debe pasar por alto las normas legales y las licencias requeridas para cada dispositivo.

Todo lo dicho anteriormente debe ir de la mano con la experiencia y las buenas practicas que se deben desarrollar para llevar a cabo los procesos referentes a la conformación de las políticas de seguridad en una empresa.

Aclaramos que la Clínica Magia y Esperanza que no existe en la vida real y fue creada con fines académicos para la realización de este informe.

Bibliografía

EcuRed. (6 de Diciembre de 2019). Obtenido de Cisco Packet Tracer: https://www.ecured.cu/Cisco_Packet_Tracer

Kaspersky. (8 de Abril de 2013). Obtenido de ¿Qué es un ataque Man-in-the-Middle?: https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

Kaspersky. (2020). Obtenido de ¿Qué es el ransomware?: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

lifeder.com. (https://www.lifeder.com/topologia-en-estrella/).

MinTIC. (27 de Junio de 2013). DECRETO NÚMERO 1377 de 2013. *"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"*. Bogotá, Colombia.

Monroy, S. (26 de Junio de 2019). *dondoctor*. Obtenido de Protección de datos en hospitales: Políticas de seguridad informática: https://dondoctor.com/sector-salud-colombia/proteccion-de-datos-en-hospitales-10-politicas-de-seguridad-informatica/

Wikipedia. (24 de Noviembre de 2020). Obtenido de Windows Server 2008: https://es.wikipedia.org/wiki/Windows_Server_2008

Wikipedia. (12 de Diciembre de 2020). Obtenido de Windows 10: https://es.wikipedia.org/wiki/Windows_10

Wikipedia. (31 de Octubre de 2020). Obtenido de Office 2016: https://es.wikipedia.org/wiki/Microsoft_Office_2016

Wikipedia. (21 de Marzo de 2020). Obtenido de GoDaddy: https://es.wikipedia.org/wiki/GoDaddy