UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN - MANAGUA

Facultad Regional Multidisciplinaria, Matagalpa

UNAN Managua - FAREM Matagalpa

MONOGRAFÍA PARA OPTAR AL TÍTULO DE INGENIERO EN SISTEMA DE INFORMACIÓN

Tema:

Evaluación de la Infraestructura de la red LAN en Sistema Local de Atención Integral a la Salud (SILAIS – Matagalpa), basada en la normativa de estándares ISO 27002 – 2013, período 2019.

Autores:

Br. Álvaro Francisco Muñiz Zapata

Br. Juan Pablo Pravia Valdivia

Tutor:

MSc. Erick Noel Lanzas

Abril, 2019

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN - MANAGUA

Facultad Regional Multidisciplinaria, Matagalpa

UNAN Managua - FAREM Matagalpa

MONOGRAFÍA PARA OPTAR AL TÍTULO DE INGENIERO EN SISTEMA DE INFORMACIÓN

Tema:

Evaluación de la Infraestructura de la red LAN en Sistema Local de Atención Integral a la Salud (SILAIS – Matagalpa), basada en la normativa de estándares ISO 27002 – 2013, período 2019.

Autores:

Br. Álvaro Francisco Muñiz Zapata

Br. Juan Pablo Pravia Valdivia

Tutor:

MSc. Erick Noel Lanzas

Abril, 2019

DEDICATORIA

“El que posee entendimiento ama su alma; el que guarda la inteligencia hallara el bien”.

Proverbios 9:8.

A Dios, nuestro creador por darme el privilegio de la vida y por bendecir mi andar.

A mis padres, por ser mi apoyo incondicional emocional y económico; a mi padre Marvin Muñiz por ser ese hombre que me ayudo a forjar mi carácter, a mi incondicional madre Yelba Zapata por ser esa mujer valiente y de carácter que siempre habla con la verdad, a mi hermano Jader Muñiz Zapata, por ser el pilar en mi andar, hasta el cielo a mis abuelos que me formaron con valores y mucho amor incondicional.

A mis ilustres maestros, que con su profesionalismo, compañerismo y honestidad forjamos no solo lazos de conocimientos sino lazos de hermandad.

Br. Álvaro Francisco Muñiz Zapata

DEDICATORIA

A Dios, por el don de la vida, por llenarme de virtudes y fuerza para seguir día a día cumpliendo cada meta plasmada en mi corazón.

A mis padres, Israel Pravia por ser el pilar en mi vida por estar en todo tiempo extendiendo su apoyo moral y económica, a mi preciada madre Inocelia Valdivia por su amor incondicional y persistencia de enseñarme a siempre luchar.

A mi tía, Amada Valdivia por ser mi apoyo y amiga incondicional.

A mi gran amigo, Álvaro Francisco Muñiz Zapata mi compañero de lucha, por extender su brazo amigo sin medida.

Bienaventurado el hombre que persevera bajo la prueba.

Santiago 1:12

Br. Juan Pablo Pravia Valdivia

AGRADECIMIENTO

A Dios por el privilegio de la vida y por bendecir mi camino en todo tiempo.

A la Institución SILAIS – MATAGALPA, por brindar el espacio, el tiempo, la accesibilidad a sus instalaciones y equipos, al personal administrativo y al personal de apoyo que nos ayudaron durante esta investigación.

Al Ingeniero Oscar Danilo Mendoza, un gran amigo que nos extendió sus conocimientos.

Al tutor MSc. Erick Noel Lanzas un gran y admirable caballero quien con su experiencia y sus conocimientos nos guio durante esta investigación,

El mayor placer de la vida es hacer lo que la gente dice que no puedes.

“Por qué Jehová da la sabiduría, y de su boca viene el conocimiento y la inteligencia”.

Proverbios 2:6.

AGRADECIMIENTO

A Dios por ser dador de vida, fortaleza, sustento y guía en mi camino.

A mi familia en general y amigos que siempre estuvieron para brindarme su brazo amigo. En especial a mis padres Israel Pravia e Inocelia Valdivia, mi tía Amada Valdivia por brindarme su apoyo incondicional en todo momento.

Al tutor Erick Noel Lanzas Martínez por ayudarnos en el camino de la perseverancia, por compartir sus conocimientos en el proceso investigativo.

A la universidad Nacional Autónoma de Nicaragua por el apoyo de abrir las puertas a jóvenes que un día soñamos con ser profesionales.

A la institución SILAIS-MATAGALPA y su personal por abrirnos camino y emprender la meta de ser investigadores.

No nos cansemos de hacer el bien, porque a su debido tiempo cosecharemos si no nos damos por vencidos.

Gálatas 6:9

CARTA AVAL DEL TUTOR

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

FACULTAD REGIONAL MULTIDISCIPLINARIA, MATAGALPA

UNAN – MANAGUA, FAREM – MATAGALPA

El suscrito tutor de Monografía para optar al título de Ingeniería en Sistemas de Información, de la Facultad Regional Multidisciplinaria de Matagalpa, de la Universidad Nacional Autónoma de Nicaragua, UNAN – Managua, por este medio extiende:

CARTA AVAL

A los bachilleres ***Álvaro Francisco Muñiz Zapata*** *(Carné 10064339) y* ***Juan Pablo Pravia Valdivia*** *(Carné 10063349)*, dado que el informe final titulado: "*Evaluación de la infraestructura de la red LAN en* SILAIS MATAGALPA *basada en la normativa de estándares ISO 27002-2013, periodo 2019*", cumple los requisitos establecidos para su defensa ante el tribunal examinador.

Dado en la ciudad de Matagalpa, a los veintidós días del mes de abril del año dos mil diecinueve.

_____

M Sc. Erick Noel Lanzas Martínez
Tutor de Monografía

RESUMEN

La presente investigación muestra la evaluación de la infraestructura de la Red de Área Local (LAN) en el Sistema Local de Atención Integral (SILAIS-MATAGALPA), basada en la normativa de estándares ISO 27002-2013, periodo 2019.

La estructura de la investigación en base a los objetivos específicos, los cuales se definieron las variables de estudio que fueron desarrolladas en el marco teórico; el universo de estudio la Red de Área Local (LAN), aporta el criterio necesario para desarrollar dicha evaluación, donde a través de la aplicación de la guía de mejoras e instrumentos, tales como: entrevistas dirigidas al responsable de informática, guías de observaciones, se logra identificar las principales debilidades y que existe en lo antes mencionado.

Los resultados alcanzados a través de esta investigación exponen, que en SILAIS-MATAGALPA, no existe un área de informática estructurada, no preexisten normativas y políticas de seguridad lógicas y físicas implementadas, el responsable de informática no está capacitado para dar la atención y mantenimiento necesario a la infraestructura física y lógica de la red LAN, por lo tanto, se propone atender la guía de recomendaciones de esta investigación.

ÍNDICE

Índice de Figuras

Índice de Tablas

Índice de Gráficos

Índice de Anexos

CAPÍTULO I

1.1. INTRODUCCIÓN

Las redes de computadoras han contribuido en gran manera a la mejora de las tecnologías de la comunicación y a la implementación de muchas nuevas. Hoy en día, a través del entramado de dichas redes, viajan datos generados por millones de personas a lo largo del mundo, dicha información puede adquirir diferentes valores, dependiendo de lo que representan para sus propietarios.

El uso de tecnologías de redes es una necesidad vital en las instituciones, ya que brinda beneficios de interconexión. Desde hace algunos años las instituciones educativas en salud han destinado recursos económicos para la obtención y retroalimentación de la información en los futuros profesionales, con el objetivo de encontrar debilidades en las plataformas y sistemas multimedia que hacen uso de la conexión a la red, para esto existen evaluaciones fundamentales tanto físicos como logísticos.

El objeto de estudio de esta investigación se centró en la evaluación de la Red de Área Local (LAN) en el Sistema Local de Atención Integral (SILAIS-MATAGALPA) con el apoyo de controles de seguridad y manuales de buen uso, la norma (ISO 27002-2013), periodo 2019. Para ello, se realizó una descripción del estado actual de la red LAN y se identificaron problemáticas existentes para sugerir mejoras a las dificultades encontradas.

Este documento está estructurado según la normativa de graduación de UNAN-Managua, la cual orienta ubicar los títulos por capítulos: capítulo I (introducción, planteamiento del problema, justificación, y objetivos de investigación); capitulo II (marco referencial y preguntas directrices); capitulo III (diseño metodológico); capitulo IV (análisis y discusión de resultados); y finalmente capítulo V (conclusiones, recomendaciones, bibliografía).

1.2. PLANTEAMIENTO DEL PROBLEMA

El sistema local de atención integral en salud (SILAIS - MATAGALPA) es una organización gubernamental de carácter administrativo conformada por compañeros y compañeras que laboran por la vigilancia y supervisión de la salud en los diferentes puestos de atención en la ciudad de Matagalpa y los municipios que la conforman.

Esta organización busca fortalecer los servicios de salud prestados a: niños, niñas, jóvenes; adultos, ancianos; misma sin fines de lucro. Para la institución SILAIS-MATAGALPA, se ha vuelto importante contar con servicios básicos de redes y comunicaciones, esta infraestructura básica permite brindar los múltiples servicios de comunicación local y gestión de información a todas las dependencias de la institución, además de permitir su presencia activa en la red mundial Internet.

La institución SILAIS – MATAGALPA, cuenta con una estructura de red LAN que en momentos actuales tiene un elevado porcentaje de inseguridad y déficit de estructuración, sobre todo el poco aprovechamiento, para la mejora de procesos críticos que esta institución define como prioritarios, dando un indicador negativo en los procesos de calidad, resulta claro que el diseño de este sistema de cableado, estructurado deberá caracterizarse por soportar un ambiente escalable multiproducto y multiproveedor, además de poder permanentemente soportar una amplia gama de productos de telecomunicaciones sin necesidad de ser modificada, estando abiertos a la expectativa de nuevos protocolos, productos y servicios de red.

Por lo antes descrito se plantea la siguiente problemática:
¿En qué estado se encuentra la infraestructura de red LAN en SILAIS - Matagalpa, con respecto a estándares y controles de seguridad bajo la normativa ISO/IEC 27002:2013?

1.3. JUSTIFICACIÓN

Esta investigación consiste evaluar la infraestructura de Red LAN en el Sistema Local de Atención Integral en Salud (SILAIS-MATAGALPA), la investigación radica en la evaluación de dicha red, bajo la norma ISO/IEC 27002:2013, para investigar si éstos se cumplen a cabalidad.

Debido a que no existe el área de informática se ve la necesidad de evaluar la infraestructura de red de la institución, ya que esta no está estructurada o certificada con estándares de calidad, y así poder proponer recomendaciones y mejoras en base a los hallazgos encontrados.

Al evaluar la red de datos, se podrán identificar las mejoras que se ofrecerán a los diferentes procesos y al responsable de informática que es quien lleva a cabo la supervisión de la red en el día a día en; SILAIS - MATAGALPA, para garantizar que el tráfico de red en tiempo real cumpla estabilidad, disponibilidad, seguridad y confiabilidad de la información.

Por lo antes citado existen razones suficientes, para llevar a efecto el trabajo investigativo dentro de la infraestructura de red LAN, y así entender cuáles son sus procedimientos, para formular una consistente fiable y profesional propuesta a situaciones encontradas tomando muy en cuenta criterios; éticos y profesionales que estén apegados a la seguridad e integridad en todo momento y lugar.

Los beneficiarios directos serán el administrador de la red y los usuarios finales la población de la ciudad de Matagalpa, debido a que la misión principal de SILAIS-MATAGALPA, es vigilar alertas tempranas para mitigar riesgos y enfermedades referentes al bienestar de la salud del pueblo, gracias a las estadísticas obtenidas por sus sistemas de información, en sus diferentes sedes de salud.

El resultado de esta evaluación permite aportar las recomendaciones necesarias para mejorar el funcionamiento de la red LAN.

1.4. OBJETIVOS DE INVESTIGACION

General:

Evaluar la infraestructura de la red LAN en SILAIS - MATAGALPA bajo los estándares y controles de seguridad de la normativa ISO/IEC 27002:2013, periodo 2019.

Específicos:

1. Describir el estado actual de la red LAN en SILAIS-MATAGALPA.

2. Identificar dificultades encontradas en la infraestructura de la Red LAN bajo la normativa ISO/IEC 27002:2013.

3. Proponer estándares de calidad y normativas de seguridad basadas en los hallazgos y dificultades encontradas en esta investigación, bajo la normativa ISO/IEC 27002:2013.

CAPÍTULO II

2.1. MARCO REFERENCIAL

2.1.1. Antecedentes

Evaluar estructuras de redes de datos es un tópico que poco se aborda en Latinoamérica; pues se confía mucho en que basta una buena documentación y requisitos bien definidos ya sean por parte del operador, por parte del creador, o el encargado de dicha Red, sin embargo, existen elementos que llevan a creer de la carencia de ciertos conocimientos que están en constante cambio para el correcto uso de estas grandes estructuras de tráfico de datos.

Europa

En Madrid, España, Tapiador (2010), en la universidad Carlos III de Madrid. En el Departamento de Informática se realizó una auditoría a los Sistemas de Comunicación y Redes, se han seguido las directrices marcadas por la ISO/IEC 27002: 2005 el objetivo de este proyecto ha sido la elaboración de una guía actualizada para realizar una auditoría a los sistemas de Comunicación y Redes para ello se han seguido las directrices marcadas por la ISO/IEC 27002: 2005. Además de las directrices marcadas por la ISO se han llevado a cabo ciertas comparativas en los puntos procedentes de la guía relacionándolos con COBIT e ITIL, la parte central del proyecto son los siguientes puntos que son la elaboración de la guía aplicable a las redes de datos de la empresa. Consiste en filtrar los controles de la ISO 27002 aplicables a las redes.

Sudamérica

En Guayaquil, Ecuador, Mideros & Chalén (2007), en la empresa LUBTECHNOLOGY SOHO, optan por el título de Ingeniero en Electrónica y Telecomunicaciones, mediante una tesis bajo el título “Auditoría de seguridad en redes y datos bajo la norma ISO 17799, mediante la auditoria se logró la optimización del desempeño de la red, dicha auditoría comprendió el estado de la seguridad de la red, se localizaron problemas en cuanto a la seguridad de la red, por lo cual se recomendó a la gerencia de la empresa LUBTECHNOLOGY hacer revisiones periódicas en la red.

Centroamérica

En San Miguel, Salvador Bolainas & Gómez (2003), optaron por el título de Ingeniero en Electrónica, con el tema "Seguridad en Redes de Datos", mediante la investigación se encontraron problemas de seguridad de los datos en la infraestructura física, por lo tanto, se propuso la implementación de una norma ISO que contribuya a la homogeneización de la seguridad de los datos y aplique políticas de seguridad, así también la implementación de tarjetas inteligentes o dispositivos biométricos que autentiquen la entrada física a los sistemas críticos.

Matagalpa, Nicaragua

En el año 2005, el tema de Seminario de Graduación para el V año de Ciencias de la Computación fue Auditoría Informática, siendo uno de los subtemas: Auditoría Informática aplicada a la red del CUR- MAT UNAN Managua, durante el segundo semestre del año 2005.Realizada por Br, Claudia Leticia Zeledón Chavarría y Br. Nydia Adelayda Brown Salgado, en este trabajo se revisaron diversos puntos necesarios para la implementación adecuada de una red de computadoras, pero les faltó fundamentación en estándares internacionales, además que sus recomendaciones no fueron dadas a conocer a las autoridades de UNAN FAREM, y por tanto no fueron implementadas. (Zeledón Chavarría & Brown Salgado, 2005).

Tres años después, en el año 2008, Sáenz & Arauz, realizaron un trabajo para su Seminario de Graduación cuyo tema fue Software Libre, y su subtema: "Reestructuración del diseño de la red, en el Recinto Universitario Marianos Fiallos Gil CUR Matagalpa – UNAN Managua, proponiendo la implementación de un servidor con plataforma Open Source y terminales con UBUNTU, para el departamento docente, durante el periodo 2008".

López & Zamora (2013), realizaron el tema de Evaluación de la Red Inalámbrica en el Hospital Escuela César Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002, periodo 2013.

En la Universidad Nacional Autónoma de Nicaragua, Managua, Facultad Regional Multidisciplinaria - Matagalpa, Blandón & Galdámez (2016), realizaron una evaluación de redes llamada “Evaluación de la infraestructura de la Red LAN, “Empresa CECOCAFEN”, basado en el Modelo de Objetivo COBIT 4.1, Matagalpa, Primer Semestre 2016”, donde se analizó la red de esta empresa mediante COBIT 4.1, para así poder determinar el nivel de madurez y seguridad de la misma. Se encontraron múltiples problemas de seguridad en la red, como cableado mal estructurado, topología de red mal implementada, virus en las computadoras y se determinó que el nivel de madurez es bajo en los dominios de COBIT que se aplicaron, por lo tanto, se realizó una propuesta de mejora, la cual detalla las pautas que se podrían implementar a la infraestructura de red para mejorar y minimizar los riesgos encontrados en la seguridad.

En la Universidad Nacional Autónoma de Nicaragua, Managua, Facultad Regional Multidisciplinaria - Matagalpa, Tercero & Castillo (2016), realizaron una evaluación de la infraestructura de red LAN, bajo la norma ISO/IEC 27002:2013, en la Alcaldía Municipal de San Ramón, Matagalpa, primer semestre 2016, se presentó una guía de mejoras, la cual podría minimizar los riesgos de la seguridad de la información.

2.1.2. Marco teórico

2.1.2.1. Redes

(Cisco Systems, 2014), en 1975, ARPAnet comenzó a funcionar como red; sirviendo como base para unir centros de investigación militares y universidades, a partir de esta se trabajó en desarrollar protocolos más avanzados para diferentes tipos de ordenadores y cuestiones específicas. En 1983 se adoptó el protocolo TCP/IP como estándar principal para todas las comunicaciones, y en 1990 desapareció ARPAnet para dar paso junto a otras redes TCP/IP a Internet.

Actualmente cada computador personal está equipado para poder interconectarse a cualquier red de datos, en todo momento y lugar, además a de poder viajar hacia Internet, con los debidos estándares y protocolos que se ofrecen hoy en día por los fabricantes de tecnología.

Hoy en día hay miles de millones de redes que se unen a diario cada minuto, dentro de la red de redes a como se suele llamar pero que no es más que internet la red entramada más grande del mundo.

2.1.2.1.1. Definición

(Cisco Systems, 2014), una red “es el medio óptico de enlace de datos más fiable y con mayor crecimiento en la actualidad”.

Desde un punto de vista técnico se comprende por red a un conjunto de máquinas conectadas entre sí con el fin de compartir información en un determinado tiempo y espacio. Esta transmisión utiliza diferentes medios, sea el aire con sus ondas de radio, microondas o medios guiados a través de impulsos eléctricos que viajan por cables de fibra óptica, enlaces seriales o cables UTP, Unshielded Twisted Pair (lo que puede traducirse como “Par trenzado no blindado”).

Las empresas utilizan las redes de datos como medios eficaces de comunicación, para transmitir datos y estadísticas en tiempo real para la mejora de sus procesos.

2.1.2.1.2. Servicios

(Cisco Systems, 2014), los servicios de red son programas de computación que respaldan la red humana. Distribuidos en toda la red, estos servicios facilitan las herramientas de comunicación en línea como emails, foros de discusión, boletines, salas de chat y Mensajería instantánea. Por ejemplo: en el caso un servicio de mensajería instantánea proporcionado por dispositivos en la nube, debe ser accesible tanto para el emisor como para el receptor.

Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas y de multimedia; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen World Wide Web, email, mensajería instantánea WhatsApp y telefonía IP o presencial como Skype.

La academia de CISCO describe los servicios de red como programas de computación que respaldan la red humana, ya que facilitan la comunicación entre sus usuarios, el servicio web es el comúnmente más utilizado.

Gracias a estos estudios de fines y propósitos militares se da a conocer lo que hoy en día podemos definir como internet.

2.1.2.1.3. La generación de los protocolos

(Cisco Systems, 2014), la familia TCP/IP, que implicaba varias decenas de protocolos, define un modelo de 4 capas de red. Se trata de los conocidos protocolos de comunicación y aplicación para conectar sistemas heterogéneos, independientes de la capa física.

El Transmission Control Protocol (TCP) es un protocolo de enrutamiento que garantiza un servicio fiable, orientado a la conexión de un grupo importante de octetos. En contraste con el TCP, el Datagram Protocol (UDP) es el protocolo de enrutamiento no orientado a la conexión. Es muy rápido, pero poco fiable.

En Nicaragua y sus empresas el control de transmisión de protocolos se lleva a cabo gracias a la seguridad y confianza que ha demostrado el tcp/ip Versión 4.

a) IPv4

(Cisco Systems, 2014) , el Internet Protocolo (IP) proporciona un sistema de entrega de paquetes, sin conexión y no fiable. Administra las direcciones lógicas, que dividen el identificador del nodo en un número de red lógico y un número de periférico sobre 4 octetos (en IP versión 4).

Evoluciona la era global como protocolo firme y confiable en el mundo digital no obstante con limitaciones debido a las grandes expansiones de dispositivos finales conectados a internet.

Actualmente el más usado dentro de Centroamérica y nuestro país por los (ISP) proveedores de servicios de internet.

b) IPv6

(Cisco Systems, 2014), a principios de los años noventa, Grupo de Trabajo de Ingeniería de Internet (IETF) centró su interés en el agotamiento de direcciones de red IPv4 y comenzó a buscar un reemplazo para este protocolo. Esta actividad produjo el desarrollo de lo que hoy se conoce como IPv6.

Una de las claves del éxito de los protocolos ipv6 de internet reside en el hecho de que el modelo propuesto es independiente de las capas físicas y de conexión de datos (capas 1 y 2 del modelo OSI).

IPv6 no es meramente un nuevo protocolo de Capa 3: es un nuevo conjunto de aplicaciones de protocolo, diseñado con escalabilidad para permitir años de crecimiento de la internetwork, sin embargo, IPv6 se está implementando lentamente y en redes selectas. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, IPv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro.

2.1.2.1.4. Arquitectura de red

(Cisco Systems, 2014), arquitectura de red es el diseño de una red de comunicaciones. Es un marco para la especificación de los componentes físicos de una red y de su organización funcional y configuración, sus procedimientos y principios operacionales, así como los formatos de los datos utilizados en su funcionamiento, todo esto engloba el proceso de la conexión publica donde se puede tener todo el acceso a la red más grande.

La red de redes es Internet, es conocida así ya que se trata de un sistema descentralizado de redes de comunicación que conecta a todas las estructuras de redes de ordenadores del mundo. World Wide Web, este es tan solo uno de los muchos servicios que ofrece Internet

Actualmente las empresas están sujetas a grandes cambios escalables, pero con un solo objetivo: conservar la estructuración de la red corporativa. Si bien los protocolos y dispositivos de red son más rápidos, más potentes y más inteligentes, su estructura la retroalimentación y su operabilidad es la misma.

a) Tolerancia a fallas

(Cisco Systems, 2014), la confianza de que Internet está siempre disponible para millones de usuarios que confían en ella requiere de una arquitectura de red diseñada y creada con tolerancia a fallas.

Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla.

Se denominan rutas redundantes a múltiples enlaces entre el origen y el destino, ejemplo claro de esto es que al solicitar servicio de mensajería electrónica ruta principal falla y el mensaje no puede ser enviado, la red como tal debe garantizar que dicho mensaje puede ser enviado en forma instantánea por una ruta de respaldo diferente, siendo optima rápida y segura para los usuarios en cada extremo.

b) Escalabilidad

(Cisco Systems, 2014), una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica.

La Red como tal debe estar preparada para hacer la aceptación de nuevos usuarios es decir este debe de tener la posibilidad de aumentar en su tamaño sin que se produzcan daños, inestabilidad, fiabilidad e inseguridad en la red.

Hoy en día hay cantidad innumerables de dispositivos que se conectan a la red de internet, a cada día millones de usuarios se anexan al “internet de las cosas”, no obstante, la red debe estar preparada para aceptar estos usuarios sin tener alteraciones de servicio y rendimiento.

c) Calidad de servicio

(Cisco Systems, 2014), Internet actualmente proporciona un nivel aceptable de tolerancia a fallas y escalabilidad para sus usuarios. Pero las nuevas aplicaciones disponibles para los usuarios en internetworks crean expectativas mayores para la calidad de los servicios enviados. Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona.

La calidad de servicio debe estar sujeta a las prioridades que el usuario final le demande a la red, el streaming como mayor utilitario de la red por usar la multimedia es el que mayor prioridad posee por su consistencia en tiempo real, los servicios como sitios web y mensajería no poseen de gran demanda debido a su nivel de prioridad de servicio es baja.

En la actualidad el internet de las cosas está bajo el control de la calidad de servicio conocida como QoS, que se encarga de definir las prioridades de un servicio solicitado por el usuario en una red otorgada por determinado proveedor ISP (Proveedor de Servicios de Internet), en este caso: CLARO en sus dispositivos de enrutamiento, le da a la multimedia más prioridad de navegación y ancho de banda, mientras que la navegación a sitios y mensajería tomarían otro nivel prioritario más bajo la configuración del QoS.

d) Seguridad

(Cisco Systems, 2014), internet evolucionó de una internetwork de organizaciones gubernamentales y educativas estrechamente controlada a un medio ampliamente accesible para la transmisión de comunicaciones personales y empresariales como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan del uso de internetworks para intercambiar información empresarial crítica y confidencial exceden lo que puede enviar la arquitectura actual.

La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

La Seguridad de la Data, la información referente a cualquier ámbito de negocio o personal se ha vuelto de suma importancia, ya que al estar enlazado con una red que puede ser vulnerable a ciertos atacantes que pueden explotar el más mínimo fallo dentro de la estructura de dicha red, para extraer información relevante y privada. Debido a esto la carrera por la seguridad se basa no obstante en protocolos de seguridad sino también en dispositivos de hardware que complementen el monitoreo al acceso de la red de personas no autorizadas.

Basándonos en la carrera por la eficacia de la de seguridad y el complemento de la lógica de los protocolos y la estabilidad del hardware, es que se utilizan nuevos dispositivos que previenen amenazas como el “Minsa Concepción Palacios”, hace uso de contraseñas y tipos de encriptaciones apoyados de Firewalls que hacen más robusta y segura la red de datos.

2.1.2.1.5. Tipos de Redes

a) Red de Área Personal (Personal Área Network)

(Cisco Systems, 2014), el alcance de red más restringido en inglés se llama Personal Área Network (PAN). Centrada en el usuario, designa una interconexión de equipos informáticos en un espacio de una decena de metros en torno al usuario, el Personal Operating Space (POS).

Ésta puede extenderse a diez metros de proximidad entre los demás usuarios, es la red comúnmente más utilizada dado por el espacio que puede abarcar.

La mayoría de personas tienen su propia red PAN, con el simple hecho de contratar un servicio de conexión a internet. Cada Proveedor de Servicios de Internet, facilita un enrutador donde se puedan conectar una serie de equipos siempre y cuando estén al alcance establecido.

b) Redes de Área Local o LAN (Local Área Network)

(Cisco Systems, 2014), la Red de Área Local son redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo dispositivos periféricos, terminales y otros dispositivos que se encuentren en un mismo edificio u otras áreas limitadas.

Red LAN una red individual generalmente que cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región.

Para pequeñas y medianas empresas, la comunicación digital de datos, voz y video es esencial para la supervivencia. En consecuencia, una LAN con un diseño apropiado es un requisito fundamental para hacer negocios en el presente.

c) Red de área amplia o WAN (Wide Área Network)

(Cisco Systems, 2014), una red de área amplia (WAN), es la que abarca una gran área geográfica, con frecuencia un país o un continente con un conjunto de máquinas diseñado para programas (es decir, aplicaciones) de usuario.

De acuerdo al crecimiento de la población y a la necesidad de estar comunicados las redes han venido evolucionando y desarrollándose tanto en servicios como en tamaño, es así como surgen las redes de área amplia abarcando hasta la totalidad de países y continentes a nivel mundial.

A través de este tipo de conexiones es que se pueden llevar a cabo diversos servicios en línea a nivel mundial tales como: la banca net , y los servicios de multimedia que están presente en la mayoría de países y ciudades del mundo, entre otros.

d) Red Internet

(Cisco Systems, 2014), internet es una red de acceso público, compuesta por redes de computadoras interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma.

Internet es la red de redes, debido a su gran presencia y cobertura en casi todo el mundo gracias al sinfín de recursos que se pueden compartir de manera inalámbrica o inalámbrica.

Internet hoy en día está presente en casi la mayoría de negocios de Nicaragua, perfilados a los diferentes giros de negocios, debido a que pueden agilizar sus transacciones de manera segura y rápida así también brindar un continuo servicio las 24 horas los 365 días del año.

2.1.2.1.6. Otros tipos de redes

a) Intranet

(Cisco Systems, 2014), el término intranet se utiliza generalmente para referirse a una conexión privada de algunas LAN y WAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización u otros que tengan autorización.

En la arquitectura de las Intranets se dividen el cliente y el servidor. El software cliente puede ser cualquier computadora local (servidor web o PC), mientras que el software servidor se ejecuta en una Intranet anfitriona.

En SILAIS MATAGALPA todas las estaciones de trabajo figuran como clientes debido a la que la red central está ubicada en la ciudad de Managua.

b) Diferencia principal respecto a Internet

(ISO27000.es, 2016), lo que distingue una intranet de la Internet pública, es que las intranets son privadas, por lo que es imprescindible que la estación de trabajo utilice un determinado rango de direcciones privadas contraseñas y demás controles para los usuarios de la misma.

Para ingresar a la red de internet no hay que obtener algún permiso en especial hoy en día nada más que la suscripción y el permiso de determinada terminal, sin embargo, las intranets o redes internas son de uso exclusivo y se ven de manera forzosa a usar contraseñas para su debido uso.

En Nicaragua muchas instituciones de carácter gubernamentales utilizan este medio de trasmisión para hacer el envío y recepción de datos de manera confidencial y segura, un ejemplo de esto es: SILAIS - MATAGALPA.

c) VPN (Redes Virtuales Privadas)

(Cisco Systems, 2014)**,** define una red virtual como una red privada a través de una red pública (en este caso internet) que permite hacer uso de los servicios públicos y

a su vez compartir información confidencial a un grupo controlado de usuarios; remotamente se puede acceder a las terminales del otro extremo de la red como si se estuviese dentro de un mismo local, aunque lejos geográficamente.

La VPN, no es más que la autopista exclusiva el canal reservado para cada flujo de información privada que va a salir hacia su canal de transmisión internet.

Se hace uso de la red virtual en aquellos casos en que la empresa o institución amerita estar en constante comunicación entre sí y que no siempre sus trabajadores están dentro de las oficinas como lo es el caso de SILAIS - MATAGALPA en Nicaragua.

d) LAN Virtuales (VLAN)

(Cisco Systems, 2014), las VLAN son grupos de ordenadores relacionados lógicamente entre sí por un número de grupo (número de VLAN) y configurados por el administrador del conmutador, gracias al software de configuración, residente en el sistema operativo del conmutador.

Las redes virtuales son agrupadas por grupos separados dentro de una misma red, esta configuración es realizada dentro del Switch o un Router para brindar una mejor organización y seguridad de diferentes áreas dentro de una empresa.

En SILAIS MATAGALPA, no poseen VLAN’s por lo tanto la red no está segmentada, lo cual implica un gran riesgo de seguridad para los datos.

2.1.2.1.7. Topologías

(Cisco Systems, 2014), la topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías de red pueden verse en el nivel físico y el nivel lógico.

El término topología de red informática es la composición de equipos que están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y

elementos de hardware (adaptadores de red y otros equipos que garantizan que los datos viajen correctamente).

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico dentro de su topología o infraestructura.

a) Topología Física

(Cisco Systems, 2014), la topología física de una red hace referencia a la configuración de cables, computadoras y otros periféricos.

Se entiende como topología de red física a los dispositivos físicos que conforman una arquitectura o infraestructura de red física tales como: servidores de red, Routers, Switches, firewalls, y los puntos de acceso inalámbricos, que se encargan de procesar, transmitir, enrutar, segmentar, codificar, y difundir la información.

La amplia gama de nuevos dispositivos de red que se encargan de la plena labor de transmisión y encriptación de datos hoy en día avanza agigantadamente gracias a la necesidad de las empresas por su deseo de expansión y su rigor en el cuido de su preciada información, no obstante, por esto existen equipos físicos de última generación que cumplen determinados requisitos.

b) Topología Lógica

(Cisco Systems, 2014), una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La capa de enlace de datos "ve" la topología lógica de una red al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a medios utilizados.

Se entiende como topología de red lógica a la amplia gama de protocolos y estándares de red que están presentes en los dispositivos que conforman una infraestructura de red.

Los protocolos de red se estandarizan gracias a los constantes cambios y necesidades que se puedan presentar en los diferentes entornos y giros empresariales, y a los nuevos equipos de enrutamiento de última generación.

2.1.2.1.8. Tipos de topologías de redes según su Infraestructura

a) Bus o Canal

(Cisco Systems, 2014) , en la topología de Bus o Canal “todos los nodos están unidos por un único enlace común, además los módulos de comunicaciones están conectados (colgados) de un único medio de comunicación (bus) que recorre todas las estaciones.

Cada paquete de información que es enviada a través de la red debe recorrer cada uno de los hosts agregados a la red recibiendo y descartando la información recibida hasta encontrar su host destino.

Hoy en día son pocas las redes con topología de bus, pero podemos tomar como un ejemplo muy claro la señal de televisión por cable, la señal es retransmitida a todos los usuarios en un solo sentido.

b) Estrella

(Cisco Systems, 2014), todas las estaciones están unidas, mediante medios bidireccionales, a un módulo nodo central que efectúa funciones de conmutación. Es también de aplicación frecuente en redes muy centralizadas o en sistemas de control.

Conjunto de equipos conectados a través de medios con direcciones a un nodo principal.

El punto central reenvía todas las transmisiones recibidas de cualquier host conectado a él a todos los demás en la red. Estos puntos centrales permiten la transmisión de datos Full Dúplex, mediante la cual los datos viajan en ambos sentidos, es decir, se pueden enviar y recibir datos al mismo tiempo.

c) Árbol

(Cisco Systems, 2014) es una extensión de la arquitectura en estrella por interconexión de varias. Permite establecer una jerarquía clasificando a las estaciones en grupos y niveles según el nodo a que están conectadas y su distancia jerárquica al nodo central.

Las características similares a la red en estrella, reduce la longitud de los medios de comunicación incrementando el número de nodos. Se adapta a redes con grandes distancias geográficas y predominancia de tráfico, características más propias de una red pública de datos que de una red privada local.

El uso común de estas redes en empresas nacionales se debe al tamaño de sus instalaciones en expansión. Por lo cual hacen el uso de topologías o infraestructuras que tienden a desarrollarse con esta topología denominadas: árbol que son implementadas en grandes edificios por la magnitud de su crecimiento.

d) Anillo

(Cisco Systems, 2014) , los nodos están unidos en cadena, uno tras otro, cerrándose ésta sobre si misma (de un único nodo raíz).

El flujo de información pasa por todos los equipos y se envían de manera única los paquetes destinados.

Para prevenir la caída de la red se utiliza topología anillo para tener un medio de emergencia o ruta de protección ante cualquier eventualidad.

e) Mixta

(Cisco Systems, 2014), la topología mixta es una topología de red una mezcla entre alguna de las otras topologías: bus, estrella o anillo.

La topología mixta es donde las redes pueden utilizar diversas conexiones para conectarse. Esta es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red.

Las redes mixtas son difíciles de configurar, dependiendo de la complejidad de las redes a combinar.

2.1.2.1.9. Diseño de Redes

a) Diseño de Red Lógica

(Cisco Systems, 2014) , las redes están organizadas en 3 configuraciones lógicas: enlace punto a punto, enlace punto a multipunto, enlace multipunto a multipunto.

Las redes se organizan en configuraciones lógicas: nodo a nodo, nodo a múltiples nodos o múltiples nodos a múltiples nodos. Las empresas a nivel mundial organizan sus equipos según el diseño más factible para que sus clientes accedan a la red.

- **Enlaces punto a punto**

(Cisco Systems, 2014), los enlaces punto a punto generalmente se usan para conectarse a internet donde dicho acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a internet.

Es la forma de conectarse a internet a través de un punto de acceso común como una caja modular con un Jack Rj-45.

Actualmente en nuestra ciudad existen instituciones que utilizan este tipo de conexión punto a punto con el proveedor de servicio de internet a través de un radio enlace inalámbrico.

- **Enlaces punto a multipunto**

CISCO CCNA (2014), la siguiente red: punto a multipunto es donde varios nodos están hablando con un punto de acceso central, esta es una aplicación punto a multipunto.

Los enlaces punto a multipunto son comunes y su conexión está basada en un punto central comunicando con el resto de puntos de manera remota o periférica.

La conexión de punto a multipunto es la que está siendo utilizada por el plan de gobierno de parques wifi, existentes en las cabeceras departamentales de todo el país de Nicaragua que utilizan dispositivos Cisco denominado Meraki.

- **Enlaces multipunto a multipunto**

(Cisco Systems, 2014), en una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

Enlace multipunto a multipunto es la comunicación directamente entre todos los nodos sin jerarquía superior sin que estos tengan que acceder a toda la red en sí para transmitir.

Este tipo de enlace es conocido por el que más competencia propone por enviar un mensaje, dentro de sus terminales asociadas hace un recuento continuo que debe de ordenar el orden de cada mensaje destino hacia un posible receptor**.**

2.1.2.1.10. Elementos de una red

a) Mensajes

(Cisco Systems, 2014), en la primera etapa del viaje desde la computadora al destino, el mensaje instantáneo se convierte en un formato que puede transmitirse en la red. Todos los tipos de mensajes tienen que ser convertidos a bits, señales digitales codificadas en binario, antes de ser enviados a sus destinos. Esto es así sin importar el formato del mensaje original: texto, video, voz o datos informáticos. una vez que

el mensaje instantáneo se convierte en bits, está listo para ser enviado a la red para su remisión.

Lo solicitado por el usuario es un comando que la computadora ejecuta como una petición que puede variar ya sea esta: una solicitud de salir a internet abrir una página web, llamadas telefónicas, videollamadas, documentos, entre otros, sin importar lo que sea estos se transmiten en la red, siendo estas peticiones transformadas en un lenguaje propio para la computadora con el debido tamaño adecuado para que este viaje dentro de la red y poder así brindar respuesta.
Un simple correo electrónico es algo sencillo de ser enviado en nuestros días gracias que el proceso complejo es realizado por la computadora, esta recibe la solicitud y se encarga de convertirla a su propio lenguaje binario para entender la necesidad del usuario y así completar la petición del usuario.

b) Dispositivos

(Cisco Systems, 2014),cuando pensamos en utilizar servicios de red, generalmente pensamos en utilizar una computadora para acceder a ellos. Pero una computadora es sólo un tipo de dispositivo que puede enviar y recibir mensajes por una red. Muchos otros tipos de dispositivos pueden conectarse a la red para participar en servicios de red. Entre esos dispositivos se encuentran teléfonos, cámaras, sistemas de música, impresoras y consolas de juegos.

Además de la computadora, hay muchos otros dispositivos por los cuales la información o los mensajes peticiones que el usuario le solicita y estos pueden viajar grandes distancias geográficas ciudades incluso países y continentes gracias a cables subterráneos, ondas aéreas y estaciones de satélites que puedan existir entre los dispositivos de origen y de destino.

El dispositivo clave aparte de la computadora es el Router ya que se encarga de enrutar por el mejor camino conocido en su tabla de enrutamiento y direccionar las peticiones del usuario y sin importar el dispositivo y asegurar que el mensaje llegue al destino de la manera más rápida y eficaz, un sinnúmero de estos dispositivos

programados son los que existen en diferentes empresas, como en SILAIS-MATAGALPA.

c) Medio de transmisión

(Cisco Systems, 2014), enviar el mensaje instantáneo al destino, la computadora debe estar conectada a una red local inalámbrica o con cables. Las redes locales pueden instalarse en casas o empresas, donde permiten a computadoras y otros dispositivos compartir información y utilizar una conexión común a Internet.

Los datos pueden viajar desde redes cableadas a redes inalámbricas, sin importar el medio, pero las cableadas permiten velocidades de transferencias más altas y más seguras que las inalámbricas.

En la actualidad la mayoría de hogares y empresas cuentan con conexión de red inalámbrica o cableada, que les asigna su ISP, sin importar el medio los servicios requeridos por el usuario se obtienen con igual manera, no obstante la latencia de la red está basada en los estándares de calidad que presenta un medio guiado y uno no guiado, es decir la señal es mucho mejor cuando el medio es guiado “cableado” que un medio no “guiado” inalámbrico, debido a muchos factores, de ubicación, estructuración, ancho de banda e incluso ambiental.

d) Reglas

(Cisco Systems, 2014), menciona que las reglas son las normas o protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino. Por ejemplo: en el caso de la mensajería instantánea, los protocolos XMPP, TCP e IP son importantes porque son conjuntos de reglas que permiten que se realice la comunicación.

Lo que significa que el ordenador conectado a la red usa protocolos para permitir que los ordenadores conectados puedan enviar y recibir datos, por ejemplo, dos computadores conectados en la misma red, pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo

idioma. En sí son un conjunto de reglas que utilizan los ordenadores para comunicarse entre sí.

Hoy en día gracias a la estandarización de reglas o protocolos, es posible que dispositivos totalmente distintos pueda comunicarse de igual manera. Esto es debido a que los protocolos especifican la funcionalidad de la red y no la tecnología de los dispositivos. Para que lo entiendas mejor, el protocolo HTTP no especifica qué sistema operativo se debe utilizar, ni que lenguaje de programación, ni los requisitos del explorador web, pero sí nos dice que hacer cuando ocurre un error al servir la información trasmitida por el servidor web.

2.1.2.1.11. Diseño de Red Física

a) Dispositivos de red

- **Enrutador (Router)**

(Cisco Systems, 2014), el Router o enrutador es un periférico de comunicaciones empleado para enlazar diferentes redes entre sí al igual que el Switch, el Router se conecta al equipo a través del puerto RJ-45 (Ethernet) y en determinados modelos, por puerto serie para entrar en modo consola.

A través de este dispositivo se pueden enrutar muchas redes, a la vez aplicar diferentes configuraciones de protocolos, seguridad y direccionamientos.

Al implementar una red de acceso a internet es parte fundamental la instalación de un enrutador, este es el punto de conexión entre el internet y la red privada del usuario. De igual manera puede ser utilizado dentro de una red privada para el direccionamiento de subredes.

- **Conmutador (Switch)**

(Cisco Systems, 2014), este dispositivo es el responsable de analizar la información que recibe de cada uno de los terminales de la red y encaminarla a su destino correspondiente. Digamos que es como una central de comunicación de datos.

Todos los datos paquetes enviados desde cada uno de los dispositivos primeramente pasan por el Switch es ahí donde se determina hacia donde será su destino, si pertenece a la misma red o salir hacia internet.

Para implementar una red inalámbrica o cableada se debe de tomar en cuenta el tipo de Switch a instalar debido al tamaño y complejidad que la red puede alcanzar.

- **Punto de Acceso o Access Point (AP)**

(Cisco Systems, 2014), el punto de acceso no sólo es el medio de intercomunicación de todos los terminales que forman la red, sino que también es el puente de interconexión de la red fija e internet.

Un AP puede tener una distancia determinada para brindar acceso a los usuarios, podemos tener acceso a él, sólo y únicamente a través de dispositivos inalámbricos.

La instalación de un AP solamente se utiliza en lugares donde necesitamos tener acceso inalámbrico, si bien vemos estos tienen la misma función de un Switch, la cantidad de AP instalados en una red será variable de acuerdo a la amplitud del local o lugar.

2.1.2.1.12. Medios de transmisión cableados o guiados

a) Cable de par trenzado

(Cisco Systems, 2014), éste consiste en dos alambres de cobres aislados, por lo general de 1 mm de grueso los alambres se trenzan en forma helicoidal, igual que una molécula de DNA, cuando se trenzan los alambres, las ondas de diferentes vueltas se cancelan, por lo que la radiación del cable es menos efectiva.

Sus categorías son:

- ✓ **Categoría 3:** soporta velocidades de transmisión hasta 10 Mbits/seg. Utilizado para telefonía de voz, 10Base-T Ethernet y Token ring a 4 Mbits/seg.

- ✓ **Categoría 4:** soporta velocidades hasta 16 Mbits/seg. Es aceptado para Token Ring a 16 Mbits/seg.
- ✓ **Categoría 5:** hasta 100 Mbits/seg.Utilizado para Ethernet100Base-TX.
- ✓ **Categoría 5e:** hasta 622 Mbits/seg. Utilizado para GigabitEthernet.
- ✓ **Categoría 6:** soporta velocidades hasta 1000 Mbits/seg.

El par trenzado es uno de los tipos de cables de pares compuesto por hilos, normalmente de cobre, trenzados entre sí. El trenzado mantiene estable las propiedades eléctricas a lo largo de toda la longitud del cable y reduce las interferencias creadas por los hilos adyacentes en los cables compuestos por varios pares.

Actualmente en Nicaragua, es el cable más utilizado en la mayoría de infraestructuras de redes LAN, estas se encuentran comúnmente en entornos de trabajo como: Universidades, Bancos, Supermercados y edificios Corporativos debido a los altos estándares de velocidad seguridad y rendimiento que estos medios de transmisión poseen.

b) **Cable coaxial**

(Cisco Systems, 2014), el cable coaxial transporta señales eléctricas de alta frecuencia, tiene dos conductores concéntricos: uno de cobre rígido (o hilos trenzados) que lleva la información, y otro exterior en forma de malla trenzada (o tubo de cobre o aluminio) que sirve de referencia de tierra y retorno de corriente. Ambos están cubiertos con una capa de aislante de tipo eléctrico.

El cable coaxial está conformado por materiales como cobre rígido grueso, rodeado por un aislante, y una malla conductiva de tejido fuertemente trenzado.

En nuestro país las telecomunicaciones que brindan los proveedores de servicios de internet como las empresas: Claro, Telecable y Movistar hacen uso de este medio para la transmisión analógica de la televisión por cable en nuestros hogares, además de poder proporcionar servicios de internet por el mismo medio.

c) Cable de fibra óptica

(Cisco Systems, 2014), es un medio de transmisión guiado que consiste en un cable de hilo muy fino (como un cabello) y flexible, de material transparente, ya sea vidrio (óxido de silicio y germanio) o plástico. Por dicho hilo se envían pulsos de luz con una fuente que puede ser un láser o un light-emitting diode, diodo emisor de luz (LED).

La fibra óptica consiste en un núcleo central de vidrio con un índice alto de refracción y con un revestimiento de vidrio, para acelerar la transmisión de datos.

En Nicaragua solo las instituciones de bienes bancarios y corporativos pueden optar a hacer uso de este tipo cable debido a sus altos costos, de operación.

2.1.2.1.13. Medio de transmisión inalámbrica

a) Ondas de radio

(Cisco Systems, 2014), son ondas omnidireccionales, es decir, emiten y reciben en los 360 grados, por lo que son necesarias antenas parabólicas. La frecuencia de estas ondas oscila entre los 3 Hz y los 3,000 MHz. Entre las ventajas está el que

las ondas de radio se caracterizan por ser electromagnéticas de radiofrecuencia (RF) que transportan información de un punto a otro punto sin límites de distancia

En Nicaragua un ejemplo claro de este tipo de tecnología, es utilizada por las empresas de seguridad y las empresas radiales, que se comunican por medio de estaciones de radios o walkies talkies.

b) Wifi

(Cisco Systems, 2014), que son un conjunto de especiaciones basadas en el estándar IEEE 802.11 que actúan en la capa física y de enlace del modelo OSI. Sus versiones 802.11b (hasta 11 Mbps) y 802.11g (hasta 54 Mbps en modo normal y 108 Mbps con técnicas de aceleración) disfrutan de una aceptación universal, debido a que trabajan en la banda 2.4 GHz, disponible casi universalmente.

Es un tipo de red que por sus características no requiere de medios guiados ya que funcionan en base a protocolos previamente establecidos en dispositivos electrónicos.

La mayoría de dispositivos utilizados hoy en día utilizan la tecnología WIFI para conectarse y salir a Internet, no obstante, en SILAIS MATAGALPA no utiliza esta tecnología.

2.1.2.1.14. Infraestructura de red Lógica

a) Servidor

(Cisco Systems, 2014), es el equipo que brinda servicios a los clientes. Los servidores son el punto central de las redes modelo cliente/servidor. Existen muchos servicios que un servidor puede brindar a los clientes de red. Por ejemplo, DNS, DHCP, almacenamiento de archivos, alojamiento de sitios web, entre otros.

El servidor además de ser un dispositivo de hardware también es una unidad lógica e informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red.

En la institución SILAIS-MATAGALPA, existe un servidor físico que se encarga del sistema financiero de gastos y operaciones en curso.

b) Direccionamiento IP

(Cisco Systems, 2014), para identificar un dispositivo dentro de una red es necesario que tenga un identificador único que lo diferencie en todo momento de otro dispositivo, y así de ser tratados como dispositivos de una misma Red de Área Local, independiente de otras redes.

La dirección IP es un protocolo lógico único e irrepetible que se le asigna a cada dispositivo que solicite una conexión a la red.

En SILAIS-MATAGALPA, las direcciones IP se asignan de manera estática para obtener el mejor control de segregación de la red.

c) Direcciones privadas

(Cisco Systems, 2014), es una dirección usada para redes internas, esta dirección obedece el direccionamiento RFC 1918. No son enrutables en internet.

Los bloques de direcciones privadas son:

1) 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
2) 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
3) 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

Las direcciones IP privadas son las que se usan generalmente en una intranet.

SILAIS MATAGALPA hace uso de estas direcciones privadas debido a que cuenta con una intranet que no entra a internet.

d) Direcciones públicas

(Cisco Systems, 2014), las direcciones públicas son asignadas por Internet Network Information Center (InterNic) y están compuestas por id de red basados en clase o bloque de direcciones basadas en CIDR que son universalmente únicas para internet.

Las direcciones IP públicas son asignadas por nuestro ISP, (Proveedor de Servicios de Internet), esta dirección IP es única para internet y se tendrá mientras se pague el servicio de internet, de lo contrario esta se le asigna a otro cliente.

En la actualidad las direcciones públicas solo son otorgadas por las empresas como claro en nuestro país, y estas se asignan en base a la necesidad que requiera el cliente en cuanto a cantidad de dispositivos.

2.1.2.1.15. Concepto de Protocolo de Red

Los protocolos de Red son reglas de comunicación que permiten controlar el flujo de la información entre computadoras que operan distintos sistemas operativos y bajo dispositivos de distintos fabricantes.

Dos computadores conectados en la misma red, pero con protocolos diferentes no podrían comunicarse, al igual que dos personas que hablen idiomas diferentes no podrían hacerlo sin antes tener conocimiento de cómo hacerlo este es el fin de los protocolos de red establecer la comunicación de dos o más computadoras a través de normas establecidas.

Los protocolos de Red Pueden estar implementados bien en hardware (tarjetas de red), software (drivers), o una combinación de ambos.

a) DHCP (Dynamic Host Configuration Protocol)

(Cisco Systems, 2014), el Protocolo de Configuración Dinámica de Anfitrión o DHCP (siglas en inglés) es un protocolo de red TCP/IP que permite a los nodos de una red obtener sus parámetros de configuración automáticamente.

El servidor DHCP asigna direcciones IP automáticamente, al dispositivo que se conecte a la red, en un rango de especificado por los administradores de la red.

Hoy en día en universidades, empresas, colegios, parques están optando por este servicio, otorgando direcciones IP automáticamente a los dispositivos que se conectan a él, evitando el trabajo tedioso de agregar manualmente las direcciones IP estáticas a los dispositivos que solicitan del servicio de navegación.

b) DNS (Domain Name System)

(Cisco Systems, 2014), DNS es un servicio cliente/servidor; sin embargo, difiere de los otros servicios cliente/servidor que estamos examinando. Mientras otros servicios utilizan un cliente que es una aplicación (como un explorador Web o un cliente de correo electrónico), el cliente DNS ejecuta un servicio por sí mismo. El cliente DNS,

a veces denominado resolución DNS, admite resolución de nombre para otras aplicaciones de red y servicios que lo necesiten.

Otro de los servicios en red llamado DNS, sirve para transformar la IP de un servidor web en un nombre de dominio.

En SILAIS-MATAGALPA, el DNS se encarga de traducir los nombres de dominios internos, de la red MINSA, por ejemplo, la traducción del dominio de la página web (WWW.MINSA.GOB.NI).

***c)* FTP (File Transfer Protocol)**

(Cisco Systems, 2014), el protocolo de transferencia de archivos (FTP) es otro protocolo de la capa de aplicación comúnmente utilizado. El FTP se desarrolló para permitir las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora y se utiliza para cargar y descargar archivos desde un servidor que ejecuta el daemon FTP (FTPd). FTP es un servicio remoto que nos permite subir archivos, descargar, usando la arquitectura de cliente servidor.

Para transferir los archivos en forma exitosa, el FTP requiere de dos conexiones entre cliente y servidor: una para comandos y respuestas, otra para la transferencia real de archivos.

SILAIS-MATAGALPA, posee carpetas compartidas en el servidor remoto que está ubicado en Managua , lo cual permite acceder por medio de este protocolo para la agilización de trasferencia de cualquier archivo.

***d)* Voz IP**

(Cisco Systems, 2014), cisco, voz sobre ip o también conocido como VoIP (Voice Over Internet Protocol) es un servicio que permite transmitir voz usando el protocolo IP. En concreto se refiere a la capacidad de transmitir voz a través de Internet. Pero no se trata de una radio por internet, sino algo más complejo.

Voz sobre IP, utiliza la red sus principios la red y protocolos para ejercer llamadas de voz.

SILAIS - MATAGALPA opto por la telefonía IP, bajando el costo de la telefonía en cuanto a llamadas de larga duración en todo el país.

***e)* Servicio de correo electrónico**

(Cisco Systems, 2014), el correo electrónico es un método de almacenamiento y envió para redactar, enviar, almacenar, y recibir mensajes por sistemas de comunicación electrónica.

El servicio de correo electrónico, es una plataforma de mensajería que alterna las cadenas de texto con la multimedia para agilizar el proceso de comunicación en una Institución.

SILAIS-MATAGALPA, está asociado a un servidor remoto de correo electrónico en su Data Center Central (MINSA-MANAGUA), para aprovechar los beneficios que presta este tipo de plataforma comunicativa.

- **SMTP**

(Cisco Systems, 2014), el protocolo para transferencia simple de correo (en inglés Simple Mail Transfer Protocol o SMTP), es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, entre otros).

El protocolo SMTP es el encargado regir cómo será él envió de un mensaje de correo electrónico que viaja en la red.

SILAIS-MATAGALPA, trabaja con el protocolo SMTP en el gestor de correos internos como norma para garantizar él envió de sus mensajes.

- **POP3**

(Cisco Systems, 2014), en informática se utiliza el Post Office Protocol (POP3, Protocolo de Oficina de Correo o "Protocolo de Oficina Postal") en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado Servidor POP. Es un protocolo de nivel de aplicación en el Modelo OSI.

El protocolo POP3 es el encargado regir cómo será la recepción un mensaje de correo electrónico que viaja en la red.

SILAIS-MATAGALPA, trabaja con el protocolo POP3 en el gestor de correos internos como norma para garantizar la recepción de sus mensajes.

***f)* Ancho de banda**

(Cisco Systems, 2014), es la cantidad de datos que se puede trasmitir en una cantidad de tiempo, hacia o desde el sitio web a través de un tiempo previamente determinado o bien la cantidad de datos que pueden enviarse y recibirse en el marco de una comunicación

El ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.
Hoy en día los proveedores de servicio de Internet en Nicaragua ofrecen diferentes anchos de banda desde 512 kbps hasta 100 Mbps, para mejorar la comunicación entre los usuarios de empresas y usuarios comunes que se conectan a la red.

2.1.2.1.16. Calidad de las Comunicaciones

(Cisco Systems, 2014), la tecnología de Red es flexible y fácil de utilizar, pero no hay que olvidar que tienen un alcance limitado así lo explica.

Desde que surgen las redes se han implementado una serie de protocolos y mejoras, todo con el fin de disminuir las diferentes dificultades al utilizar esta tecnología que hoy en día se ha convertido en una de las más utilizadas e implementadas en la mayoría de dispositivos electrónicos.

Una red local es muy vulnerable a interrupciones por motivos físicos, como lógicos, un ejemplo es la red LAN en SILAIS-MATAGALPA, donde los dispositivos están expuestos a manipulaciones lógicas y físicas, por falta de políticas de seguridad que minimicen este riesgo.

a) Distancia

(Cisco Systems, 2014), el hardware de red básico tiene un alcance teórico de 30 metros en interior y de 100 metros en exterior. En la práctica hay que contar más bien con un alcance de 10 a 15 metros interior,

La distancia de alcance de una red inalámbrica siempre va a depender de la cantidad de obstáculos que se encuentren sea en interior o exterior.

Este factor se debe tomar en cuenta cuando se está instalando una red diseñando de manera que cada dispositivo alcance su máximo alcance, ubicándolo en lugares estratégicos y seguros.

b) Obstáculos

(Cisco Systems, 2014), si quita los potenciales obstáculos y fuentes de interferencia, la mayoría de dispositivos de red pueden alcanzar distancias de casi el doble de lo que puede esperar adentro.

Cada obstáculo que interviene en una red provoca pérdidas de señal entre el punto de acceso y los dispositivos que se conecten a él. Por tal razón se debe de instalar la cantidad de puntos de accesos necesarios para cubrir por completo cada área que conforma esta red.

Dificultosamente se logra eliminar por completo los impedimentos en una red, solo podemos tratar de minimizar ciertas ubicaciones en donde los dispositivos se vean comprometidos a cumplir sus funciones.

c) Seguridad

(Cisco Systems, 2014), su punto de acceso puede ser de unos pocos cientos de metros, un usuario con una antena de gran ganancia puede ser capaz de hacer uso, aunque esté a varias manzanas de distancia la información en la red no está al 100% por ciento segura en ningún momento y lugar.

La información puede ser interceptada por cualquier individuo con intención de realizar daños a la red utilizando herramientas diseñadas para realizar ataques y poner en peligro la información personal o privada de cada usuario o de la institución a la que pertenece la red.

Esta es la razón por la que cada empresa debe adoptar medidas de seguridad que protejan y garanticen la confiabilidad y la disponibilidad de la red.

2.1.2.2. ISO/IEC 27002:2013

(ISO, ISO/IEC 27002:2013 , 2014), se refiere a una serie de aspectos sobre la seguridad de las tecnologías de información. Es el estándar Internacional orientado a la seguridad de la información en las empresas u organizaciones las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

La ISO/IEC 27002:2013, establece una guía de pasos a seguir para brindar buenas prácticas a la seguridad de la información, para su integridad.

No obstante ISO/IEC 27002:2013 aporta controles y técnicas que permiten a las empresas emplear buenas prácticas para proteger su información de una manera íntegra.

2.1.2.2.1. **Concepto**

(ISO, 2013) es una guía de buenas prácticas que describe cuáles deben de ser los objetivos de control que se deben aplicar sobre la seguridad de la información. No es certificable. En total la norma contiene 35 objetivos de control y 114 controles los cuales están agrupados en 14 dominios.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

(ISO27000, 2019), fuente: Adaptada

La ISO/IEC 27002:2013 no es para fines de certificación, esta ofrece una muy buena guía para la gestión de la seguridad de la información de determinadas empresas, permitiéndole adoptar buenas prácticas que ayuden a mantener la integridad y disponibilidad de la misma.

Al presente ISO/IEC 27002:2013 no es una guía que permita certificar una empresa, sino que otorga una serie de dominios y controles que permiten aplicar buenas prácticas para la seguridad de la información.

2.1.2.2.2. Controles de la normativa ISO 27002/2013

(ISO, 2013) , control consiste en el cálculo y corrección del trabajo, con la finalidad de asegurarse de que se cumplan los objetivos de determinadas empresas y sus planes para lograrlo".

Controles, se establecen para las inspecciones de ciertas finalidades en un determinado lugar, para brindar resultados esperados.

Se adjudica, son los que se establecen para medir los resultados esperados por medio de cálculos y correcciones dentro de una empresa.

a) Políticas de Seguridad

(Gupta, 2012), un documento denominado "política" es aquel que expresa una intención e instrucción global en la manera que formalmente ha sido expresada por la dirección de la organización.

Política de seguridad, es un documento del más alto nivel que denota los compromisos de la gerencia, con la seguridad y la integridad de la información.
En Nicaragua, las diferentes instituciones públicas y privadas prefieren este tipo de normas y documentos que les permiten alcanzar objetivos, de acuerdo a necesidades.

- **Directrices de la dirección en seguridad de la información**

(Gupta, 2012), la gerencia debería establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la organización.

Los objetivos de toda institución deben de estar unidos al más alto nivel, con el fin de que estas políticas se comuniquen a todas las áreas de la institución, basándose en los principios de autenticidad confidencialidad, integridad y disponibilidad.

Actualmente las diferentes instituciones restituyen de manera habitual las políticas de seguridad, para mitigar los riesgos de la información.

b) **Aspectos organizativos de la seguridad de la información**

(Pritesh, 2012), el objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.

Las empresas deben definir muy explícitamente su rol de cometidos para efectuar tareas tales como la aprobación de políticas de seguridad desde el más alto nivel organizativo, todo esto en plena coordinación y comunicación, su implementación debe de estar dentro del marco de la seguridad, la delegación de funciones y responsabilidades a cada miembro activo.

Todas las organizaciones con fines prósperos muy bien definidos, toman en cuenta y muy seriamente los aspectos enfocados a la organización y delegación de funciones desde el más alto nivel.

- **Organización interna**

(Gupta, 2012), la gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

Todas las empresas con visión y misión, deben de inquietarse por establecer y mantener políticas de seguridad de la información provenientes desde la alta gerencia.

En nuestros días todas las organizaciones, sin importar su giro laboral cuentan con políticas de seguridad, debido a que la información es lo más preciado para la continuidad del trabajo.

- **Segregación de tareas**

(Gupta, 2012), se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.

Las instituciones asignan tareas y responsabilidades a cada área de trabajo, con el fin de poder controlar la información de manera más detallada y eficiente, brindando así un mayor nivel de seguridad

Las instituciones están trabajando para minimizar la dependencia, gracias a que se asignan roles a las personas en las diferentes áreas de trabajo.

- **Seguridad ligada a los recursos humanos**

(Gupta, 2012), el objetivo del presente dominio es la necesidad de informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad y asuntos de confidencialidad. Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no

autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Las empresas están en el deber de explicar funciones en materia de la seguridad de la información, en la etapa de contratación, para garantizar que el personal atienda las normas establecidas, y cuáles son los componentes de seguridad por los cuales atraviesa la información y las responsabilidades que esta conlleva.

Actualmente en Nicaragua las instituciones ejercitan planes de capacitación a todo su personal, sea este nuevo ingreso o personal que ya es residente, para reducir el peligro de la integridad de la información.

c) Gestión de activos

(Gupta, 2012), el objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Toda institución clasifica su información, de acuerdo al grado de sensibilidad que esta genere, con el fin de manifestar las medidas para el debido procesamiento y protección de la información.

Las instituciones gestionan sus activos con diferentes metodologías para la minimizar los riesgos.

- **Responsabilidad sobre los activos**

(Gupta, 2012), todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados.

El empleado goza del término “propietario” identificándolo como responsable, es decir que cuenta con la aprobación de la dirección, para el control uso y seguridad de dicho

activo. Mas sin embargo el término “propietario” no significa que la persona disponga de los derechos de propiedad reales del activo.

En la actualidad las instituciones usan diferentes métodos para tener el control de activos otorgados al empleado, estos pueden ser leyendas de códigos, o números de series que ayuden en las tareas de realización de inventario y para vincular equipos de TI con empleados.

Inventario de activos

(Gupta, 2012), todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los datos más importantes.

Todas las herramientas TIC’s, conocidas como recursos computacionales deben de ser y estar claramente identificados en un inventario para conocer su existencia real forma regulada.

Las instituciones al día de hoy, validan el inventario de equipos computacionales muy importante, para estar al tanto con cuantos recursos se cuentan, esto debido a la información detallada de los inventarios.

Uso aceptable de los activos

(Gupta, 2012), se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

Es la normativa la cual regula el uso correcto de cada activo que posee la institución, esto con el fin de proteger el bienestar de los activos y la calidad de la información.

En este momento las instituciones supervisan la correcta práctica de activos, en base a esto pueden administrar de forma correcta sus recursos.

Manejo de los soportes de almacenamiento

(Gupta, 2012), los medios deberían ser controlados y físicamente protegidos. Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

La misión es impedir la destrucción de activos computacionales no autorizada, y que cuenten con información aun almacenada en sus unidades.

Hoy en día las instituciones excluyen equipos de cómputo con información alojada en sus unidades de almacenamiento, eliminando información oportuna que puede ser necesitada y reutilizada.

d) Control de accesos

(Gupta, 2012), el objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

La data debe de estar protegida mediante técnicas de control que permitan mantener la entereza de los datos y evitar la intromisión de ajenos y que esta sea manipulada de forma no autorizada.

Actualmente las instituciones ostentan medidas que restringen el acceso de personas ajenas a la información, con el fin de mantener la integridad de la información.

- **Requisitos de negocio para el control de accesos**

(Gupta, 2012), se deberían controlar los accesos la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la organización.

La misión esencial es vigilar los accesos, a las áreas donde se dé el procesamiento de la información.

En la actualidad las empresas usan diferentes tipos de cifrados en las áreas de cómputo, para evitar que personas ajenas del área o de la empresa en sí, puedan ingresar.

Política de control de acceso

(Gupta, 2012), se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

Las políticas de control se deben de instaurar con el único fin de ofrecer soluciones a las necesidades de la seguridad de los datos.

A la fecha todas las instituciones establecen sus propias políticas de seguridad, en base a las necesidades de seguridad presentadas.

Control de acceso a las redes y servicios asociados

(Gupta, 2012), se debería proveer a los usuarios los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

La vigilancia de acceso a las redes de datos tiene como finalidad asegurar que a los usuarios que se conectan a dicha red.

En la actualidad las instituciones, proveen agregación de importancia a las redes de datos debido al crecimiento de estas, ya que cada vez estas son escalables, y no centralizadas.

- **Gestión de acceso de usuarios**

(Gupta, 2012), se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Las programaciones para el acceso a los sistemas de información y sus diferentes servicios, deben de estar controlados.

Al presente las empresas utilizan control de cuentas de usuarios para supervisar accesos y manipulaciones a los sistemas, mediante privilegios de usuarios.

- **Gestión de altas/bajas en el registro de usuarios**

(Gupta, 2012), debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

Se debe de implementar una política de seguridad la cual especifique que usuario se debe de dar de baja en los sistemas dentro de la institución, y dar de alta a todos aquellos usuarios que estén activos y deban poseer privilegios de acceso a los sistemas.

Hoy en día las instituciones deben de controlar a los usuarios que son dados de baja de los sistemas, implementando procedimientos de inspección, que les permita controlar el acceso a la información, por parte de los usuarios activos y autorizados.

e) Cifrado

(Gupta, 2012), el objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

La criptografía o cifrado de la información es sin duda el elemento más importante de la seguridad de la información, ya que permite protegerla para que esta no sea alterada o eliminada de ninguna manera y que pueda viajar dentro de la red de forma íntegra y segura.

Actualmente las instituciones establecen diferentes tipos de cifrados en la transmisión de su información, con el fin de mitigar riegos que transgredan la integridad de esta.

- **Controles criptográficos**

(Gupta, 2012), controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

El fin de los controles criptográficos es certificar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Actualmente algunas organizaciones utilizan protocolos y controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información.

f) Políticas de uso de controles criptográficos

(Gupta, 2012), se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.

Por medio de las políticas de seguridad de la información, se establece el uso de cifrado de la información permitiendo así la administración de este tipo de controles más organizadamente.

Presentemente en la mayoría de instituciones se establecen políticas de seguridad, el uso del cifrado se da gracias a túneles virtuales que protegen el tráfico de datos dentro de la red, más sin embargo hay muchos más métodos de seguridad.

g) Seguridad física y ambiental

(Gupta, 2012), el objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

Es necesario que existan normas y políticas que permitan minimizar eventualidades que tengan que ver con riesgos enlazados a la seguridad física y con el medio

ambiente, evitando así que los medios físicos que almacenan información se estropeen, ya sea por factores humanos o factores ambientales.

Al día de hoy las instituciones implementan políticas que les permiten proteger la información por afectaciones ambientales de cualquier índole, también por afectaciones humanas, de manera directa o indirecta, esto les permite estar preparados ante cualquier eventualidad y propagar la continuidad de servicio.

- **Áreas seguras**

(Gupta, 2012), las áreas seguras deben de evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial deberían ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.

Las estaciones de procesamiento de información como servidores y demás activos deben estar físicamente protegidos del acceso no autorizado, daños e interferencia. El principal objetivo de las áreas seguras denegar el acceso físico no autorizado a personas ajenas a la institución

.

En nuestros días algunas organizaciones salvaguardan la información y sus activos tecnológicos, con medios e instalaciones secundarias para mitigar desastres de carácter ambiental, o daños que puedan ser ocasionados el mismo humano.

- **Controles físicos de entrada**

(Gupta, 2012), las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.

Debe de existir una bitácora que posea el control estricto a las ubicaciones de los medios físicos tecnológicos que contienen la información, garantizando así que

únicamente el personal autorizado pueda ingresar a áreas en donde se opera la información.

Actualmente las organizaciones poseen controles estrictos para regular el acceso físico por personas no autorizadas a las instalaciones y a las diferentes áreas que poseen estaciones computacionales con acceso a los sistemas.

- **Protección Contra Amenazas Externas y Ambientales**

(Gupta, 2012), se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

Las instituciones deben de contar con políticas de seguridad que permitan minimizar los riesgos contra desastres naturales y ataques desde fuera de la red, mediante virus o códigos maliciosos, que atenten contra la integridad de los datos.

Actualmente las organizaciones cuentan con medidas de seguridad y planes de contingencia, que les permitan mitigar riesgos y tomar decisiones cuando se presentan algún evento con índole ambiental, así también medidas de seguridad que eviten ataques lógicos desde fuera de la red claro ejemplo de esto serían los antivirus.

- **Seguridad de los equipos**

(Gupta, 2012), deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo. Así mismo, se debería considerar la ubicación y eliminación de los equipos. Se podrían requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

El designio de esta política es prescindir de la pérdida, deterioro, la sustracción de la información, también proveer la continuidad de servicio evitando la interrupción a las operaciones de la organización.

Actualmente los vigilantes de seguridad impiden a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita.

- **Seguridad del cableado**

(Gupta, 2012), los cables eléctricos y de telecomunicaciones que transportan datos y apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.

Se deben de aplicar normas en la implementación del cableado de una institución, para así poder certificar que la estructura está bien implementada y que cumpla con todos los parámetros de seguridad de la información.

En nuestros días no todas las empresas se rigen mediante normas e estándares internacionales de seguridad del cableado, para dar cumplimiento con parámetros de seguridad y calidad en las comunicaciones.

- **Mantenimiento de los equipos**

(Gupta, 2012), los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

Se debe de dar soporte técnico continuo a los equipos, para garantizar la disponibilidad de estos en todo momento.

Actualmente las instituciones brindan soporte técnico a sus equipos informáticos cada cierto tiempo, por ejemplo, esto se hace periódicamente cada seis meses, con el fin de garantizar la continuidad de servicio.

h) Seguridad en la Operativa

(Gupta, 2012), el objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización

Actualmente las instituciones cumplen con políticas que les permiten aplicar procedimientos de seguridad en las operaciones que se desarrollan con la información de esta.

i) Protección contra código malicioso

(Gupta, 2012), el software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.

El código malicioso es código informático que provoca infracciones de seguridad para dañar un sistema informático.

El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de Troya y bombas lógicas.

j) Controles contra código malicioso

(Gupta, 2012), se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

Las instituciones deben de aplicar medidas de seguridad lógicas y físicas que mitiguen el riesgo que conllevan los códigos maliciosos, para asegurar que la información este integra y disponible en todo momento.

Actualmente las medidas más utilizadas para el control de acceso no deseados figuran entre: antivirus, firewalls, antimalware, entre otros que permiten a la institución evitar que códigos maliciosos pongan en riesgo la integridad de los datos de información.

- **Copias de seguridad**

(Gupta, 2012), hay que mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización.

Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación.

Actualmente existen múltiples mecanismos de recuperación de datos, las copias de seguridad son la principal fuente de respaldos de información.

k) Copias de seguridad de la información

(Gupta, 2012), se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

Mantener las copias de seguridad es fundamental en la continuidad de los procesos de una institución en caso de que algo falle.

En este momento toda institución debe de contar con respaldos físicos y lógicos de su información.

l) Consideraciones de las auditorías de los sistemas de información

(Gupta, 2012), durante las auditorías de los sistemas de información deberían existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

Acordar con el/las áreas/s que corresponda los requerimientos de auditoría.

Actualmente las instituciones deben de Identificar claramente los recursos TI, para llevar a cabo las verificaciones y puestos a disposición de los auditores (Sistemas de información, Bases de datos, hardware, software de auditoría, dispositivos magnéticos, personal, conexiones a red).

m) Controles de auditoria de los sistemas de información

(Gupta, 2012), identificar claramente los recursos TI para llevar a cabo las verificaciones y puestos a disposición de los auditores (Sistemas de información, Bases de datos, hardware, software de auditoría, dispositivos magnéticos, personal, conexiones a red,).se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

Debe de existir el registro histórico de los sistemas de información, así como también los medios lógicos y físicos de respaldo donde se almacenan dichos datos.

En el presente toda institución debe estar sujeta a controles de autoría de los sistemas de información, con el fin de evitar riesgos que pongan en peligro los procesos relacionados con la seguridad y continuidad de la información.

n) Seguridad en las telecomunicaciones

(Gupta, 2012), el objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección.

En la actualidad las instituciones intercambian información por medio de redes privadas y túneles virtuales para evitar la pérdida de información.

ñ) Gestión de la seguridad en las redes

(Gupta, 2012), se deberían controlar los accesos a servicios internos y externos conectados en red.

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red.

Actualmente existen estándares y políticas que apoyan la seguridad de las redes con herramientas de seguridad, de manera lógica y física.

o) Controles de Red

(Gupta, 2012), se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.

Es necesario controlar los accesos a los servicios internos y externos de la red, con el propósito de administrar de forma eficiente el acceso a la información que viaja por este medio.

Hoy en día toda empresa que hace uso de las redes de datos, implementa revisiones que le permiten mantener una administración rigurosa y detallada sobre la información viaja dentro y fuera la misma.

p) Mecanismos de seguridad asociados a servicios de red

(Gupta, 2012), se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

Se deben de implementar acuerdos a nivel de servicios que den cumplimiento al control de los accesos de los usuarios a los servicios de información.

Hoy en día los mecanismos de seguridad de los servicios de red, desempeñan un papel importante en la seguridad de la información de las instituciones, ya que a través de dichos servicios se provee la información a los distintos procesos que se llevan a cabo en la institución.

q) Segregación de redes

(Gupta, 2012), se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.

La segmentación de las redes permite crear grupos red específicos, que sean independientes a los demás grupos, es decir permite organizar distintas redes de comunicación de datos independientes entre sí.

Actualmente las organizaciones implementan la segmentación de las redes, con el fin de crear grupos de trabajos independientes que compartan el mismo medio, pero no la misma información.

r) Intercambio de información con partes externas

(Gupta, 2012), se deberían realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente.

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.

En la actualidad se busca que los canales de comunicaciones principales cuenten con un canal secundario para reducir fallos de continuidad de servicio.

s) Políticas y procedimientos de intercambio de información

(Gupta, 2012), deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

Las políticas y procedimientos en la seguridad de la información permiten proteger la información en todos los medios por donde se mueve, es decir desde que se emite, se trasmite y se recibe.

Las instituciones en la actualidad aplican estas políticas de envío y recepción de información, con el fin en el de asegurar que la información viaje de forma íntegra.

t) Mensajería electrónica

(Gupta, 2012), se debería proteger adecuadamente la información referida en la mensajería electrónica.

Se deben aplicar mecanismos que proporcionen niveles de seguridad en el servicio de mensajería electrónica y así poder evitar riesgos que conlleven a la manipulación no autorizada de la información que viaja dentro de la red.

Actualmente muchas empresas poseen su propio servicio de correo electrónico, por medidas de seguridad, y así evitar que la información se vea comprometida por agentes externos.

u) Relaciones con suministradores

(Gupta, 2012), el objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

En la actualidad las empresas verifican el cumplimiento de los acuerdos de los servicios contratados a terceros, con el objetivo de verla por el cumplimiento.

v) Gestión de la prestación del servicio por suministradores

(Gupta, 2012) la organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.

Se deben implementar acuerdos que permitan gestionar y monitorear el cumplimiento de los servicios acordados con terceros, con el fin de que ambas partes estén de acuerdo.

Actualmente las instituciones verifican el cumplimiento de los acuerdos que se adquieren de la prestación de los servicios de terceros, esto les permite llevar un control adecuado para que sus servicios estén siempre disponibles.

w) Supervisión y revisión de los servicios prestados por terceros

(Gupta, 2012), las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.

Es decir, se debe de llevar a cabo un control exhaustivo para verificar si el proveedor está dando cumplimiento con los servicios prestados.

En la actualidad se controla que el proveedor cumpla con los requisitos del contrato, y brinde un servicio de calidad los proveedores de servicios de internet son un ejemplo claro.

x) Gestión de incidentes en la seguridad de la información

(Gupta, 2012), el objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Las instituciones como tal poseen muchos activos, y cada de uno de estos están expuestos a sufrir incidentes que atenten contra su seguridad e integridad.

Hoy en día las instituciones deben de poder contar con estrategias que fortalezcan los planes de mitigación contra incidentes, consiguiendo detectarlos a tiempo y así prevenirlos en el futuro.

y) Gestión de incidentes de seguridad de la información y mejoras

De acuerdo a (ISO, 2012), deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados se debería aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información. Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales.

Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.

Todos los empleados, deben de conocer los procedimientos y la manera en que deben de informar las eventualidades ocurridas, o de cualquier evento o debilidad que pueda ocurrir en la seguridad de la información lo más rápido posible al punto de contacto designado.

z) Responsabilidades y procedimientos

(Gupta, 2012), se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Se deben establecer responsabilidades de cada parte en dependencia de los incidentes asociados a la seguridad de los datos.

En la actualidad las instituciones deben de poder aplicar procedimientos para gestionar cualquier incidente de seguridad ocurrido, con el objetivo de obtener una solución rápida y viable ante cualquier incidente ocurrido.

- **Notificación de eventos de seguridad de la información**

(Gupta, 2012), los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.

Todo suceso que ocurra con la seguridad de la información debe de ser informada a lo inmediato.

Actualmente las instituciones deben de constar con un personal que notifique eventualidades de la seguridad de la información inmediatamente para tomar medidas en el asunto.

- **Notificación de puntos débiles de la seguridad**

Para (ISO, 2012), se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.

Se debe comunicar inmediatamente cualquier punto débil detectado, para poder aplicar los mecanismos necesarios en pro de fortalecer la seguridad y la integridad de la información sea violada.

En el presente deben de existir no uno sino varios mecanismos que alerten sobre un posible ataque de penetración en los sistemas de dicha institución, entre ellos los mecanismos lógicos y físicos que estén implementados.

2.1.2.2.3. Aspectos de seguridad de la información en la gestión de la continuidad de negocio

(Gupta, 2012) el objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar y tomar en cuenta dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial.

En nuestros días la continuidad de servicio de las instituciones es vital, se deben elaborar planes de continuidad que les permitan asegurar la disponibilidad de los procesos críticos ante cualquier incidente.

a) Continuidad de la seguridad de la información

(Gupta, 2012) se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.

La organización se comprometería a fundar, documentar, implementar y mantener procesos, para mantener los controles de seguridad de la información existentes durante una situación desfavorable.

Las instituciones deben de velar por la validez y la efectividad de las medidas de continuidad por las que ha optado, para controlar que la seguridad de la información regularmente ese correcta, especialmente cuando se hacen actualizaciones o cambios de los sistemas de información. Planificación de la continuidad de la seguridad de la información

b) Implantación de la continuidad de la seguridad de la información

(Gupta, 2012), la organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.

La implementación de métodos de continuidad de servicio que permitan conservar la integridad de la información son estrategias muy positivas, estas garantizan la continuidad de la empresa o institución.

Hoy en día la continuidad de servicios de una determinada institución, pueda surgir efecto debe de existir la ejecución del proceso de seguridad, que se debe lleva a cabo durante situaciones que atenten contra la información.

c) Redundancias

(Gupta, 2012), se deberían considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes que se demuestren insuficientes.

Se debería evidenciar que, la mayoría de los sistemas de información esenciales sean redundantes, para garantizar la disponibilidad de los dispositivos intermediarios.

En el presente las instituciones que hacen uso de sistemas de información, deben garantizar la implementación de dispositivos que sean redundantes y permitan mantener la información disponible en todo momento por diferentes rutas de trasmisión.

d) Disponibilidad de instalaciones para el procesamiento de la información

(Gupta, 2012), se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

Es de gran importancia contar con dispositivos redundantes que permitan mantener los datos en movimiento, de un lugar a otro en caso de que el principal falle este podrá apoyarse en el secundario.

En la actualidad es necesaria que existan dispositivos que apoyen la redundancia de rutas alternativas y necesarias en todas las áreas que procesan la información, para asegurar la disponibilidad de la información este en todo momento.

2.2. PREGUNTAS DIRECTRICES

1. ¿Cuál es estado actual de la red LAN en SILAIS-MATAGALPA?

2. ¿Cuáles son las dificultades encontradas en la infraestructura de la Red LAN, bajo la normativa ISO/IEC 27002:2013?

3. ¿Qué aspectos del estándar de calidad y normativa de seguridad de la normativa ISO/IEC 27002:2013 dan respuesta a los hallazgos y dificultades encontradas en esta investigación?

CAPÍTULO III

3.1. DISEÑO METODOLÓGICO

3.1.1. Enfoque de investigación

Los estudios se basaron en la aplicación de controles de la norma: ISO/IEC 27002:2013, la investigación se basa en la observación de las situaciones y no se manipulo ningún tipo de proceso de la red LAN en la institución SILAIS - MATAGALPA, el enfoque de nuestra investigación es cualitativa con técnicas cuantitativas, aplicando métodos de indagación de datos como (entrevistas, y observación).

3.1.2. Tipo de investigación según su alcance, diseño y corte

- ✓ Según su alcance: descriptiva ya que muestra cómo se encuentra estructurada la infraestructura de red.

- ✓ Según su diseño: es no experimental porque no se maniobraron variables y se relató de forma existente el diseño de la red LAN.

- ✓ Por su corte: es transversal porque el estudio ocurrió en un tiempo determinado donde se aplicaron los instrumentos de estudio ya mencionados, periodo 2019.

3.1.3. Universo de estudio

El universo de estudio fue la Infraestructura de la red LAN del Sistema Local de Atención Integral (SILAIS MATAGALPA).

Métodos y técnicas para el análisis de datos:

- Entrevistas dirigidas al encargado de informática (Anexo 2)
- Observación no participativa (Anexo 3)

3.1.4. Recolección y análisis de datos

Toda la información recopilada fue estudiada a través de los métodos deductivo e inductivo, esta se analizó y se procesó a través de la paquetería ofimática y herramientas informáticas: Paquetería Microsoft Office: Word 2019, Microsoft Excel 2019 y Cisco Packet Tracert.

Los materiales didácticos que se utilizaron para el desarrollo y elaboración del informe final son: computadoras, multifuncional, memorias USB, internet, curricular Cisco CCNA versión 4.0, más la respectiva papelería de oficina.

3.1.5. Las variables de estudio que se analizaron (Anexo 1)

1. Infraestructura de red (LAN) en el Sistema Local de Atención Integral (SILAIS-MATAGALPA).

2. ISO/IEC 27002:2013 (guía de buenas prácticas para la seguridad de la información).

CAPITULO IV

4.1. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

4.1.1. Descripción de ámbito

Es el Sistema Local de Atención Integral SILAIS-MATAGALPA, es una organización gubernamental de carácter administrativo conformada por compañeros y compañeras que laboran por la vigilancia y supervisión de la salud en los diferentes puestos de atención en nuestra ciudad de MATAGALPA. Esta organización busca fortalecer los servicios de salud prestados a: niños, niñas, jóvenes; adultos, ancianos sin fines de lucro.

Hoy por hoy esta institución cuenta con una infraestructura de red LAN desorganizada y sin documentación, que afecta el rendimiento y la seguridad de la información.

4.1.1.1. Estado actual de la arquitectura de red LAN de SILAIS-MATAGALPA

SILAIS-MATAGALPA, actualmente cuenta con una sola red LAN, con diferentes debilidades, ejemplo claro de esto es que la red no es: tolerante a fallos y no puede brindar la continuidad de servicio, debido a que solo cuentan con un único ISP, (proveedor de servicio de internet), causando que la red principal deje de operar de manera inmediata si este proveedor falla por cualquier motivo que sea.

La red principal se denomina como una red interna, (INTRANET), es esta la que ofrece los servicios de enlace como vía principal para que la información viaje de punto a punto de manera correcta dentro de la LAN.

(Mendoza, 2019), gracias a palabras obtenidas por el responsable de informática se conoce que la red no es escalable, se ha observado que la arquitectura de red actual crece de manera desorganizada por la demanda de nuevos usuarios y dispositivos cada día.

Esta red carece de calidad de servicios (QoS), puesto que la red no está segmentada evitando que la red no enrute en base a la prioridad de servicios que viajan dentro de

la red, servicios tales como multimedia e información. Se destaca que el responsable de informática no conoce estos términos y su debida implementación.

La Intranet en SILAIS-MATAGALPA, no posee procedimientos y herramientas óptimas de seguridad que permitan mitigar fallas en dicha arquitectura de red.

4.1.1.2. Tipos de Red

SILAIS-MATAGALPA, cuenta con una sola red LAN, que interconecta las estaciones de trabajo conectadas y ubicadas en las diferentes áreas. Dicha red esta no sobrepasa extensiones territoriales fuera de Matagalpa, por lo tanto, es una red LAN.

4.1.1.3. Topología de Red

(Mendoza, 2019), adjudicaba que desconoce sobre cualquier tipo documentación de topología lógica y física implementada en la red LAN, sin embargo, mediante la indagación se pudo identificar que esta se asimila a la topología denominada: MIXTA, debido a que se deriva de la unión de varios tipos de topologías de red.

4.1.1.4. Calidad de las comunicaciones

La forma en que está organizada la red LAN de la institución exhibe un determinado grado de complejidad, que impacta en la eficacia de las comunicaciones, debido a que dicha estructura de red se encuentra desorganizada y sin documentación, un ejemplo claro es el cuello de botella que se da en base a la cantidadde mensajes que se trasmiten de manera simultánea.

Figura 1. Red mal estructurada

Fuente: *elaboración propia mediante método observación*

4.1.1.5. Infraestructura física dispositivos de red

La tabla 1 muestra los componentes de la infraestructura de red LAN la cual cuenta con enrutadores, conmutadores, panel de conexión y un Grandstream como central telefónica

Tabla 1. Dispositivos de la red LAN SILAIS-MATAGALPA

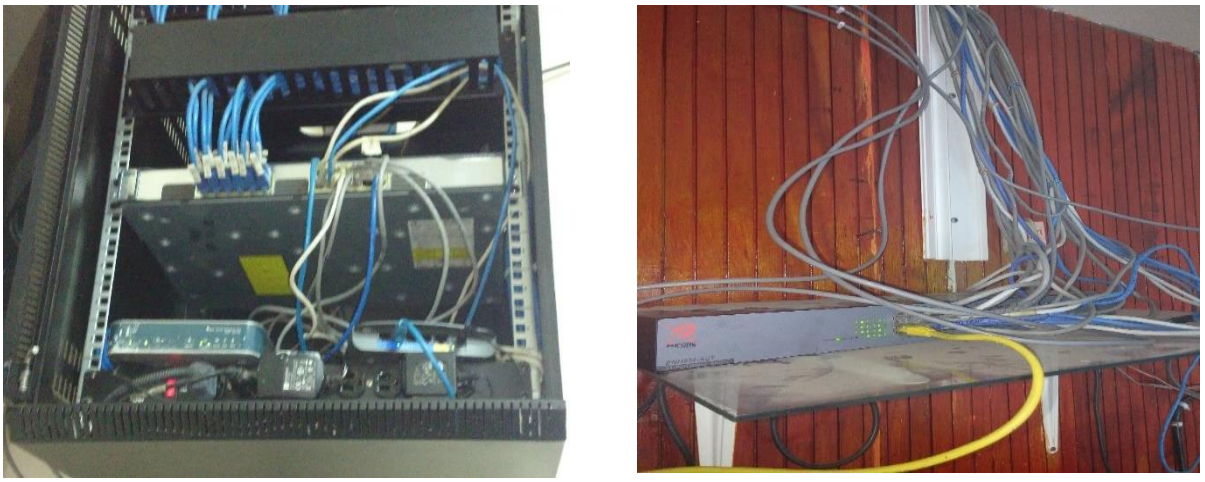
INVENTARIO DE DISPOSITIVOS DE RED						
Tipo de Dispositivo	**Marca**	**Modelo**	**Dirección IP**	**Ubicación**	**Rol de Trabajo**	**Tipo de protocolo**
SWITCH	ENCORE ELECTRONICS	ENH9-16P-NWY	172.16.XXX.XXX	DIRECCION DE COOPERACION EXTERNA Y PLANIFICACION	CONMUTADOR	PREDETERMINADO
SWITCH	NEWLINK	6020	172.16.XXX.XXX	ESTADISTICAS	CONMUTADOR	PREDETERMINADO
ROUTER	CISCO	LINKSIS	172.16.XXX.XXX	FINANZAS	REPETIDOR	DNS, HTTP, PROXYS, DHCP
SWITCH	ENCORE ELECTRONICS	ENH9-16P-NWY	172.16.XXX.XXX	CONTABILIDAD	CONMUTADOR	PREDETERMINADO
SWITCH	NEXXT SOLUTION	ASFRM164U1	172.16.XXX.XXX	RECURSOS HUMANOS	CONMUTADOR	PREDETERMINADO
ROUTER	ELTEL	ET-530	172.16.XXX.XXX	ADMINISTRACION	ENRUTADOR	DNS, HTTP, PROXYS, DHCP
SWITCH	ENCORE ELECTRONICS	ENH9-16P-NWY	172.16.XXX.XXX	SECRETARIA	CONMUTADOR	PREDETERMINADO
SWITCH	NEWLINK	6020	172.16.XXX.XXX	DIRECCION	CONMUTADOR	PREDETERMINADO
ROUTER	CISCO	LINKSIS	172.16.XXX.XXX	SALA SITUACIONAL	REPETIDOR	DNS, HTTP, PROXYS, DHCP
SWITCH	NEXXT SOLUTION	ASFRM164U1	172.16.XXX.XXX	SUBDIRECCION	CONMUTADOR	PREDETERMINADO
SWITCH	ENCORE ELECTRONICS	ENH9-16P-NWY	172.16.XXX.XXX	SECRETARIA DE ENFERMERIA	CONMUTADOR	PREDETERMINADO
SWITCH	NEXXT SOLUTION	ASFRM164U1	172.16.XXX.XXX	DOCENCIA	CONMUTADOR	PREDETERMINADO
ROUTER	NEXTEL	R-8000	172.16.XXX.XXX	AUDITORIA	REPETIDOR	DNS, HTTP, PROXYS, DHCP
SWITCH	NEWLINK	6020	172.16.XXX.XXX	LAB-INFORMATICO	CONMUTADOR	PREDETERMINADO

Fuente: Elaboración propia mediante método observación

4.1.1.6. Medios de transmisión cableados

El cableado de la red principal está estructurado mediante el uso de cable de par trenzado (UTP) cat5e, el cual permite interconectar todos los dispositivos finales e intermediarios de la red a una velocidad de hasta 622 Mb/s. se destaca que el cableado se encuentra desorganizado por lo tanto no está estructurado y sin la debida protección.

Figura 2. Cableado de red principal



Fuente: Elaboración propia mediante método de observación

4.1.1.7. Estaciones de trabajo

Se preguntó al responsable de informática por la cantidad de computadoras por área, tal como se muestra a continuación.

Tabla 2. Cantidad de computadoras por áreas SILAIS - Matagalpa

AREA	CANTIDAD
PLANIFICACION	6
SUBDIRECCION MEDICA	2
ADMINISTRACION	3
DIRECCION	2
ESTADISTICAS	6
TESORERIA	3
FINANZAS	4
COMPRAS	3
CONTABILIDAD	10
RRHH	5
PAI	3
BODEGA	1
TB VIH	2
COMUNICACION	4
FARMACIA	1
ASESORIA LEGAL	1
VIGILANCIA	3
AIMNA	6
ETV	3
ENFERMERIA	2
PUESTO DE MANDO	2

Fuente elaboración propia mediante entrevista

4.1.1.8. Políticas de seguridad físicas

En SILAIS-MATAGALPA, no existen políticas de seguridad físicas implementadas en la infraestructura la red LAN, sin duda alguna esto conlleva una gran amenaza de seguridad en todos los dispositivos.

No se cuenta con un procedimiento de seguridad que permita evitar la manipulación y acceso no autorizado a la información por personal no autorizado, cabe señalar que el personal no conoce de ningún tipo de políticas de seguridad sobre los procedimientos que se deben de llevar a cabo para salvaguardar la información.

Los dispositivos que se encuentran fuera de la oficina de informática no están debidamente protegidos, dado que permanecen a la intemperie donde cualquier persona ajena puede manipular de manera no autorizada los dispositivos.

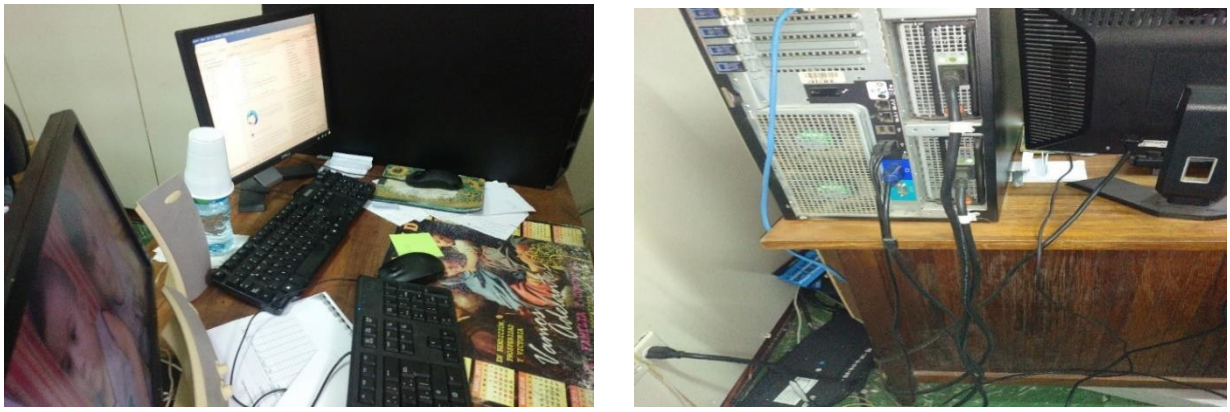
Figura 3. Dispositivos desprotegidos

Fuente elaboración propia mediante observación

4.1.1.9. Infraestructura Lógica Servidores

SILAIS-MATAGALPA, cuenta únicamente con un servidor financiero, (SIAFI), Sistema Integrado de Administración Financiera de la institución que ayuda con la contabilidad de dicha institución, basado en la plataforma de sistema operativo Windows server 2003.

Figura 4. Servidor SIAFI

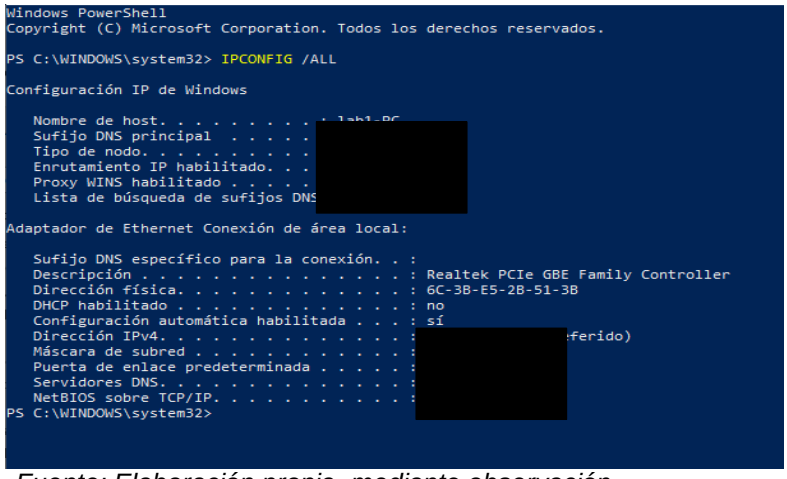


Fuente: elaboración propia, mediante observación

4.1.1.10. Direccionamiento IP

El rango de IP privado implementado en la red principal es 172.16.0.0/24, las direcciones IP son asignadas de manera estáticas a cada computadora:

Figura 5. Direccionamiento IP



Fuente: Elaboración propia, mediante observación

4.1.1.11. Servicios de Red

Las redes de la institución ofrecen los siguientes servicios.

1. Proxy
2. Mensajería Electrónica
3. Impresiones en red
4. Protocolo de trasferencias de archivos (FTP).

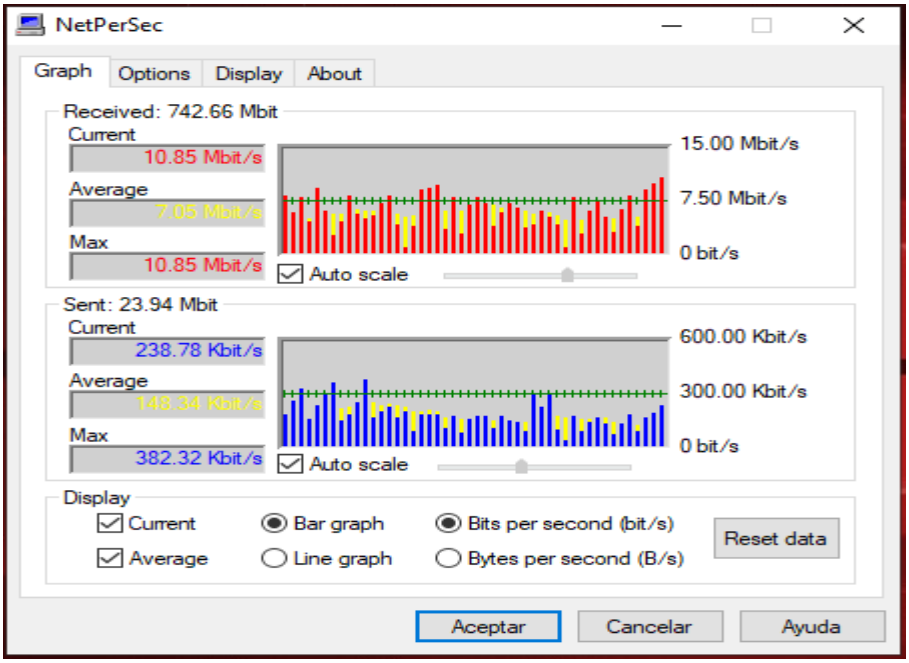
4.1.1.12. Segmentación de red

La institución no implementa ningún tipo de o agrupación por área de su red LAN o mejor conocidas como LAN VIRTUALES (VLAN's), por lo tanto, no existe ningún tipo de segmentación de red.

4.1.1.13. Ancho de banda

La red LAN cuenta con un ancho de banda de 10 Mb/s brindado por el principal y único (ISP) Proveedor de Servicios de Internet (CLARO).

Figura 6. Prueba de Ancho de banda



Fuente: Elaboración propia, mediante observación

4.1.1.14. Firewall

Únicamente se utilizan los predeterminados por los sistemas operativos de Windows conocidos como firewalls lógicos.

4.1.1.15. VPN

Cisco VPN, una herramienta que se utiliza para hacer la conexión entre un sistema que viaja por medio de este túnel, hacia servidores que están ubicados en la presidencia de la república, en función de dar a conocer la estadística del sistema PAMOR, programa amor para los más chiquitos.

4.1.1.16. Central Telefónica

La cuenta de teléfonos análoga o mejor conocida en la institución como “teléfonos de 4 dígitos”, es manejada de manera lógica por un (GRANDSTREAM), que se encarga de enlazar las llamadas dentro del local, se destaca que este dispositivo no es cuenta con documentación técnica de la misma, por lo tanto, no puede ser administrada por el responsable de informática.

Figura 7. Central Telefónica

Fuente: Elaboración propia, mediante observación

4.1.1.17. Políticas de seguridad Lógicas

SILAIS-MATAGALPA, de igual manera que no cuenta con políticas de seguridad físicas no tiene establecida ni documentadas las políticas de seguridad lógicas.

4.1.1.18. Amenazas lógicas

Para mitigar las amenazas externas en las estaciones de trabajo SILAIS-MATAGALPA, implementa como mecanismo de seguridad el antivirus McAfee (The McAfee Agent), con licencia valida por 5 años, valida desde el 2018 hasta el año 2023.

4.1.2. ISO/IEC 270002-2013

Según (ISO, 2013) es una guía de buenas prácticas que describe cuáles deben de ser los objetivos de control que se deben aplicar sobre la seguridad de la información no es certificable. En total la norma contiene 35 objetivos de control y 114 controles los cuales están agrupados en 14 dominios.

La ISO/IEC 27002:2013 no es para fines de certificación, esta ofrece una muy buena guía para la gestión de la seguridad de la información de determinadas empresas, permitiéndole adoptar buenas prácticas que ayuden a mantener la integridad y disponibilidad de la misma.

Se cuestionó al responsable de informática, sobre si conocía de algún tipo de normas que rigen las políticas de seguridad de la información, el respondió “no conocer de tales normativas”.

De la misma manera se le abordo sobre si conocía la guía o la Norma ISO/IEC 27002:2013, respondió que no tenía conocimiento de dicha guía inmediatamente. Se destacará la importancia de normativas que ayudan a regir la seguridad de la información, dado que esta es el principal y más importante activo de la institución.

4.1.2.1. Políticas de Seguridad conjunto de políticas

El responsable de informática fue abordado sobre este tema, de una manera directa sobre si existían políticas de seguridad que afianzaran la seguridad de la red, respondiendo que no existen tales políticas. SILAIS/MATAGALPA, evidentemente no cumple con el objetivo: ISO/IEC 27002:2013, ya que no cuenta con normativas que protejan la seguridad de la información.

4.1.2.2. Aspectos organizativos de la seguridad de la información Segregación de tareas

Las instituciones asignan tareas y responsabilidades a cada área de trabajo, con el fin de poder controlar la información de manera más detallada y eficiente, brindando así un mayor nivel de seguridad. Las instituciones están trabajando para minimizar la dependencia, gracias a que se asignan roles a las personas en las diferentes áreas de trabajo.

4.1.2.3. Seguridad ligada a los recursos humanos antes de la contratación

Se indago al responsable de informatíca si antes de su contratación se le dieron a conocer cuales eran las normas y medidas de seguridad sobre la información, a lo cual respondío que no se le habia brindado tal informacion antes de su contratación. Este objetivo de control es desconocido por el responsable de informatica por lo cual no cumple con el objetivo: ISO/IEC 27002:2013.

4.1.2.4. Gestión de activos Responsabilidad sobre los activos

El entrevistado respondió que el mantenimiento adecuado a los equipos está bajo su responsabilidad. Los roles de propietario de los equipos como se figura el entrevistado para su debido mantenimiento son orientados de manera directa por el administrador que figura como jefe inmediato del responsable de informática de: SILAIS-MATAGALPA, este no posee documentos oficiales de este tipo de control por lo tanto no cumple con el objetivo: ISO/IEC 27002:2013.

4.1.2.5. Inventario de activos

El abordado comunicó que el inventario de equipos no está a cargo de su persona sino más bien del área de requisición de equipos e inventarios del almacén da

suministros de SILAIS-MATAGALPA. El inventario detallado de equipos computacionales, aunque no esté a cargo del responsable de informática, está a cargo de otra área por lo tanto el objetivo de control: ISO/IEC 27002: 2013.se cumple de manera parcial.

4.1.2.6. Uso aceptable de los activos

El responsable de informática al ser abordado sobre este tema, afirmó que no existe ninguna documentación sobre la regulación del manejo y los procedimientos de dispositivos de redes. La Institución no docu0menta regulaciones necesarias para regir el uso adecuado de estos activos, por la tanto no cumple con el objetivo: ISO/IEC 27002:2013.

4.1.2.7. Manejo de los soportes de almacenamiento

El responsable de informática al ser cuestionado sobre cómo era el manejo almacenamiento y respaldo de la información de equipos que de una u otra manera no estaban activos, respondió: que era almacenada en diferentes dispositivos: tales como discos duros o memorias USB, solo si esto era autorizado por sus autoridades inmediatas. La Institución cumple parcialmente el objetivo de control: ISO/IEC 27002:2013.

4.1.2.8. Control de accesos Requisitos de negocio para el control de accesos

Se cuestionó al responsable de informática sobre si se controla el acceso a las áreas donde se da el procesamiento de la información y respondió que no hay ningún control. SILAIS-MATAGALPA, por lo antes expuesto no cumple con el objetivo: ISO/IEC 27002:2013.

4.1.2.9. Política de control de acceso

Al realizar la entrevista al responsable de informática se le pregunto si están establecidas y documentadas las políticas de control de acceso, este respondió que no. A la fecha SILAIS-MATAGALPA, no posee dicha implantación ni documentación de políticas de acceso, por lo antes expuesto no cumple con el objetivo: ISO/IEC 27002:2013.

4.1.2.10. Control de acceso a las redes y servicios asociados

Se abordó al responsable de informática sobre si existe la vigilancia de acceso a las redes de datos, este respondió que no se controla a los usuarios que hacen uso de la red. La institución no cumple con el objetivo: ISO/IEC 27002:2013.

4.1.2.11. Gestión de acceso de usuarios

Se cuestiono al encargado de informática, sobre la existencia de procedimientos formales que le permitan determinar los parámetros necesarios para asignar los permisos de acceso a la red, respondiendo que no. El responsable de informática no cuenta con parámetros definidos que le permita asignar los permisos de acceso a los sistemas y red, por lo cual no se cumple el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.12. Gestión de altas/bajas en el registro de usuarios

(Mendoza, 2019), posee algún tipo de proceso formal para dar de alta o de baja a un usuario de la red. En SILAIS-MATAGALPA, no existen operaciones formales para realizar altas y bajas de usuarios que accedan a la red, por lo consiguiente el objetivo de ISO/IEC 27002:2013 no se cumple

4.1.2.13. Cifrado

Se abordó al jefe del área informática sobre si existe, algún mecanismo de encriptación de la información, a lo que respondió que no. La institución no implementa métodos de seguridad que respalde la seguridad de la información, por lo deducido el objetivo de ISO/IEC 27002:2013 no se cumple.

4.1.2.14. Políticas de uso de controles criptográficos

Se le pregunto al encargado sobre si existen políticas de seguridad que regulen el uso de criptografía en la información, este respondió que no. SILAIS-MATAGALPA, no establece mecanismos de cifrado o criptografía en su información por lo tanto no aplica las políticas del uso de control de la seguridad, incumpliendo el objetivo de ISO/IEC 27002:2013.

4.1.2.15. Seguridad física y ambiental Áreas seguras

El objetivo de la pregunta al responsable de informática fue, si los dispositivos de la red están ubicados en áreas debidamente protegidas ante cualquier intrusión o manipulación, respondiendo que solo un 75 por ciento está protegido. En SILAIS-MATAGALPA, no se salvaguardan los dispositivos de red al 100 por ciento, por lo tanto, el objetivo de control de ISO 27002:2013 se cumple de manera parcial.

4.1.2.16. Controles físicos de entrada

El jefe del área informática, al ser abordado sobre la temática, si existe algún control para acceso donde están ubicados los dispositivos de red, este respondió que el 80% de los dispositivos ubicados en diferentes áreas están, resguardados por que estas oficinas están protegidas bajo llave. Actualmente SILAIS-MATAGALPA, tiene desprotegidos el 20 por ciento de dispositivos de red, por esta razón el objetivo de control de ISO/IEC 27002:2013 se cumple parcialmente.

4.1.2.17. Protección contra amenazas externas y ambientales

Los dispositivos de red están en ubicaciones seguras en caso de que ocurra un desastre natural fue la pregunta que se le hizo al encargado de informática, respondiendo este que no existe un lugar seguro para estos dispositivos en caso de que un desastre de carácter ambiental o mal intencionado ocurriese.

SILAIS-MATAGALPA, no cuenta con un plan que le ayude a proteger sus bienes computacionales ante desastres naturales y/o por ataques maliciosos de personas ajenas a la institución, por lo tanto, no se cumple el control de ISO/IEC 27002:2013.

4.1.2.18. Seguridad de los equipos

El jefe del área informática fue abordado sobe si los dispositivos de red se encuentran debidamente protegidos y ubicados de manera correcta en el rack de datos, este respondió que solo una parte cuenta con energía de respaldo y climatización correcta, los otros dispositivos no cuentan con lo antes mencionado. Actualmente esta institución cumple de manera parcial el objetivo propuesto por ISO/IEC 27002:2013.

4.1.2.19. Seguridad del cableado

Se le cuestiono al encargado de informática si el cableado está debidamente asilado de cualquier contacto con el usuario, para evitar una manipulación indeseada, este respondió que no todo el cableado viaja dentro de canaletas plásticas. La institución no cuenta con un cableado de red estructurado, por lo tanto, incumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.20. Mantenimiento de los equipos

El entrevistado al ser cuestionado de cada cuanto tiempo se da el mantenimiento de dar soporte técnico a los equipos, para garantizar la disponibilidad de estos, respondió que se realiza mantenimiento preventivo cada 6 meses, y el correctivo este en el momento que sea necesario. SILAIS-MATAGALPA, cumple a cabalidad el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.21. Seguridad Operativa Protección contra código malicioso

Al ser abordado sobre cual método utiliza para proteger a los equipos de códigos maliciosos, este respondió que está vigente el antivirus: McAfee Endpoint Security. Esta institución, cumple a de manera correcta el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.22. Controles contra código malicioso

Se preguntó al entrevistado si existe algún método que permita la detección y mitigación de códigos maliciosos, este respondió que únicamente el antivirus. La institución no implementa controles adecuados que permitan la mitigación de malware y la recuperación de los datos ante situaciones que afecten la seguridad de la información, solo se implementa el uso de antivirus, por lo tanto, el objetivo de control propuesto por ISO/IEC se cumple parcialmente.

4.1.2.23. Copias de seguridad

Se entrevisto al encargado del área informática sobre cuales son los procesos de copias de seguridad, este contesto que se cumple. El objetivo de control propuesto por ISO/IEC 27002:2013 se cumple parcialmente ya que no cumple con todas las medidas de seguridad establecidas.

4.1.2.24. Copias de seguridad de la información

Se entrevistó al responsable de informática, si se realizan copias de seguridad y cada cuanto tiempo, este respondió que únicamente al servidor (SIAFI), y cada semana luego de esto la información es almacenada en un escritorio seguro en un disco duro externo. El objetivo de control propuesto por ISO/IEC 27002:2013 se cumple parcialmente ya que no cumple con todas las medidas de seguridad establecidas.

4.1.2.25. Consideraciones de las auditorías de los sistemas de información

Se cuestionó al encargado de informática si se realizan auditorías a los sistemas de información y de redes, a lo que respondió que no. La institución no realiza auditorías a sus sistemas y red, por lo tanto no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.26. Controles de auditoria de los sistemas de información

El encargado de informática afirmo que no existen controles de auditoria puesto que la institución no aplica auditorías a sus sistemas y a su red LAN. Por consiguiente, no cumple con el objetico de control propuesto por ISO/IEC 27002:2013.

4.1.2.27. Seguridad en las telecomunicaciones

Se abordó al responsable de informática sobre si existen procesos en la seguridad de las telecomunicaciones en SILAIS-MATAGALPA, este afirmo que no. Por consiguiente, no cumple con el objetico de control propuesto por ISO/IEC 27002:2013.

4.1.2.28. Gestión de la seguridad en las redes

Se entrevistó al responsable del área de informática si existe controles a los servicios internos y externos de la red en el SILAIS-MATAGALPA, a lo que respondió que no. Por consiguiente, no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013

4.1.2.29. Controles de Red

El encargado de informática fue abordado si existe algún método o herramienta para monitorear y supervisar la red, este contesto que no cuenta con nada de lo antes mencionado. La institución no implementa herramientas que le permitan monitorear y

detectar intrusiones en la red con el fin de asegurar la integridad de los datos, por consiguiente, no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.30. Mecanismos de seguridad asociados a servicios de red

Se le cuestiono al responsable de informática que mecanismos utiliza para darle protección a la red, este contesto que únicamente los mecanismos lógicos, tales como antivirus, y firewall de Windows. La institución no identifica y/o emplea ningún mecanismo de seguridad físico para la protección de los servicios de red, por consiguiente, cumple parcialmente con el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.31. Segregación de redes

La segmentación de la red LAN fue una pregunta en cuestión hacia el encargado de informática, este respondió que no existe ningún tipo de VLAN, que permita agrupar la red LAN, por áreas. SILAIS-MATAGALPA, no implementa (VLAN's), debido a la desorganización y mala estructuración de la red, por consiguiente, no se cumple el objetivo de control de ISO/IEC 27002:2013

4.1.2.32. Intercambio de información con partes externas

Se le cuestiono al responsable de informática si intercambian información con entidades externas a la institución, este respondió que no. La institución al no utilizar la red para intercambiar información con entidades externas, no implementa políticas y acuerdos de intercambio, por lo tanto, no cumple con el objetivo propuesto por ISO/IEC 27002:2013.

4.1.2.33. Políticas y procedimientos de intercambio de información

Se cuestionó al responsable de informática si existen políticas y procedimientos de Intercambio, a lo que respondió que no. La institución, por lo tanto, no cumple con el objetivo propuesto por ISO/IEC 27002:2013.

4.1.2.34. Mensajería electrónica

El responsable de informática comento que en SILAIS-MATAGALPA, se utiliza correo electrónico interno, para proteger adecuadamente la informacion. Actualmente el objetivo de control propuesto por ISO/IEC 27002:2013 se cumple de manera correcta.

4.1.2.35. Relaciones con suministradores

Se entrevistó al encargado del área informática si existe relación con los suministradores de servicios terceros, a lo que este comento que no. Actualmente el objetivo de control propuesto por ISO/IEC 27002:2013 no se cumple.

4.1.2.36. Gestión de la prestación del servicio por suministradores

Se abordó al responsable de informática sobre si monitorea el cumplimiento de servicios prestados a la red por terceros, en este caso el (ISP), Proveedor de Servicios de Internet, este comento que únicamente se vigila el cumplimiento del ancho de banda prestado por dicho proveedor. Actualmente el objetivo de control propuesto por ISO/IEC 27002:2013 se cumple de manera correcta.

4.1.2.37. Supervisión y revisión de los servicios prestados por terceros

El responsable de informática al ser abordado si monitorea el servicio prestado por su Proveedor de Servicios de Internet, asevero que si se monitorea. SILAIS-MATAGALPA, el objetivo de control propuesto por ISO/IEC 27002:2013 se cumple de manera correcta.

4.1.2.38. Gestión de incidentes en la seguridad de la información

Se entrevistó al encargado del área informática si existe el procedimiento de garantizar que los eventos de seguridad de la información sean comunicados en tiempo oportuno este contesto que no existe tal procedimiento. Actualmente el objetivo de control propuesto por ISO/IEC 27002:2013 se cumple de manera correcta.

4.1.2.39. Gestión de incidentes de seguridad de la información y mejoras

Se preguntó a la entrevistada si se implementan procedimientos para el manejo de los incidentes relacionados con la seguridad de la información en el área de redes, a

lo que respondió que no. La institución no implementa procedimientos que permitan detectar y documentar Incidentes en relación con la seguridad de la información, por lo que no cumple el objetivo de control de ISO/IEC 27002:2013.

4.1.2.40. Responsabilidades y procedimientos

Se le preguntó al responsable de informática, si están establecidos los procedimientos para dar respuesta a incidente de seguridad de la información en el área de redes, a lo que respondió que no. La institución no ha establecido procedimientos necesarios dar respuesta a Incidentes de seguridad, por lo tanto, no cumple con el objetivo de control de ISO27002:2013.

4.1.2.41. Notificación de eventos de seguridad de la información

Se le abordo al encargado de informática si se notifican a la administración lo eventos asociados a la seguridad de la información del área de informática, a lo que respondió que a veces solo cuando se tratan de incidentes relacionados con los sistemas internos. En la institución no existe una administración adecuada de los incidentes de seguridad, porque solo se notifican aquellos incidentes relacionados a los sistemas internos, por lo tanto, se cumple de manera parcial el objetivo de control propuesto por ISO 27002:2013.

4.1.2.42. Notificación de puntos débiles de la seguridad

Se le cuestiono al entrevistado si documenta y notifica a la administración, las sospechas de puntos débiles en la seguridad de la información que viaja mediante la red. Dentro de la institución no se notifican los puntos débiles de la seguridad de la información, por lo tanto, no se cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

4.1.2.43. Continuidad de la seguridad de la información

Se cuestionó al entrevistado si existen un plan de continuidad y recuperación de los procesos de seguridad de la información ante desastres a lo que respondió que no. La institución no cuenta con un plan de continuidad de negocio, que permita la recuperación inmediata de la información ante desastres, por ende no cumple con el objetivo de control de ISO/IEC 27002:2013.

4.1.2.44. Implantación de la continuidad de la seguridad de la información

Se abordo al encargado del area informatica si se han implementado procesos, procedimientos y controles, para garantizar un nivel necesario de seguridad de la información ante situaciones adversas a lo que respondió que no.

Al no existir un plan de continuidad de la seguridad de la información, no existe documentación e implementación de procedimientos que brinden un nivel necesario para mantener la seguridad de la información, por lo tanto la entidad no cumple con el objetivo de control de ISO/IEC 27002:2013.

4.1.2.45. Redundancias

Se le pregunto al encargado de informática si existen dispositivos de red que permitan la redundancia en la infraestructura de red, a lo que respondió que no. No existen redundancias en la infraestructura de red, por lo tanto, este objetivo de control de ISO/IEC 27002:2013 no se cumple.

4.1.2.46. Disponibilidad de instalaciones para el procesamiento de la información

Se le pregunto al encargado de informática si los dispositivos de red son redundantes en caso de que deban de brindar la continuidad de servicio en las instalaciones, el respondió que no. No existen redundancias en la infraestructura de red ni en las instalaciones, por lo tanto, este objetivo de control de ISO/IEC 27002:2013 no se cumple.

4.1.3. Evaluación de madurez respecto a los controles definidos de ISO 27002:2013

4.1.3.1. Porcentajes de dominios ISO27002:2013

El cuadro de porcentaje de dominios muestra de manera descriptiva sus 14 niveles donde se evaluó el 68 por ciento del 100 por ciento, el porcentaje más alto representado en esta grafica muestra: el dominio: seguridad en la operativa es el más afectado con un 50 por ciento, el dominio: seguridad física y ambiental con una afectación de un 14 por ciento, el 3 por ciento de déficit lo representa el dominio: gestión de incidentes en la seguridad de la información, y el 1 por ciento para el dominio: seguridad de los activos. La suma de los dominios antes citados nos demuestra que la institución (SILAIS- MATAGALPA), no cumple al 100 por ciento los dominios evaluados de la normativa ISO 27002/2013, representando así el total porcentual de inseguridad de la información, para dicha grafica se tomaron en cuenta los puntos básicos que miden el funcionamiento de la red LAN por dominios bajo la normativa ISO 27002/2013, #NCBaja conformidad, #NC Alta Efectividad, #NC OK No se cumplen o no existen.

Tabla 3. Porcentajes de dominios ISO/IEC 27002:2013

	Dominio	% de conformidad	# NC baja efectividad	# NC alta efectividad	# NC OK
A.5	POLÍTICAS DE SEGURIDAD	0%	2	0	0
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	0%	7	0	0
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	0%	6	0	0
A.8	GESTIÓN DE ACTIVOS.	1%	10	0	0
A.9	CONTROL DE ACCESOS.	0%	14	0	0
A.10	CIFRADO.	0%	2	0	0
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	14%	12	2	1
A.12	SEGURIDAD EN LA OPERATIVA.	50%	12	0	2
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	0%	6	0	1
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE	#N/A	0	0	0
A.15	RELACIONES CON SUMINISTRADORES.	0%	5	0	0
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	3%	7	0	0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	0%	4	0	0
A.18	CUMPLIMIENTO.	#N/A	0	0	0

Fuente: Elaboración propia, mediante observación

4.1.3.2. Porcentaje de conformidad de dominios

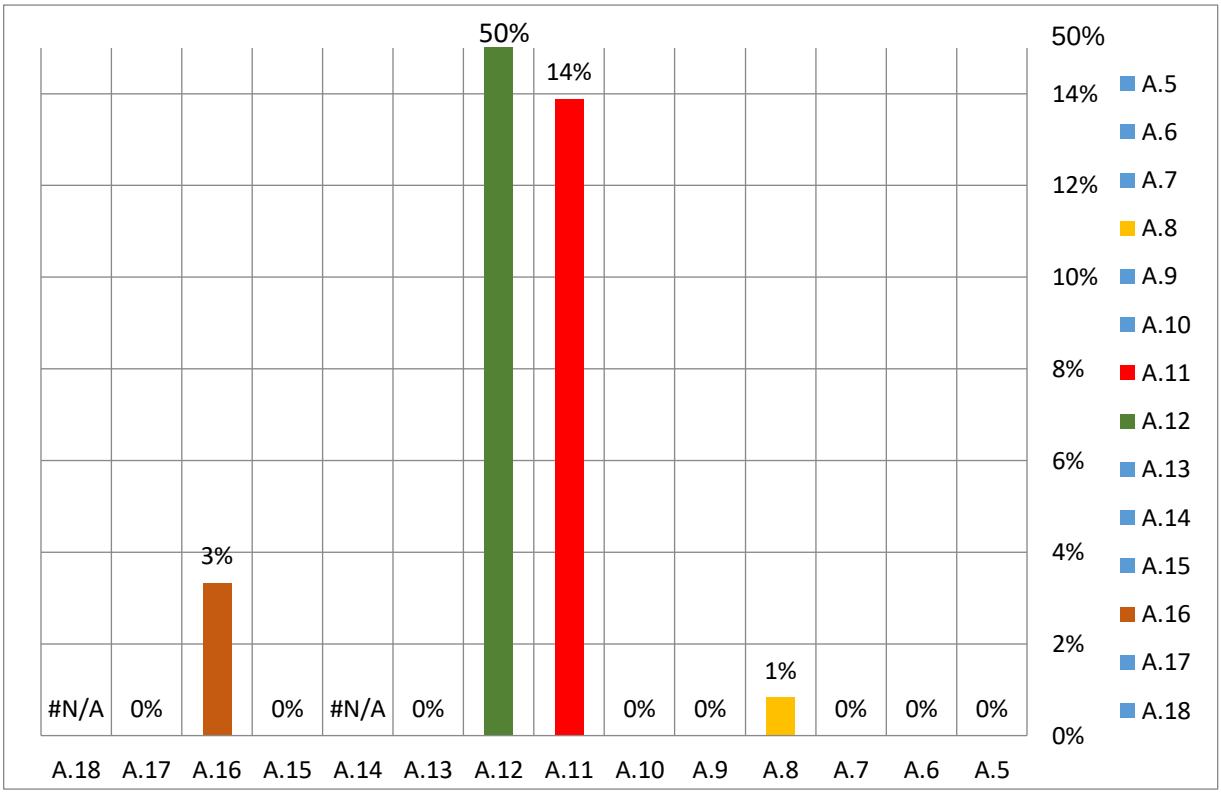


Gráfico 1. Porcentaje de conformidad con ISO 27002:2013 por dominios

Fuente: Elaboración propia a partir de estándar ISO 27002:2013

El gráfico muestra los cuatro dominios que generan la suma de un 68 % de conformidad se cumplen con respecto al 100 % en función de los 14 dominios de la ISO 27002:2013.

4.1.3.3. Tabla de efectividades ISO 27002:2013

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	85
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	2
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	2
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	0
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	1
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	3
L6	N/A	No aplica		21

La tabla de efectividad muestra el valor de manera resumida de los controles y los objetivos de control, que se caracterizan como valores existentes y no existentes.

Tabla 4. Efectividades ISO/IEC 27002:2013

Fuente: Elaboración propia, mediante observación

4.1.3.4. Aprobación de dominios

Según los datos obtenidos de los 114 objetivos de control que conforman los 14 dominios, se clasifican de la siguiente forma: Aprobados 4, No Aprobados 89 y no aplican 21.

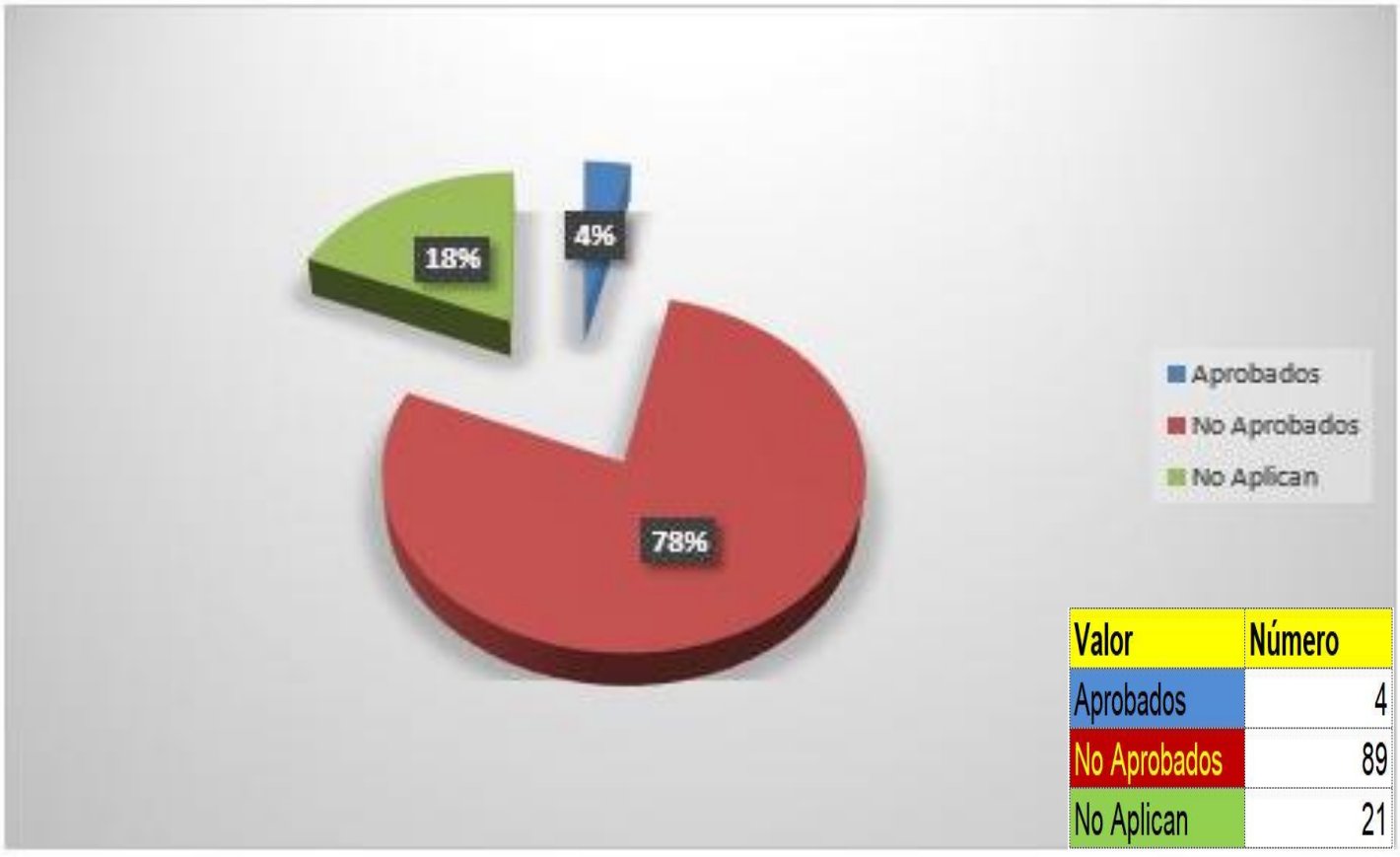


Gráfico 2. Aprobación de dominios

Fuente: Elaboración propia, a través del proceso de investigación.

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN - MANAGUA

Facultad Regional Multidisciplinaria, Matagalpa
UNAN Managua - FAREM Matagalpa

Tema:

Guía de mejora bajo la norma ISO/IEC 27002:2013 para la Infraestructura de red LAN de SILAIS – Matagalpa.

Autores:
Br. Álvaro Francisco Muñiz Zapata
Br. Juan Pablo Pravia Valdivia

Tutor:
MSc. Erick Noel Lanzas

Abril, 2019

Índice

Índice de Anexos

I. Introducción

La siguiente guía proporciona los cumplimientos necesarios para optimizar la infraestructura la Red de Área Local (LAN) en el Sistema Local de Atención Integral (SILAIS - Matagalpa). bajo la norma ISO/IEC 27002:2013, la cual es un manual de buenas prácticas para la seguridad de la información, esto se llevó a cabo bajo las técnicas de recolección de información ya antes mencionadas, concluyendo así que la infraestructura de la red, posee un déficit de estructuración y diseño en cuanto al beneficio de la seguridad de la información.

Esta guía muestra los principales problemas encontrados, y como es el estado actual la Red de Área Local (LAN).

Primordialmente esta guía propone soluciones para mitigar y disminuir los riesgos de la información que viaja dentro de la infraestructura la Red de Área Local (LAN).

II. Resumen ejecutivo

La investigación muestra el estado actual infraestructura la Red de Área Local (LAN) para dar a conocer una guía de mejoras y buenas prácticas, en pro de la información en el Sistema Local de Atención Integral (SILAIS-MATAGALPA), bajo la norma ISO/IEC 27002:2013, periodo 2019.

La información más relevante se obtuvo gracias a los instrumentos aplicados al responsable de informática y a la observación precisa y detallada pertinentemente.

En base al estudio realizado concluimos:

1. La Red de Área Local (LAN), en el Sistema Local de Atención Integral (SILAIS-MATAGALPA), no está estructurada bajo ningún tipo de normas de buenas prácticas en pro de la seguridad de la información.

2. Existe un alto déficit de cumplimiento de la normativa ISO 27002-2013.

Esto se representará en los instrumentos que a continuación podrán encontrar dentro de esta guía, como auditores esperamos que la gerencia de SILAIS- MATAGALPA, y el encargado de informática, opten por tomar en cuenta nuestras sugerencias.

III. Alcance del estudio realizado

Los criterios de la infraestructura de red que se tomaron en cuenta son los siguientes:

- Infraestructura física (dispositivos de red, medios de transmisión, estaciones de trabajo, políticas de seguridad físicas).
- Infraestructura lógica (servidores, direccionamiento IP, servicios de red, amenazas lógicas, políticas de seguridad lógicas)
- Tipos de Redes.

IV. Objetivos de la guía

General:

- Proponer a la gerencia y al encargado de informática, soluciones a la Red de Área Local (LAN), en el Sistema Local de Atención Integral (SILAIS-MATAGALPA), bajo los estándares y controles de seguridad de la normativa ISO/IEC 27002:2013, periodo 2019.

Específicos:

1. Elaborar el cumplimiento la norma ISO 27002-2013 en el Sistema Local de Atención Integral (SILAIS-MATAGALPA).

2. Mostrar los principales hallazgos y proponer las debidas recomendaciones para la seguridad de la información en la Red de Área Local (LAN).

..

V. Metodología de la guía

El objetivo de esta guía es mostrar las principales problemáticas de la infraestructura de red en SILAIS-MATAGALPA, y así sugerir posibles soluciones, esta investigación se basó bajo los estándares y controles de seguridad de la normativa ISO/IEC 27002:2013.

Los estándares y controles de seguridad de la normativa ISO/IEC 27002:2013, aplicados son los siguientes:

ISOIEC 27002:2013 consta de 14 dominios:

1. Políticas de seguridad
2. Aspectos organizativos de la seguridad de la información
3. Seguridad ligada a los recursos humanos
4. Gestión de activos
5. Control de acceso
6. Cifrado
7. Seguridad Física y ambiental
8. Seguridad operativa
9. Seguridad en las telecomunicaciones
10. Adquisición, desarrollo y mantenimiento de los sistemas de información.
11. Relaciones con suministradores
12. Gestión de incidentes en la seguridad de la información
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio
14. Cumplimiento

De la normativa ISO únicamente se hizo uso de 12 dominios para esta investigación:

1. Políticas de seguridad
2. Aspectos organizativos de la seguridad de la información
3. Seguridad ligada a los recursos humanos
4. Gestión de activos
5. Control de acceso
6. Cifrado
7. Seguridad Física y ambiental
8. Seguridad operativa
9. Seguridad en las telecomunicaciones
10. Relaciones con suministradores
11. Gestión de incidentes en la seguridad de la información
12. Aspectos de seguridad de la información en la gestión de continuidad del negocio

Los dominios **adquisición desarrollo y mantenimiento de los sistemas de información y cumplimiento, no fueron incluidos en esta investigación,** ya que esta basa en la evaluación de la infraestructura de red, y por motivos de limitaciones del ente gubernamental y por el compromiso del sigilo profesional que nos caracteriza no se evaluaron los dominios ya mencionados.

Cada de los siguientes dominios presentan su objetivo de control y sus controles, de estos se evaluaron los que presentamos a continuación:

1. Políticas de seguridad:

- Directrices de la dirección en seguridad de la información

2. Aspectos organizativos de la seguridad de la información

- Organización interna
    - Segregación de tareas

3. Seguridad ligada a los recursos humanos

4. Gestión de activos:

- Responsabilidades sobre los activos
    - Inventario de activos
    - Uso aceptable de los activos
- Manejo de los soportes de almacenamiento

5. Control de acceso

- Requisitos de negocio para el control de acceso
    - Políticas de control de acceso
    - Control de acceso a las redes y servicios asociados
- Gestión de acceso de usuarios
    - Gestiones altas/bajas en el registro de usuarios

6. Cifrado

- Controles criptográficos
    - Políticas de uso de controles criptográficos

7. Seguridad Física y ambiental

- Áreas seguras
    - Controles físicos de entrada
    - Protección contra amenazas externas y ambientales
    - Seguridad de oficinas y recursos
- Seguridad de los equipos
    - Seguridad del cableado
    - Mantenimiento de los equipos

8. Seguridad en la operativa

- Protección contra código malicioso
    - Controles contra código malicioso
- Copias de seguridad
    - Copias de seguridad de la información
- Consideraciones de las auditorias de los sistemas de información.
    - Controles de auditoria de los sistemas de información

9. Seguridad en las telecomunicaciones

- Gestión de la seguridad en las redes
    - Controles de red
    - Mecanismos de seguridad asociados a servicios de red
    - Segregación de redes
- Intercambio de información con partes externas
    - Políticas y procedimientos de intercambio de información
    - Mensajería electrónica

10. Relaciones con suministradores

- Gestión de la prestación del servicio por suministradores
    - Supervisión y revisión de los servicios prestados por terceros

11. Gestión de incidentes en la seguridad de la información

- Gestión de incidentes de seguridad de la información y mejoras
    - Responsabilidades y procedimientos
    - Notificación de eventos de seguridad de la información
    - Notificación de puntos débiles de la seguridad

12. Aspectos de seguridad de la información en la gestión de continuidad del negocio.

- Continuidad de la seguridad de la información
    - Implantación de la continuidad de la seguridad de la información
- Redundancias
    - Disponibilidad de las instalaciones para el procesamiento de la información.

VI. Hallazgos y recomendaciones

Dominio: Políticas de seguridad.

Objetivo de control: Directrices de la dirección en seguridad de la información.

Control: Conjunto de políticas.

Informe: No se cumple.

En SILAIS-MATAGALPA, no existen políticas de seguridad en la red LAN**.**

Hallazgo	**No se implementan políticas de seguridad.**
Objetivo	
Crear una normativa de políticas de seguridad para el resguardo de la red LAN.	
Recomendación	
Elaborar una guía de procedimientos y restricciones en el manejo de la seguridad de la red LAN y sus dispositivos.	
Riesgos a mitigar	
integridad de los dispositivos y la información.	

Dominio: Aspectos organizativos de la seguridad de la información

Objetivo de control: Organización interna

Control: Segregación de tareas

Informe: No se cumple.

El responsable de informática, no posee un manual de tareas.

Hallazgo	**No están definidas las actividades que el encargado debe de realizar en pro de la seguridad de la información.**
Objetivo	
Realizar tareas que vigilen el pro de la seguridad de la información dentro de la red LAN.	
Recomendación	
Elaborar un marco de trabajo que designe las responsabilidades del responsable de informática, para el resguardo eficaz de la información.	
Riesgos a mitigar	
Incumplimiento de labores por falta de información al responsable de informática.	

Dominio: Seguridad ligada a los recursos humanos.

Objetivo de control: Antes de la contratación.

Control: Investigación de antecedentes.

Informe: No se cumple

No hay investigación de antecedentes de personal.

Hallazgo	**No existen planes de contratación e investigación de antecedentes, al personal de nuevo ingreso.**
Objetivo	
Controlar el ingreso de nuevo personal a las instalaciones.	
Recomendación	
Indagación de antecedentes basadas en referencias profesionales y de carácter de ley.	
Riesgos a mitigar	
Personal no apto para el desempeño laboral. **Manipulación negligente de la información.**	

Dominio: Gestión de activos

Objetivo de control: Responsabilidades sobre los activos

Control: Inventario de activos

Informe: Se cumple parcialmente.

No se realiza inventario de manera detallada.

Hallazgo	**No existen al 100 % archivos o documentos del inventario actual de manera detallada de los dispositivos de TIC.**
Objetivo	
Conocer la existencia real del inventario de equipos.	
Recomendación	
Crear un tiempo definido para realizar inventarios, de la mano de documentos que respalden dicha indagación.	
Riesgos a mitigar	
Extravió de equipos, y desorganización de los activos computacionales dentro de la institución.	

Dominio: Gestión de activos

Objetivo de control: Responsabilidades sobre los activos

Control: Uso aceptable de los activos.

Informe: No se cumple.

No hay ningún procedimiento controle el uso y manejo de los activos de TIC.

Hallazgo	**No existen normas ni procedimientos oficiales para el correcto uso de los equipos computacionales.**
Objetivo	
Crear procesos que eviten el uso inadecuado de dispositivos informáticos.	
Recomendación	
Implementar políticas del buen manejo de los recursos informáticos.	
Riesgos a mitigar	
Daños en los equipos de informática con los que cuenta la institución.	

Dominio: Gestión de activos

Objetivo de control: Responsabilidades sobre los activos

Control: Manejo de los soportes de almacenamiento.

Informe: No se cumple.

No existen procedimientos que resguarden los dispositivos de almacenamiento.

Hallazgo	**No se resguardan los dispositivos de almacenamiento.**
Objetivo	
Proteger medios que puedan guardar cualquier tipo de información de la institución	
Recomendación	
Establecer políticas de protección del resguardo de medios sensibles dentro de la institución.	
Riesgos a mitigar	
Pérdida de información.	

Dominio: Control de acceso.

Objetivo de control: Requisitos de negocio para el control de acceso

Control: Políticas de control de acceso

Informe: No se cumple

No existen políticas que restrinjan el control de acceso.

Hallazgo	**No hay seguridad documentada ni divulgada que impida el control de personal no autorizado a dispositivos informáticos.**
Objetivo	
Implementar normativas de seguridad y de restricciones a los dispositivos de la institución.	
Recomendación	
Definir políticas de control de acceso a los dispositivos de informática.	
Riesgos a mitigar	
Manipulación ajena a los dispositivos, por parte de personal no deseado.	

Dominio: Control de acceso.

Objetivo de control: Requisitos de negocio para el control de acceso

Control: control de acceso a las redes y servicios asociados.

Informe: No se cumple.

No existe vigilancia que garantice el acceso no autorizado a la red.

Hallazgo	**No hay ningún tipo de control en cuanto al resguardo de la red.**
Objetivo	
Monitorear el uso adecuado de la red.	
Recomendación	
Monitorear de manera permanente los accesos y el uso adecuado del tráfico de datos que genera la red.	
Riesgos a mitigar	
Instrucciones a todos los servicios de la red. **Continuidad de servicio.** **Salvaguardar la información de carácter sensible por agentes externos.**	

Dominio:

Objetivo de control: Gestión de acceso de usuarios

Control: Gestión Altas/bajas en el registro de usuarios

Informe: No se cumple.

No hay controles que documenten el alta y baja de los usuarios.

Hallazgo	**No existe una bitácora oficial de los usuarios activos y usuario inactivos.**
Objetivo	
Definir la debida documentación que administre dicho proceso.	
Recomendación	
Crear una bitácora que administre los roles de los diferentes usuarios activos e inactivos del sistema.	
Riesgos a mitigar	
Evitar la pérdida y modificación de información por usuarios no activos dentro de la institución.	

Dominio: Cifrado.

Objetivo de control: Controles criptográficos.

Control: Políticas de uso de Controles criptográficos.

Informe: No se cumple.

No poseen controles criptográficos para la protección de la información.

Hallazgo	**No existen controles criptográficos.**
Objetivo	
Salvaguardar la información.	
Recomendación	
Definir controles criptográficos para la integridad de la información.	
Riesgos a mitigar	
Manipulaciones y alteraciones de la información.	

Dominio: Seguridad Física y ambiental.

Objetivo de control: Áreas seguras.

Control: Controles físicos de entrada.

Informe: Se cumple parcialmente.

Aproximadamente el 75% de los activos de informáticas no se encuentran en áreas seguras.

Hallazgo	**Los controles físicos de entrada son los que brinda la seguridad interna de la Institución**
Objetivo	
Promover la seguridad al 100%.	
Recomendación	
Mejorar controles físicos de accesos a las ubicaciones donde se resguardan los dispositivos de red.	
Riesgos a mitigar	
Daños a los dispositivos informáticos por personal no autorizado.	

Dominio: Seguridad Física y ambiental.

Objetivo de control: Áreas seguras.

Control: Protección contra amenazas externas y ambientales

Informe: Se cumple parcialmente

El 75% de los activos informáticos están protegidos.

Hallazgo	**No existen políticas que prevengan con ubicaciones correctas los accidentes al 100 % de los activos informáticos.**
Objetivo	
Protección de ubicaciones correctas para la continuidad de servicios.	
Recomendación	
Implementar ubicaciones alternas y de respaldos para los dispositivos informáticos.	
Riesgos a mitigar	
Desastres de carácter naturales. **Continuidad de los servicios.** **Pérdida de la información.**	

Dominio: Seguridad Física y ambiental.

Objetivo de control: Seguridad de los equipos.

Control: Seguridad del cableado.

Informe: No se cumple

El cableado está protegido por ningún tipo de aislación alterna.

Hallazgo	**El cableado no está debidamente organizado.**
Objetivo	
Normativas de estructuración del cableado.	
Recomendación	
Aplicar estándares de cableado estructurado.	
Riesgos a mitigar	
Pérdida de la información, y daño de los medios guiados.	

Dominio: Seguridad Física y ambiental.

Objetivo de control: Seguridad de los equipos.

Control: Mantenimiento de los equipos.

Informe: Se cumple.

Se realiza mantenimiento preventivo y correctivo cada 6 meses.

Hallazgo	**Los equipos reciben mantenimiento oportuno.**
Objetivo	
Garantizar la disponibilidad y funcionalidad de los activos informáticos.	
Recomendación	
Continuar con el mantenimiento propuesto.	
Riesgos a mitigar	
Vida útil.	

Dominio: Seguridad en la operativa.

Objetivo de control: Protección contra código malicioso.

Control: Controles contra código malicioso.

Informe: Se cumple de manera correcta.

Se implementa como control contra código malicioso el uso de antivirus.

Hallazgo	**Las máquinas están con licencias activas de antivirus: desde el año em corriente hasta el año 2023.**
Objetivo	
Se garantizar la protección de la información contra código malicioso mediante antivirus.	
Recomendación	
Monitorear el correcto uso de este tipo de medidas.	
Riesgos a mitigar	
Código malicioso (gusanos, troyanos, malware)	

Dominio: Seguridad en la operativa.

Objetivo de control: Copias de seguridad.

Control: Copias de seguridad de la información.

Informe: Se cumple de manera correcta.

Semanal se hacen copias de seguridad de los archivos del servidor y de la información más relevante.

Hallazgo	**Se hacen copias de seguridad periódicamente.**
Objetivo	
Garantizar la seguridad y el buen manejo de la información.	
Recomendación	
Implementar copias de seguridad en varios dispositivos de almacenamiento.	
Riesgos a mitigar	
Pérdida de la información.	

Dominio: Seguridad en la operativa.

Objetivo de control: Consideraciones de las auditorias de los sistemas de Información.

Control: Controles de auditoria de los sistemas de información.

Informe: No se cumple.

No existen controles de auditoria.

Hallazgo	**No se realizan auditorías de carácter informático.**
Objetivo	
Minimizar las debilidades de los procesos informáticos.	
Recomendación	
Planificar auditorias en un tiempo promedio, para vigilar los procesos informáticos.	
Riesgos a mitigar	
Aumento de debilidades en los procesos de TI.	

Dominio: Seguridad en las telecomunicaciones.

Objetivo de control: Gestión de la seguridad en las redes.

Control: Controles de red.

Informe: No se cumple.

No existe ningún tipo de vigilancia y monitoreo de la red LAN.

Hallazgo	**No se monitorea la eficiencia de la red LAN.**
Objetivo	
Aplicar estándares de seguridad a la red.	
Recomendación	
Implementar herramientas de monitoreo de red.	
Riesgos a mitigar	
Instrucciones no deseadas.	

Dominio: Seguridad en las telecomunicaciones.

Objetivo de control: Gestión de la seguridad en las redes.

Control: Mecanismos de seguridad asociados a servicios de red.

Informe: No se cumple.

No se implementa ningún tipo de mecanismo que ayude con la seguridad de la red.

Hallazgo	**No hay ningún procedimiento o agente externo software que, vigile la seguridad de la red.**
Objetivo	
Garantizar la continuidad de servicios de red.	
Recomendación	
Optar por herramientas de seguridad dedicadas a la red.	
Riesgos a mitigar	
Inestabilidad, secuestro de datos, e inutilización de la red.	

Dominio: Seguridad en las telecomunicaciones.

Objetivo de control: Gestión de la seguridad en las redes.

Control: Segregación de redes.

Informe: No se cumple.

No se implementa segmentación de redes en la institución.

Hallazgo	**No se han implementado (VLAN)**
Objetivo	
Aplicar segmentación a la red para su estabilidad.	
Recomendación	
Crear segmentaciones de red por oficinas, dentro de la institución bajo los dispositivos CISCO.	
Riesgos a mitigar	
Saturación de enrutamiento de datos dentro de la red LAN.	

Dominio: Seguridad en las telecomunicaciones

Objetivo de control: Intercambio de información con partes externas.

Control: Políticas y procedimientos de intercambio de información.

Informe: No se cumple.

No se intercambia información con ningún medio o entidad externa.

Hallazgo	**No hay intercambio de información.**
Objetivo	
Garantizar el sigilo de la información gubernamental.	
Recomendación	
Tener en cuenta mecanismos de seguridad de alta tecnología, si se cumpliese en el futuro este proceso.	
Riesgos a mitigar **Integridad de la información.**	

Dominio: Seguridad en las telecomunicaciones

Objetivo de control: Intercambio de información con partes externas.

Control: Mensajería electrónica.

Informe: Se cumple de manera correcta.

Existe seguridad ligada a la mensajería electrónica.

Hallazgo	**Se implementa uso de seguridad en el correo Electrónico, gracias al gestor de correo Mozilla Thunderbird.**
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información que se transmite mediante la mensajería electrónica.	
Recomendación	
Implementar actualizaciones del gestor de correo.	
Riesgos a mitigar	
Uso indebido de la información. **Daño a la seguridad, integridad y confiabilidad de la información.**	

Dominio: Relaciones con suministradores.

Objetivo de control: Gestión de la prestación del servicio por suministradores.

Control: Supervisión y revisión de los servicios prestados por terceros.

Informe: No se cumple.

No se supervisa ningún tipo de relación prestada por los suministradores.

Hallazgo	**No hay monitoreo de servicios prestados por terceros.**
Objetivo	
Velar por el cumplimiento de los servicios prestados.	
Recomendación	
Monitorear el servicio de manera periódica por agentes de servicios externos, ejemplo claro de esto proveedor de ISP.	
Riesgos a mitigar	
Mal servicio de recursos.	

Dominio: Gestión de incidentes en la seguridad de la información.

Objetivo de control: Gestión de incidentes de seguridad de la información y mejoras.

Control: Responsabilidades y procedimientos.

Informe: No se cumple.

No existe control de cualquier incidente de seguridad de la información.

Hallazgo	**No se registran los incidentes que le ocurren a la información.**
Objetivo	
Promover el correcto uso de la información.	
Recomendación	
Crear bitácoras donde se registren los procesos críticos de la seguridad de la información.	
Riesgos a mitigar	
Minimizar a futuro los daños alternos por no atender ocurrencias en el presente.	

Dominio: Gestión de incidentes en la seguridad de la información.
Objetivo de control: Gestión de incidentes de seguridad de la información y mejoras.
Control: Notificación de eventos de seguridad de la información.
Informe: Se cumple parcialmente.
Se notifica a la administración de manera oral los eventos que pueden perjudicar con la continuidad del servicio.

Hallazgo	**No métodos adecuados de comunicación.**
Objetivo	
Extender la continuidad y la protección del servicio.	
Recomendación	
Poseer un medio eficaz y rápido, para notificar eventualidades sobre la detención de los servicios informáticos, y sobre todo documentados.	
Riesgos a mitigar	
Detención de servicios.	

Dominio: Gestión de incidentes en la seguridad de la información.

Objetivo de control: Gestión de incidentes de seguridad de la información y mejoras.

Control: Notificación de puntos débiles de la seguridad.

Informe: No se cumple.

No se documentan las posibles debilidades de la red.

Hallazgo	**No se administra un plan de posibles mejoras a las debilidades de la red.**
Objetivo	
Mantener la disponibilidad de la información y el giro del negocio.	
Recomendación	
Documentar cualquier falla de la seguridad de la información.	
Riesgos a mitigar	
Aumento de daños mayores a la seguridad de la información.	

Dominio: Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Objetivo de control: Continuidad de la seguridad de la información

Control: Implantación de la continuidad de la seguridad de la información.

Informe: No se cumple.

No existen planes de continuidad.

Hallazgo	**No hay un plan elaborado sobre la continuidad de servicio de la seguridad de la información.**
Objetivo	
Garantizar la continuidad de servicio de manera confiable.	
Recomendación	
Se deben de establecer políticas de control, para la continuidad del servicio.	
Riesgos a mitigar	
Detención de los servicios del giro del negocio.	

Dominio: Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Objetivo de control: Redundancias.

Control: Disponibilidad de las instalaciones para el procesamiento de la información.

Informe: No se cumple.

No existe una red redundante.

Hallazgo	**No existen dispositivos que hagan que la red sea redundante.**
Objetivo	
Garantizar continuidad y disponibilidad de la información.	
Recomendación	
Implementar una estructura de red, bajo dispositivos CISCO que le permita la redundancia a la red y así evitar el descontrol y detención de servicios no deseados.	
Riesgos a mitigar	
Detención del giro del negocio.	

VII. Problemáticas relevantes encontradas

Detalle de las problemáticas encontradas

SILAIS-MATAGALPA

Encargado de Informática

Problemática	Causa	Recomendación	Problemática	Causa	Recomendación
1. No se han implementados políticas de seguridad.	No se conoce de la importancia de las políticas de seguridad lógicas y físicas para salvaguardar la información, de SILAIS-MATAGALPA.	Definir las normas y procedimientos de seguridad, destinadas a la protección de la información.	2. No existen procedimientos para la protección de los medios de almacenamiento.	No se ha definido una normativa que proteja los medios extraíbles en donde se almacene la información.	Definir e implementar controles de seguridad que permitan proteger los medios de almacenamiento.

3. No se ha definido un área de TI con dominio de la gerencia.	No hay conciencia acerca de la importancia de poseer el área informática dentro de SILAIS-MATAGALPA.	Concientizar a la dirección de la importancia de tener un área protegida donde se pueda salvaguardar la información.	4. No existen de políticas de control acceso.	No existe normativa que vigile el control no autorizado a la información por personas no deseadas.	Puntualizar y efectuar políticas de control de acceso.
5. No se implementan capacitaciones sobre nuevas tecnologías de las TIC's.	El responsable de informática no Se capacita en pro de la seguridad e integridad de la información.	Elevar el nivel de conocimiento sobre la seguridad, mantenimiento y administración de las tecnologías de la información.	6. No están definidos los controles de acceso a la red.	No se han definido controles de acceso a la red LAN.	Concretar, justificar y efectuar controles de acceso a la red

7. El inventario de los activos informáticos debe de ser realizado por el responsable de informática.	El responsable de informática no se encarga de realizar el inventario de activos.	Otorgar los permisos para la labor de inventario al responsable de informática.	8. Los dispositivos de red que están fuera del área de informática están desprotegidos.	Los dispositivos de red no están ubicados en una determinada área.	Centralizar la todos los dispositivos de la red LAN.

9. No existe la implementación de controles criptográficos	No se conoce de la importancia de la implementación de encriptación de la información.	Definir procedimientos de control de encriptamiento de la información.	10. El cableado no se encuentra estructurado.	Cuando se estructuro la red no se implementaron estándares de estructuración para la red LAN.	Aplicar estándares que permitan la aislación y correcta ubicación de los cables de red.
11. No se supervisan los servicios prestados por	No existe supervisión y revisión de	Se deben supervisar y revisar de	12. No se gestionan los incidentes	No existen procedimientos de manejo y servicios periódicamente la gestión de los incidentes	Se deben definir procedimientos para gestionar

13. No existe un plan de continuidad de seguridad.	No se ha definido un plan de continuidad y recuperación.	Elaborar el plan de continuidad de seguridad de la información, en caso de que se presenten situaciones que pongan en riesgo la misma.	14. No se realizan auditorías a los sistemas de información y la red LAN.	No exi de controles auditoria.	Planificar y establecer controles de auditoria/

15. No se gestionan los eventos de seguridad.	No se evalúan ni clasifican los eventos e incidentes de seguridad.	Gestionar los eventos de seguridad y clasificarlos según su magnitud, con el fin de poder tomar decisiones acertadas acerca de cómo mitigar los incidentes.	16. No existe monitoreo y no se registran los eventos de la seguridad.	No se han implementado herramientas de monitoreo.	Aplicar herramientas que ayuden al monitoreo de seguridad.

17. No existe monitoreo de red.	No se implementan controles de red.	Implementar herramientas que permitan el monitoreo de la red LAN.	18. No se implementan redes de área local virtuales (VLAN).	No se han implementados dispositivos que permitan la segmentación de redes.	Adquirir implementar que la de las dispositivos permitan necesidades segmentación redes de servicio según

Evaluadores

Br. Álvaro F Muñiz Z.

Br. Juan P Pravia V.

Aprobado

ING. OSCAR D MENDOZA.

SILAIS-MATAGALPA.

VIII. Conclusiones de la guía de mejoras

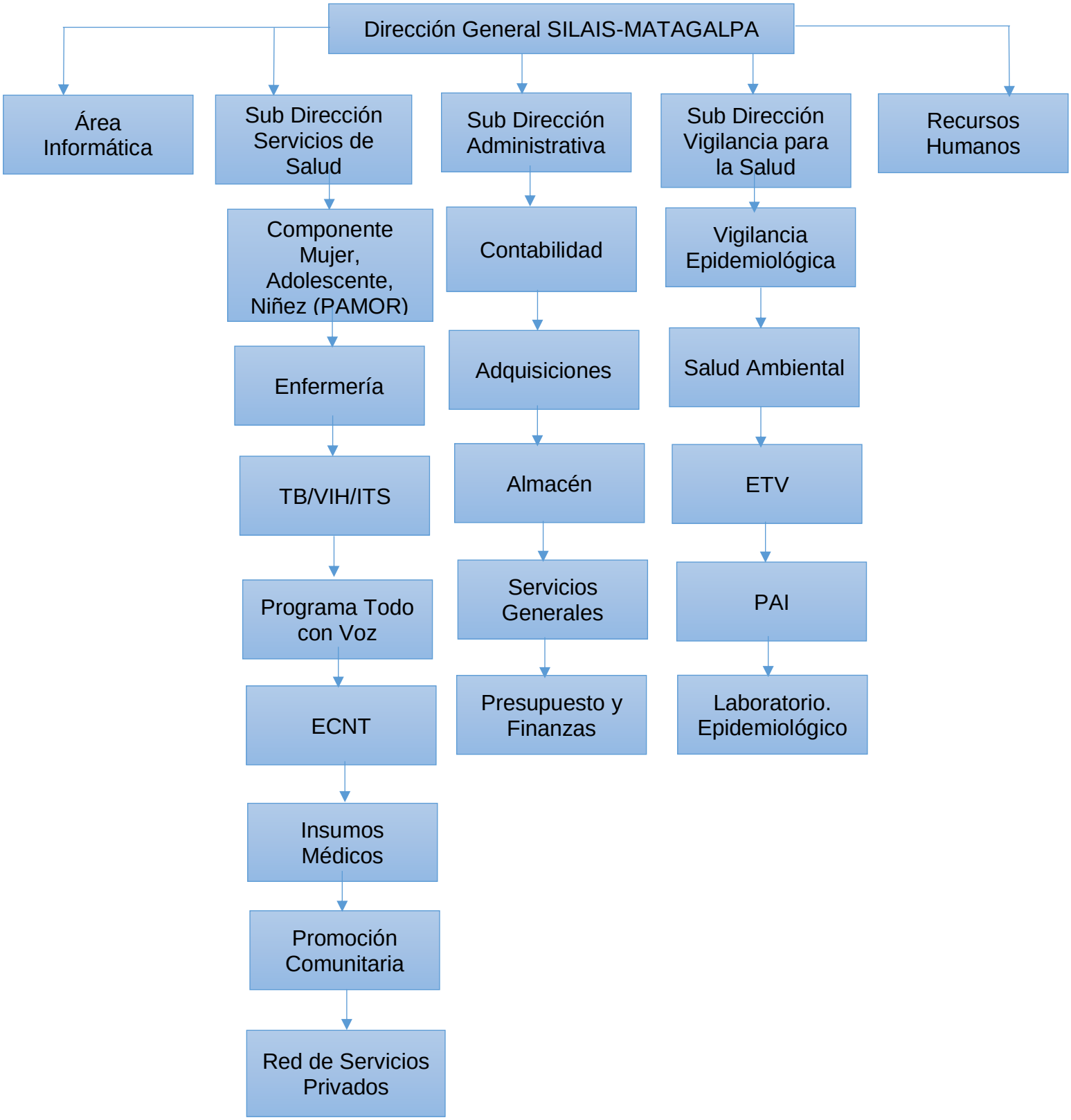
Se propone tomar en cuenta las recomendaciones en SILAIS-MATAGALPA, en beneficio de proyectar un resultado productivo y eficiente de la seguridad de la información.

1. No se cumple, porque no se aplica estándares de calidad. (Anexo tabla 5,6)

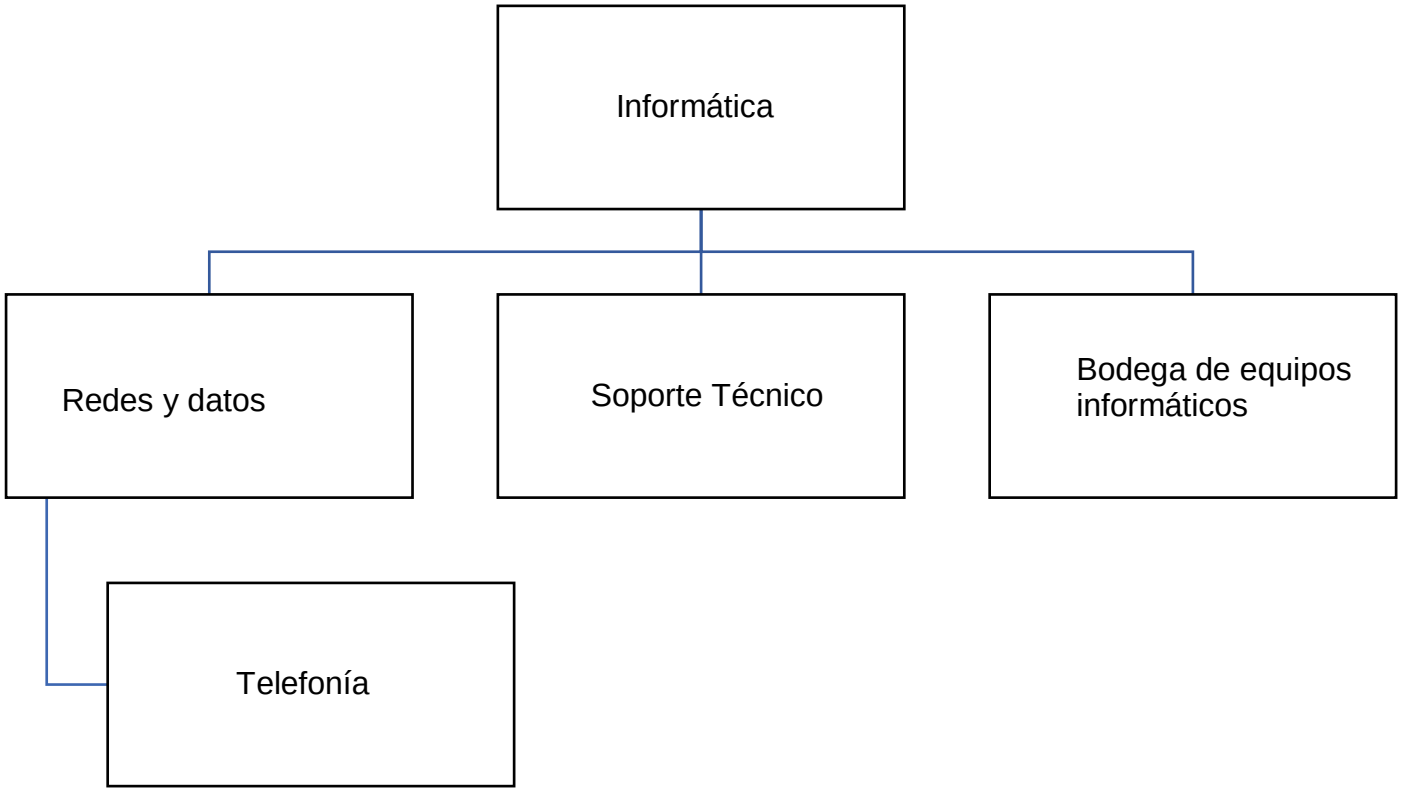
2. A través de los hallazgos encontrados, durante la aplicación de la guía se sugiere mitigar las debilidades y fortalecer la infraestructura de la red LAN, y sus principales problemáticas las cuales se reflejaron en los siguientes dominios de la ISO: políticas de seguridad y control de acceso.

ANEXOS

Anexo 1.
Organigrama propuesto



Anexo 2.
Estructura interna propuesta del área de informática

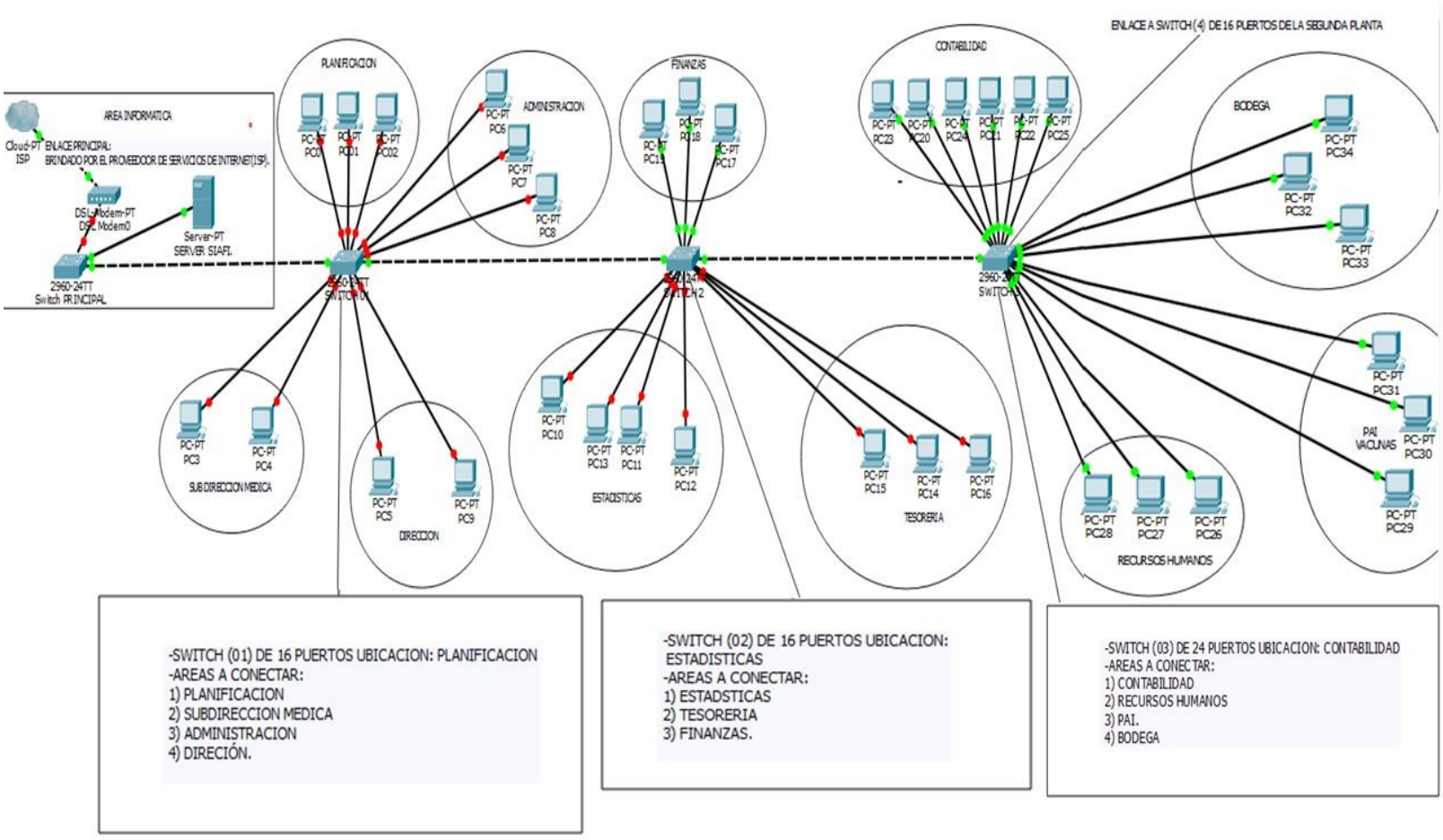


Anexo 3.
Funciones de la estructura propuesta del responsable de Informática

Cargo	Perfil	Funciones
Responsable de informática	Ingeniero en sistemas de computación	**1.** Planear, dirigir y controlar las estrategias de TI. **2.** Gestión y soporte de las TIC. **3.** Gestión de las políticas y normas de seguridad de la información. **4.** Elaboración de inventarios de los recursos
Redes y Datos(telefonía)	Ingeniero en sistemas o computación / Preferible Certificado A CISCO CCNA.	1. Administración, soporte y mantenimiento de la infraestructura de red. 2. Administración de usuarios. 3. Monitoreo de red y sistemas**.**
Soporte técnico	Ingeniero en sistemas o computación.	1. Desarrollo de planes de mantenimiento. 2. Mantenimiento correctivo y preventivo de equipos informáticos.

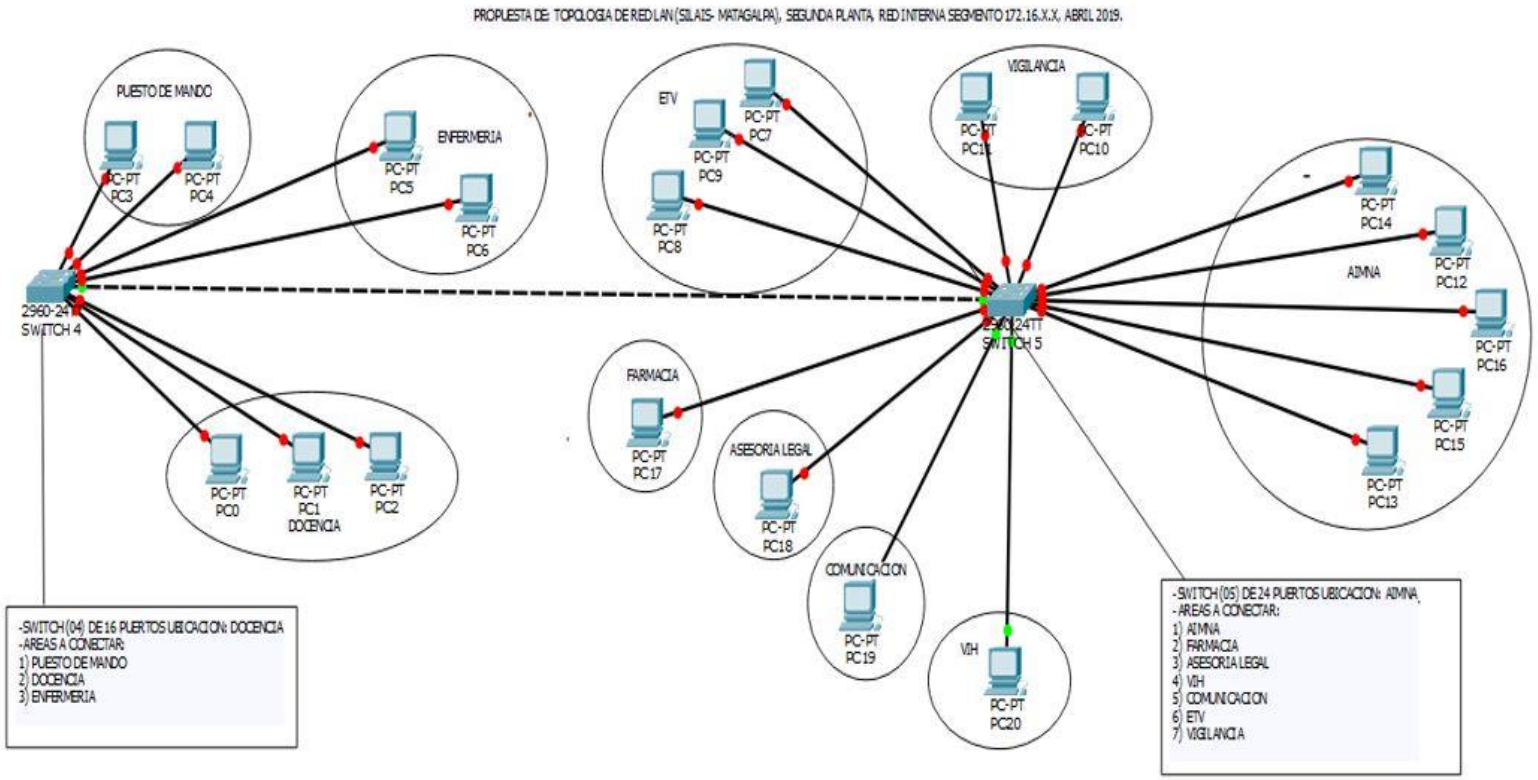
Anexo 4.

Propuesta de topología de red de datos (SILAIS - MATAGALPA), primera planta.



Anexo 4.

Propuesta de topología de red de datos (SILAIS - MATAGALPA), segunda planta.



CAPÍTULO V

5.1. CONCLUSIONES

Se concluye que a través de la aplicación de la normativa ISO 27002:2013, se encontró que en el ámbito de la estructura de la red LAN, SILAIS-MATAGALPA, pone en riesgo la eficiencia y productividad con la comunicación dirigido al sector administrativo de la salud durante el periodo 2019.

1. Siendo la ISO 27002:2013, el principal instrumento se describe que el estado actual de la red LAN en SILAIS-MATAGALPA, no cuenta con políticas de control de accesos, y políticas de seguridad.

2. Tomando en cuenta como instrumento principal la ISO 27002:2013, se identificó que el estado de la infraestructura de la red LAN en SILAIS-MATAGALPA, muestra un alto grado de deficiencia en su seguridad operativa.

3. Las mejoras, sobre las políticas de acceso y seguridad, se establecen a través de sistemas de seguridad y ubicaciones correctas para los diferentes dispositivos de red que impidan el acceso no deseado a terceros, bajo la guía de buenas prácticas que nos ofrece la ISO 27002:2013.

5.2. RECOMENDACIONES

Para mejorar la calidad de la infraestructura de red LAN, y aplicar objetivos de control para la seguridad de la información en, SILAIS-MATAGALPA, proponemos lo siguiente:

A la gerencia:

1) Al aplicar los estándares de la ISO 27002:2013, esta generara las buenas prácticas de uso y manejo en la seguridad de la red LAN del SILAIS-MATAGALPA.

2) Delegar y establecer un área específica de informática en SILAIS-MATAGALPA, y siendo esta quien garantice la calidad de los servicios y procesos de la información.

3) Agendar capacitaciones tecnológicas al responsable de informática.

Al encargado de informática:

- Tomar como referencia la guía propuesta, con la solución de optimizar la infraestructura de la red LAN, SILAIS-MATAGALPA, en bienestar de la seguridad de la información.

5.3. BIBLIOGRAFÍA

ACADEMY, C. N. (2014). *Aspectos Basicos de Networking*. Obtenido de www.netacad.com/es/: www.CISCO_CCNA/Exploration1IntSpanish/index.html

Aroche, S. F. (14 de 02 de 2006). *MAESTROS DEL WEB* . Obtenido de La historia de Internet: http://www.maestrosdelweb.com/internethis/

CCNA Eploration Aspectos basicos de networking. (2014). Obtenido de Comunicación a través de la red : file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de Comunicación a través de la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de La vida en un mundo centrado en la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de La vida en un mundo centrado en la red : file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de La vida en un mundo centrado en la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de La vida en un mundo centrado en la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de La vida en un mundo centrado en la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de La vida en un mundo centrado en la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos basicos de networking.* Obtenido de Aspectos básicos de networking : file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Eploration Aspectos básicos de Networking.* Obtenido de La red como plataforma: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=1

Cisco Systems. (2014). *CCNA Exploration Aspectos basicos de networking.* Obtenido de Redes que respaldan la forma en que vivimos: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=1

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Técnicas de control de acceso al medio: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Comunicacion a través de la red: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Direccionamiento de la red: IPv4.

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Direccionamiento de la red: IPv6:

file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Conmutaciòn y conexiòn inalàmbrica de LAN: file:///C:/CISCO_CCNA/Exploration3IntSpanish/theme/cheetah.html?cid=1300000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Conmutaciòn y conexiòn inalàmbrica de LAN: file:///C:/CISCO_CCNA/Exploration3IntSpanish/theme/cheetah.html?cid=1300000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Aspectos bàsicos de networking.

Cisco Systems. (2014). *CCNA Exploration Aspectos básicos de networking.* Obtenido de Aspectos bàsicos de networking: file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Cisco Systems. (2014). *CCNA Exploration Aspectos Basicos de networking .* Obtenido de Comunicación a través de la red : file:///C:/CISCO_CCNA/Exploration1IntSpanish/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro

Gupta. (2012). Obtenido de El portal de ISO 27002 en Español: http://iso27000.es/iso27002_16.html

Gupta. (2012). Obtenido de El portal de ISO 27002 en Español: http://iso27000.es/iso27002_16.html

ISO. (10 de 2013). *International Organization for Standardization*. Obtenido de https://www.iso.org/standard/54533.html

ISO. (2014). *ISO/IEC 27002:2013* . Obtenido de International Organization for Standardization: https://www.normas-iso.com/iso-27002/

ISO27000.es. (2016). *ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES.* Obtenido de Descargas de ISO27000.es: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Mendoza, O. D. (2019). *Condicion actual de la red LAN SILAIS-MATAGALPA.* Matagalpa.

Tercero&Castillo. (2016). Obtenido de https://farematagalpa.unan.edu.ni/

ANEXOS

Anexo 1.
Operacionalización de variables

Variables	Concepto	Sub variable	Indicadores	Preguntas	Informante	Técnicas
Infraestructura de la red LAN			Definición	¿Conoce el significado red de computadoras? Sí_ No__ ¿Percibe cuáles son los objetivos de la implementación de una red LAN? Sí No	Responsable Informática	Entrevista
	Una evaluación de la infraestructura de red LAN es el proceso por el cual se explora la red para identificar riesgos, asumirlos y minimizarlos mediante técnicas y protocolos de seguridad.	Redes	Arquitectura de red	¿La red disponible es capaz de soportar los servicios que se brindan a través de esta? Sí No ¿La red LAN está siempre disponible? Sí_ No_ ¿Existe un proveedor alternativo de servicio de internet (ISP), en caso que el principal falle? Sí No ¿La infraestructura de red admite a nuevos dispositivos y usuarios en la red? Sí No ¿Se priorizan servicios de streaming en red, por ejemplo, videollamada y telefonía VoIP, etc.? Sí	Responsable Informática	Entrevista

		Tipos de redes	¿Qué tipo de red existe en SILAIS-MATAGALPA? a) LAN b) MAN c) WAN	Responsable Informática	**Entrevista**
		Topología de red	¿Qué topología de red está ¿Implementada en la institución? a) Bus b) Estrella c) Anillo d) Mixta e) Árbol f) Ninguna	Responsable Informática	**Entrevista**
		Elementos de una red	¿Qué servicios ofrece la red de datos de la institución?	Responsable Informática	**Entrevista**
	Calidad de las comunicaciones	Factores Externos	Según s u criterio ¿ la red posee todos los dispositivos necesarios para ofrecer un servicio de calidad?	Responsable Informática	**Entrevista**
		Factores Internos	¿Qué tipo de datos se transportan a t r a v é s d e l a red? (Conexión a base de datos, sitios web, videos, VoIP, etc.)?	Responsable Informática	**Entrevista**
	Infraestructura Física	**Dispositivos de Red**	**¿Con cuántos dispositivos de red cuenta la institución?**	**Responsable Informática**	**Entrevista**

			Cableados o Guiados	¿Qué tipo de cable y categoría utilizan las conexiones de red?	Responsable Informática	**Entrevista**
			Estación de trabajo	¿Con cuantas computadoras cuenta la institución? ¿Todas las computadoras de la institución tiene acceso a la red? Sí_ No_ ¿Se realizan mantenimientos de manera continua a los ordenadores? Sí_ No_ ¿Se encuentran en óptimas condiciones las computadoras? Sí_ No_	Responsable Informática	Entrevista
			Políticas de seguridad Físicas	¿Existen políticas de seguridades físicas implementadas en la infraestructura de red? Sí_ No_ ¿Existen planes de contingencia para la recuperación de la información en caso de que ocurra un desastre? Sí_ No_ ¿La institución cuenta con procedimientos de seguridad física de la red que permitan prevenir la manipulación y acceso no autorizado de la de la información? Si No	Responsable Informática	Entrevista Observación

				¿El personal de informática está en constante capacitación sobre sus funciones? Sí_ No_		
			Amenazas Físicas	¿Se encuentran protegidos los equipos de red dentro de la institución? Sí_ No_ ¿Los dispositivos de red se encuentran climatizados? Sí_ No_ ¿Los dispositivos de red se encuentran debidamente conectados a la fuente eléctrica? Sí_ No_ ¿Existen antecedentes de riesgos de la infraestructura red? Sí_ No_	Responsable Informática	Entrevista Observación

		Infraestructura Lógica	Servidores	¿Qué sistema operativo utiliza el servidor?	Responsable Informática	Entrevista
			Direccionamiento IP	¿Qué rango de direccionamiento IP privado esta implementado en la infraestructura de red? **a)** 10.0.0.0 /8 **b)** 172.16.0.0 /16 **c)** 192.168.1.0 /24	Responsable Informática	Entrevista Observación
			Servicios de Red	¿La red ofrece múltiples servicios?	Responsable Informática	Entrevista
			Segmentación de Red	¿Se implementa segmentación de red? Sí_ No	Responsable Informática	Entrevista
			Ancho de Banda	¿Con cuanto ancho d e banda cuenta la institución? ¿El ancho de banda contratado es suficiente para proporcionar una conexión optima a los usuarios? Si No	Responsable Informática	**Entrevista Observación**
			VPN	¿Actualmente cuenta con VPN? Sí_ No_	Responsable Informática	Entrevista

			Centrales Telefónicas	¿Posee una central telefónica? Sí No ¿Esta cuenta con la suficiente cantidad de terminales telefónicas? Sí No	Responsable Informática	Entrevista
			Políticas de seguridad Lógica	¿Existen políticas de seguridad establecidas en la red?	Responsable Informática	Entrevista
			Amenazas Lógicas	¿La red cuenta con los mecanismos necesarios para prevenir los riesgos lógicos? (Firewalls, antivirus)	Responsable Informática	Entrevista
ISO/IEC 27002:2013	La ISO /IEC 27002:2013 proporciona controles que permiten aplicar buenas prácticas para la seguridad de la información.	ISO/IEC 27002:2013	Concepto	¿Usted conoce acerca de normativas internacionales que ayudan a regir la seguridad de la información? ¿Considera importante implementar normativas internacionales que regulan la seguridad de la información? ¿Conoce, acerca de la Norma ISO/IEC 27002:2013?	Responsable Informática	Entrevista
		Políticas de seguridad	Directrices de la dirección en seguridad de la información.	¿Están definidas las políticas de seguridad de la información en la red de la institución?	Responsable Informática	Entrevista

		Aspectos organizativos de la seguridad de la información	Segregación de tareas de tareas	¿Está definida el área de TI? Si No	Responsable Informática	Entrevista
		Seguridad ligada al recurso humano	Antes de la contratación	¿Se le dieron a conocer cuáles son los términos y condiciones de su empleo? Si No	Responsable Informática	Entrevista

		Gestión de activos	Responsabilidades sobre los activos	¿Existen controles adecuados sobre los activos, para conservar la seguridad de las redes? Si No	Responsable Informática	Entrevista
			Inventario de activos	¿Lleva a cabo el inventario del área de informática? Si No ¿Cada cuánto tiempo realiza dicho inventario?	Responsable Informática	Entrevista
			Uso aceptable de los activos	¿Existen los procedimientos para regular el uso adecuado de los activos del área de redes? Si No	Responsable Informática	Entrevista
			Manejo de los soportes el almacenamiento	¿Existen controles y procedimientos que se aplican para proteger los medios de almacenamiento? Si No	Responsable Informática	Entrevista
		Control de acceso	Requisitos de negocio para el control de acceso	¿Se controla el acceso a la información? Si No	Responsable Informática	Entrevista
			Política de control de accesos	¿Se encuentran establecidas las políticas de control de acceso? Si No	Responsable Informática	Entrevista

			Gestión de altas/bajas registro de usuarios	¿Se cuenta con procedimientos formales, al momento de dar de alta o baja a un usuario de la red?	Responsable Informática	Entrevista
		Cifrado	Políticas de uso de controles criptográficos	¿Existen políticas de seguridad que regulen el uso de cifrado?	Responsable Informática	Entrevista

		Seguridad Física y ambiental	Controles físicos de entrada	¿Existen controles físicos a las áreas donde se encuentran los dispositivos de red? Si No	Responsable Informática	Entrevista
			Protección contra amenazas externas y ambientales	¿Los dispositivos de red y los servidores se encuentran en un lugar capaz de soportar desastres naturales y evitar incidentes malintencionados a la información? Si No	Responsable Informática	Entrevista
			Seguridad de oficinas y recursos	¿Se implementa medidas de seguridad de acceso físico a las oficinas?	Responsable Informática	Entrevista
			Seguridad de los equipos	¿Los dispositivos de red e Intermediarios como conmutadores se encuentran ubicados en un RACK, el cual evite la manipulación no autorizado?	Responsable Informática	Entrevista
			Seguridad del cableado	¿Los cables de red están aislados de otros cables? Si No	Responsable Informática	Entrevista
			Mantenimiento de los equipos	¿Qué tipo de mantenimiento se les suministra a los dispositivos de red y al servidor? (Preventivos y correctivos)	Responsable Informática	Entrevista

		Seguridad operativa	Controles contra código malicioso	¿Existen controles de seguridad ante malware? Si No	Responsable informática	Entrevista
			Copias de seguridad de la información	¿Realiza copias de seguridad del servidor? Si No ¿Las copias de seguridad son guardadas en un lugar seguro? Si No	Responsable informática	Entrevista

			Consideraciones de las auditorías de los sistemas de información	¿Se realizan auditorías de sistemas de información y redes? Si No	Responsable informática	Entrevista
		Seguridad de las telecomunicaciones	Controles de red	¿Hace uso de herramientas de monitoreo de red? Si No	Responsable informática	Entrevista
			Mecanismos de seguridad asociados a servicios de red	¿Implementa mecanismos de seguridad emplea para proteger los servicios que ofrece la red? Si No	Responsable informática	Entrevista
			Segregación de redes.	¿Existen redes virtuales locales en la institución? Si No	Responsable informática	Entrevista
			Intercambio de información con partes externas	¿Intercambia información con entidades externas? Si No	Responsable informática	Entrevista

			Políticas y procedimientos de intercambio de información	¿Utiliza políticas y procedimientos para realizar intercambios de información? Si No	Responsable informática	Entrevista
			Mensajería electrónica	¿Utiliza mecanismos de seguridad para enviar información, por ejemplo: ¿el uso de correo electrónico? Si No	Responsable informática	Entrevista
		Relaciones con Suministradores.	Supervisión y revisión de los servicios prestados por terceros	¿La institución monitorea el cumplimiento prestado por los proveedores de servicio de internet (ISP)? Si No	Responsable informática	Entrevista

		Gestión de incidentes en la seguridad de la información	Responsabilidades y procedimientos	¿Están establecidos los procedimientos para dar respuesta a los incidentes de seguridad de la información de la red? Si No	Responsable informática	Entrevista
			Notificación de eventos de seguridad de la información	¿Se notifica a la administración de los eventos asociados a la seguridad de la información? Si No	Responsable informática	Entrevista
			Notificación de puntos débiles de la seguridad	¿Se documenta y notifica a la administración las sospechas de puntos débiles en la seguridad de la información que viaja por la red? Si No	Responsable informática	Entrevista

		Aspecto de seguridad de la información en la gestión de la continuidad de negocio	Continuidad de la seguridad de la información	¿Existe un plan de continuidad y recuperación de los procesos de seguridad de la información ante desastres? Si No	Responsable informática	
			Redundancias	¿Existen dispositivos de red que permitan la redundancia en la infraestructura de red? Si No	Responsable informática	Entrevista

Anexo 2.
Entrevista dirigida a responsable de Informática SILAIS - Matagalpa

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida al responsable de informática de SILAIS-MATAGALPA.

El objetivo de esta entrevista es con el fin de recaudar información para determinar la condición actual de la infraestructura de red LAN, de SILAIS-MATAGALPA.

Redes

- **Definición**

1. ¿conoce el significado red de computadoras?

Sí ○ No ○

2. ¿Percibe cuáles son los objetivos de la implementación de una red LAN?

Sí ○ No ○

- **Arquitectura de Red**

1. ¿La de red disponible en SILAIS- ¿MATAGALPA, es capaz de soportar de los servicios que se brindan a través de esta?

Sí ○ No ○

2. ¿La red LAN está siempre disponible?

Sí ○ No ○

3. ¿Existe un proveedor alternativo de servicio de internet (ISP), en caso que el principal falle?

Sí ○ No ○

4. ¿La infraestructura de red admite a nuevos dispositivos y usuarios en la red?

Sí ○ No ○

5. ¿Se priorizan servicios de streaming en la red, por ejemplo: videollamadas telefonía VoIP, ¿etc.?

6. ¿Existen herramientas e instrucciones aplicados para mitigar las fallas de seguridad en la red LAN?

Sí ○ No ○

- **Tipos de Redes**

1. ¿Qué tipo de red existe en SILAIS-MATAGALPA
   a) LAN
   b) MAN
   c) WAN

- **Topología de Red**

1. ¿Qué topología de red está implementada en la institución?
   a) Bus

b) Estrella

c) Anillo

d) Mixta

e) Árbol

f) Ninguna

Elementos de una Red

1. ¿Qué servicio ofrece la red de datos de la institución?

Calidad de las Comunicaciones

- **Factores Externos**

1. Según su criterio, ¿La red posee todos los dispositivos necesarios para ofrecer un servicio de calidad?

- **Factores Internos**

1. ¿Qué tipo de datos se transportan a través de la red? (Conexión a base de datos, sitios web, videos, VoIP etc.)?

Infraestructura Física

- **Dispositivos de Red**

1. ¿Con cuántos dispositivos de red cuenta la institución?

- **Cableados o Guiados**

1. ¿Qué tipo de cable y categoría utilizan las conexiones de red?

- **Estación de trabajo**

1. ¿Con cuántas computadoras cuenta la institución?

2. ¿Todas las computadoras de la institución tienen acceso a la red?

Sí ○ No ○

3. ¿Se realizan mantenimientos de manera regular a las computadoras?

Sí ○ No ○

4. ¿Se encuentran en óptimas condiciones las computadoras?

Sí ○ No ○

- **Políticas de Seguridad Físicas**

1. ¿Existen políticas de seguridad físicas implementadas en la infraestructura de red?

Sí ○ No ○

2. ¿Existen planes de contingencia para la recuperación de la información en caso de que ocurra un desastre?

Sí ○ No ○

- **Amenazas Físicas**

1. ¿La infraestructura de red cuenta con procedimientos de seguridad física que permitan prevenir la manipulación y acceso no autorizado de la información?

Sí ○ No ○

.2. ¿Se encuentran protegidos los equipos de red dentro de la institución?

Sí ○ No ○

1. ¿Los dispositivos de red se encuentran climatizados?

4. ¿Los dispositivos de red se encuentran debidamente conectados a la fuente eléctrica?

5. ¿Existen antecedentes de riesgos y amenazas hacia la seguridad física de la infraestructura red?

Sí ○ No ○

Infraestructura Lógica

- **Servidores**

1. ¿Qué sistema operativo utiliza el servidor?

- **Direccionamiento IP**

1. ¿Qué rango de direccionamiento IP privado esta implementado en la infraestructura de red?
   - **d)** 10.0.0.0 /8
   - **e)** 172.16.0.0 /16
   - **f)** 192.168.1.0 /24

Servicios de Red

1. ¿la red ofrece múltiples servicios?

- **Segmentación de Red**

1. ¿Se implementa segmentación de red?

Sí ○ No ○

Ancho de Banda

1. ¿Con cuanto ancho de banda cuenta la institución?

2. ¿El ancho de banda contratado es suficiente para proporcionar una conexión óptima a los usuarios?

Sí ○ No ○

VPN

1. ¿Actualmente se cuenta con redes virtuales privadas?

Sí ○ No ○

- **Centrales Telefónicas**

1. ¿Existe una central telefónica?

Sí ○ No ○

1. ¿Se cuenta con la suficiente cantidad de terminales telefónicas para proveer el servicio a los usuarios?

Sí ○ No ○

1. ¿Están establecidas políticas de seguridad lógica en la red?

Sí ○ No ○

Amenazas Lógicas

1. ¿La red cuenta con los mecanismos necesarios para prevenir los riesgos lógicos? (Firewalls, antivirus)

Anexo 3

Entrevista dirigida a responsable de Informática SILAIS – Matagalpa

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida al responsable de informática de

SILAIS-MATAGALPA.

El objetivo de esta entrevista es con el fin de recaudar información para determinar si se poseen conocimientos acerca de los objetivos y dominios de control que comprende el **Estándar ISO/IEC 27002-2013,** y de esta manera verificar si estos son aplicados en la infraestructura de red lógica y física de SILAIS-MATAGALPA.

ISO/IEC 27002:2013

Definición

1. ¿Usted conoce acerca de normativas internacionales que ayudan a regir la seguridad de la información?

   Sí ○ No ○

2. ¿Considera importante implementar normativas internacionales que regulan la seguridad de la información?

   Sí ○ No ○

3. ¿Conoce acerca de la Norma ISO/IEC 27002:2013?

   Sí ○ No ○

Políticas de Seguridad

- **Directrices de la dirección en seguridad de la información.**

1. ¿Están definidas las políticas de seguridad en la red de la institución?

Sí ○ No ○

Aspectos Organizativos de la Seguridad de la Información

- **Organización Interna**

✓**Segregación de Tareas**

1. ¿Está definida el área de TI?

Sí ○ No ○

Seguridad Ligada al Recurso Humano

- **Antes de la Contratación**

1. ¿Se le dieron a conocer cuáles son los términos y condiciones del empleo?

Sí ○ No ○

Gestión de Activos

- **Responsabilidades sobre los Activos**

1. ¿existen controles adecuados sobre los activos para conservar la seguridad de las redes?

Sí ○ No ○

✓ **Inventario de Activos**

1. ¿Lleva a cabo el inventario de activos del área de informática?

Sí ○ No ○

2. ¿Cada cuánto tiempo se realiza dicho inventario?

✓ **Uso aceptable de los Activos**

1. ¿Existen los procedimientos para regular el uso adecuado de los activos del área de redes?

Sí ○ No ○

Manejo de los Soportes de Almacenamiento

1. ¿Existen controles y procedimientos que se aplican para proteger los medios de almacenamiento?

Sí ○ No ○

Control de Acceso

Requisitos de Negocio para el Control de Acceso

1. ¿Se controla el acceso a la información?

Sí ○ No ○

✓ **Política de Control de Accesos**

1. ¿Se encuentran establecidas las políticas de control de acceso?

Sí ○ No ○

Gestión de Acceso de Usuarios

✓ **Gestión de altas/bajas en el Registro de Usuarios**

1. ¿Se cuenta con procedimientos formales al momento de dar de alta o baja a un usuario de la red?

Sí ○ No ○

Cifrado

Controles Criptográficos

Políticas de Uso de Controles Criptográficos

1. ¿Existen políticas de seguridad que regulen el uso de cifrado?

Sí ○ No ○

Seguridad física y ambiental

Áreas Seguras

Controles Físicos de Entrada

1. ¿Existen medidas de controles físicos aplicadas a las áreas donde se encuentran los dispositivos de red?

Sí ○ No ○

Protección contra Amenazas Externas y Ambientales

1. ¿Los dispositivos de red y el servidor se encuentran en un lugar capaz de soportar desastres naturales y evitar incidentes malintencionados a la información?

Sí ○ No ○

Seguridad de Oficinas y Recursos

1. ¿Se implementan medidas de seguridad de acceso físico a las oficinas?

Seguridad de los Equipos

1. ¿Los dispositivos de red intermediarios como conmutadores se encuentran ubicados en un rack, el cual evite la manipulación no autorizada?✓

✓ **Seguridad del Cableado**

1. ¿Los cables de red están aislados de otros cables?

Sí ○ No ○

✓ **Mantenimiento de los Equipos**

1. ¿Qué tipo de mantenimiento se les suministra a los dispositivos de red y al servidor? (Preventivos y correctivos)

Anexo 4.

Entrevista dirigida a responsable de Informática SILAIS – Matagalpa

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida al responsable de informática de SILAIS-MATAGALPA.

El objetivo de esta entrevista es con el fin de recaudar información para determinar si se poseen conocimientos acerca de los objetivos y dominios de control que comprende el **Estándar ISO/IEC 27002-2013,** y de esta manera verificar si estos son aplicados en la infraestructura de red lógica y física de SILAIS-MATAGALPA

Seguridad en la operativa

Protección contra código malicioso

Controles contra código malicioso

1. ¿Existen controles de seguridad que permitan la detección y mitigación de malware?

Sí ○ No ○

Copias de seguridad

✓ **Copias de seguridad de la información**

1. ¿Realiza copias de seguridad del servidor y la información vital de la institución, y cada cuánto?

2. ¿Las copias de seguridad son guardadas en un lugar seguro?

Sí ○ No ○

Consideraciones de las auditorías de los sistemas de información

Controles de auditoria de los sistemas de información

1. ¿Se realizan auditorías de sistemas de información y redes?

Sí ○ No ○

Seguridad de las telecomunicaciones

Gestión de la seguridad en las redes

Controles de red

1. ¿Hace uso de herramientas de monitoreo de red?

Sí ○ No ○

✓ **Mecanismos de seguridad asociados a servicios de red**

1. ¿implementa mecanismos de seguridad para proteger los servicios que ofrece la red?

Sí ○ No ○

✓ **Segregación de Redes**

1. ¿Existen redes virtuales locales en la institución?

Sí ○ No ○

Intercambio de información con partes externas

1. ¿intercambia información con entidades externas?

Sí ○ No ○

Políticas y procedimientos de intercambio de información

1. ¿Utiliza políticas y procedimientos para realizar intercambios de información?

Sí ○ No ○

✓ **Mensajería electrónica**

1. ¿utiliza mecanismos de seguridad para enviar información, por ejemplo: el uso de correo electrónico?

Relaciones con Suministradores

Gestión de la prestación del servicio por suministradores

Supervisión y revisión de los servicios prestados por terceros

1. ¿La institución monitorea el cumplimiento prestado por los proveedores de servicio de internet (ISP)?

Sí ○ No ○

Anexo 5

Entrevista dirigida a responsable de Informática SILAIS – Matagalpa

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida al responsable de informática de

SILAIS-MATAGALPA.

El objetivo de esta entrevista es con el fin de recaudar información para determinar si se poseen conocimientos acerca de los objetivos y dominios de control que comprende el **Estándar ISO/IEC 27002-2013,** y de esta manera verificar si estos son aplicados en la infraestructura de red lógica y física de SILAIS-MATAGALPA.

Gestión de incidentes en la seguridad de la información
Gestión de incidentes de seguridad de la información y mejoras.

✓ **Responsabilidades y procedimientos**

1. ¿Están establecidos los procedimientos para dar respuesta a los incidentes de seguridad de la información de la red?

Sí ○ No ○

✓ **Notificación de eventos de seguridad de la información**

1. ¿Se notifica a la administración de los eventos asociados a la seguridad de la información?

Sí ○ No ○

✓ **Notificación de puntos débiles de la seguridad**

1. ¿Se documenta y notifica a la administración la sospecha de puntos débiles en la seguridad de la información que viaja por la red?

Sí ○ No ○

Aspecto de seguridad de la información en la gestión de la continuidad de negocio

Continuidad de la seguridad de la información

Continuidad de la seguridad de la información

1 ¿Existe un plan de continuidad y recuperación de los procesos de seguridad de la información ante desastres?

Sí ○ No ○

Redundancias

1. ¿Existen dispositivos de red que permitan la redundancia en la infraestructura de red?

Sí ○ No ○

Anexo 6.

Observación de Infraestructura de Red SILAIS - Matagalpa

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de observación dirigida aplicada en SILAIS-MATAGALPA

Indicador	Observación	Detalles
Tipos de redes	Tipos de redes existes en SILAIS-MATAGALPA.	La única red implementada en SILAIS-MATAGALPA, es una red LAN interna (INTRANET)
Topología de red	Topología de red implementada en la institución	No existe documentación de la topología actual, pero mediante la observación se pudo determinar que la topología implementada es de MIXTA.
Elementos de una red	Medio de trasmisión de datos usados en la institución	El medio de trasmisión usado en la red LAN, a través de medios guiados.

Factores Internos	Monitoreo en el tráfico de red	No se realiza monitoreo de red en la institución
Dispositivos de Red	Dispositivos de red actuales	Se observó que los dispositivos de red utilizados están desfasados
Cableado	Cable y categoría utilizado	En la red principal se usa cable de par trenzado (UTP) de categoría 5e.
Políticas de seguridad Físicas	Políticas de seguridad físicas implementadas en la infraestructura de red	No existen políticas de seguridad
Amenazas Físicas	Protección de equipos fuera del área de informática	Se determinó que los dispositivos de red ubicados en las diferentes áreas no poseen ninguna protección contra acceso y manipulación no autorizada
	Climatización de equipos	Únicamente los equipos que están en oficinas con aire acondicionados están protegidos.
	Dispositivos de red conectados a fuentes de respaldo de energía eléctrica	No todos los dispositivos de red cuentan con baterías o estabilizadores

Ancho de Banda	Ancho de banda en las redes	Se realizaron pruebas de velocidad con un total de 10 MB no Sincrónicos.
Centrales Telefónicas	Central telefónica	Se cuenta con una central telefónica (Grandstream).

Amenazas Lógicas	Mecanismos de prevención para amenazas lógicas	El único mecanismo de prevención utilizado contra amenazas lógicas es el antivirus.
Asignación de responsabilidades.	Área de TI	En el organigrama de la institución no se refleja un área de TI definida.
Áreas seguras	Área de dispositivos protegida ante el acceso no autorizado	Los dispositivos que están no están protegidos ante acceso no autorizado.
Seguridad de oficinas y recursos	Medidas de seguridad de acceso físico implementada en las diferentes oficinas.	El único control físico usado son las puertas para acceso.

Protección contra amenazas externas y ambientales	Área capaz de proteger los dispositivos contra desastres naturales y evitar incidentes malintencionados a la información	No existen áreas debidamente estructuradas capaces de soportar incidentes que pongan en riesgo la seguridad de los dispositivos de red LAN y la información.
Seguridad de los equipos	Dispositivos intermediarios ubicados en rack	El rack de datos esta no está centralizado
Seguridad del cableado	Cables canaleteados	El cableado no está estructurado,

Anexo 7.
Matriz de resultado de las entrevistas

Matriz de resultado de las entrevistas realizada al responsable de informática

Indicadores	**Responsable de informática**
¿Conoce el significado red de computadores?	SI
¿Percibe cuáles son los objetivos de la implementación de una red LAN?	SI
¿La red disponible es capaz de soportar los servicios que se brindan a través de esta?	SI
¿La conexión a internet está siempre disponible?	SI
¿Existe un proveedor alternativo de servicio de internet (ISP), en caso que el principal falle?	NO
¿La infraestructura de red admite a nuevos dispositivos y usuarios en la red?	SI
¿Se priorizan servicios de streaming en red, por ejemplo, videollamada y telefonía VoIP, etc.?	No, el tráfico de datos trabaja por sí solo.
¿Existen herramientas e instrucciones aplicados para mitigar las fallas de seguridad en la red LAN?	NO
¿Qué tipo de red existe en **SILAIS-MATAGALPA**? a) LAN b) MAN c) WAN	Una red LAN, solo nos conectamos internamente, no compartimos información con agentes externos.
¿Qué topología de red está implementada en la institución? a) Bus b) Estrella c) Anillo d) Mixta e) Árbol	Desconozco, cuando yo entré a trabajar ya estaba todo implementado y no existe ninguna documentación.

f) Ninguna ¿Qué servicios ofrece la red de datos de la institución?	
Según su criterio ¿la red posee todos los dispositivos necesarios para ofrecer un servicio de calidad?	No lo sé, desconozco el tipo de topología
¿Qué tipo de datos se transportan a través de la red? (Conexión a base de datos, sitios web, videos, VoIP, etc.)?	Llamadas VoIP, sitios web y videos.
¿Con cuántos dispositivos de red cuenta la institución?	4 Routers, 10 Switches.
¿Qué tipo de cable y categoría utilizan las conexiones de red?	UTP categoría 5e.

¿Con cuantas computadoras cuenta la institución?	72 computadoras de escritorio y dos portátiles.
¿Todas las computadoras de la institución tienen acceso a la red?	SI
¿Se realizan mantenimientos de manera regular a los ordenadores?	SI
¿Se encuentran en óptimas condiciones las computadoras?	SI
¿Existen políticas de seguridad físicas implementadas en la infraestructura de red?	NO
¿Existen planes de contingencia para la recuperación de la información en caso de que ocurra un desastre?	NO
¿La infraestructura de red cuenta con procedimientos de seguridad física de la red que permitan prevenir la manipulación y acceso no autorizado de la información?	NO
¿El personal de informática está en constante capacitación sobre las reglas y procedimientos establecidos sobre la seguridad física de la red?	NO

¿Se encuentran protegidos los equipos de red dentro de la institución?	NO
¿Los dispositivos de red se encuentran climatizados?	Algunos, solo los que están dentro de oficinas que tienen aire acondicionado.
¿Los dispositivos de red se encuentran debidamente conectados a la fuente eléctrica?	No todos porque algunos no cuentan con estabilizadores y baterías.
¿Existen antecedentes de riesgos y amenazas hacia la seguridad física de la infraestructura red?	NO
¿Qué sistema operativo utiliza el servidor?	Windows server 2003 para el servidor del sistema SIAFI.
¿Qué rango de direccionamiento IP privado esta implementado en la infraestructura de red? **a)** 10.0.0.0 /8 **b)** 172.16.0.0 /16 **c)** 192.168.1.0 /24	**b)** 172.16.0.0 /16
¿La red ofrece múltiples servicios?	Mensajería interna, bases de datos, impresiones en red y llamadas.
¿Se implementan segmentación de red?	NO
¿Con cuanto ancho de banda cuenta la institución? ¿El ancho de banda contratado es suficiente para proporcionar una conexión optima a los usuarios? Si No	10 Mb con claro SI
¿Actualmente se cuenta con redes virtuales privadas?	NO
¿Existe una central telefónica?	SI

¿Se cuenta con la suficiente cantidad de terminales telefónicas para proveer el servicio a los usuarios?	SI
¿Están establecidas políticas de seguridad lógica en la red?	NO
¿La red cuenta con los mecanismos necesarios para prevenir los riesgos lógicos? (Firewalls, antivirus)	Solo se hace uso de antivirus

Anexo 8.
Matriz de resultado de las entrevistas

(Entrevistas ISO/IEC 27002:2013)

Matriz de resultado de las entrevistas realizadas al responsable de informática

Dirigida a: responsable de informática

¿Usted conoce acerca de normativas internacionales que ayudan a regir la seguridad de la información?	NO
¿Considera importante implementar normativas internacionales que regulan la seguridad de la información?	NO
¿Conoce acerca de la Norma ISO/IEC 27002:2013?	NO
¿Están definidas las políticas de seguridad en la red de la institución?	NO
¿Está definida el área de TI?	NO
¿Se le dieron a conocer cuáles son los términos y condiciones del empleo?	NO
¿Existen controles adecuados sobre los activos, para conservar la seguridad de las redes?	NO
¿Lleva a cabo el inventario de activos del área de informática? ¿Cada cuánto tiempo se realiza dicho inventario?	NO Cada año
¿Existen los procedimientos para regular el uso adecuado de los activos del área de redes?	NO
¿Existen controles y procedimientos que se aplican para proteger los medios de almacenamiento?	NO
¿Se controla el acceso a la información?	NO

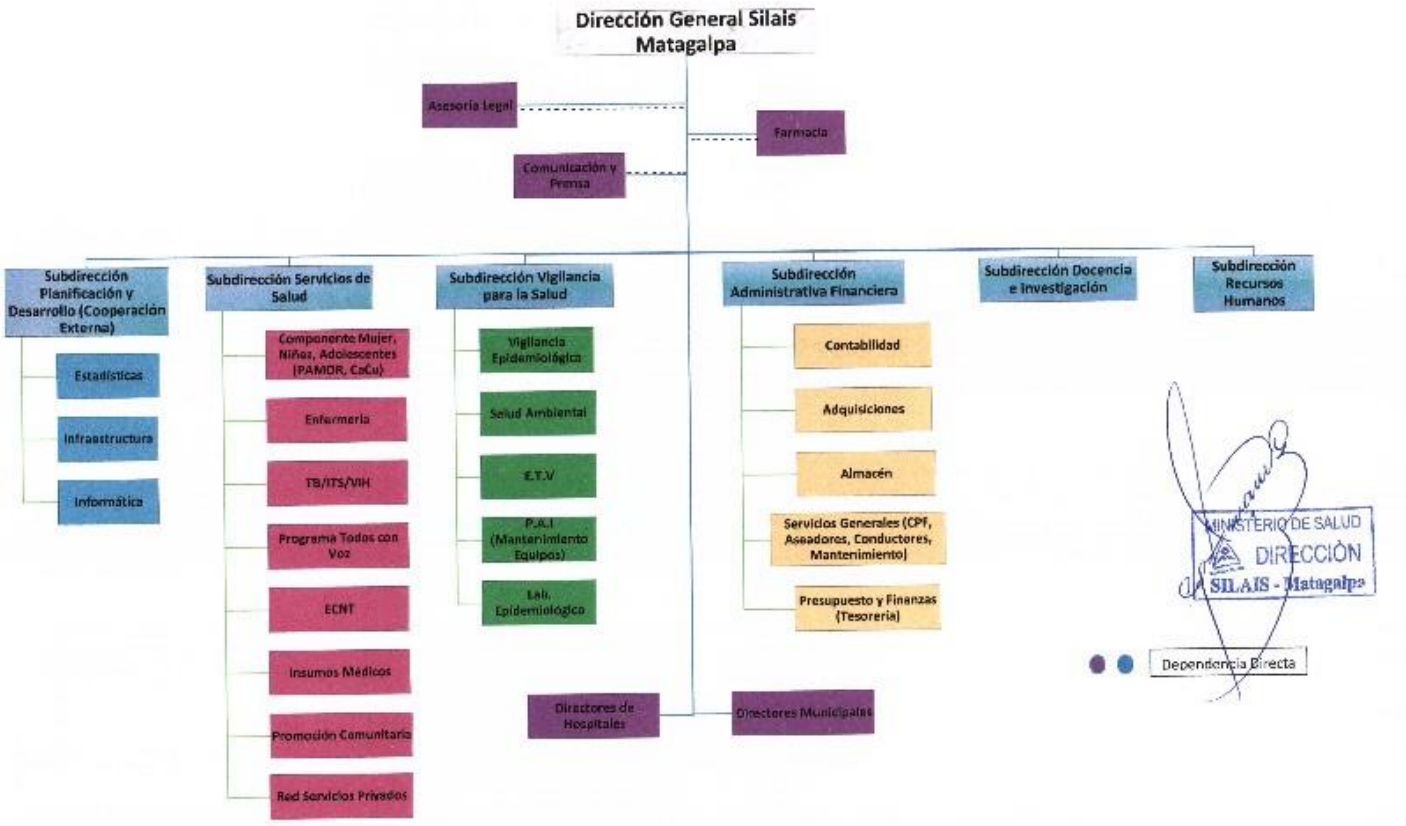
¿Se encuentran establecidas las políticas de control de acceso?	NO
¿Se cuenta con procedimientos formales, al momento de dar de alta o baja a un usuario de la red?	NO
¿Existen políticas de seguridad que regulen el uso de cifrado?	NO
¿Existen medidas de controles físicos aplicadas a las áreas donde se encuentran los dispositivos de red?	NO

¿Los dispositivos de red y los servidores se encuentran en un lugar capaz de soportar desastres naturales y evitar incidentes malintencionados a la información?	NO
¿Se implementa medidas de seguridad de acceso físico a las oficinas?	Si, las puertas
¿Los dispositivos de red e Intermediarios como conmutadores se encuentran ubicados en un RACK, el cual evite la manipulación no autorizado?	Los equipos no se encuentran centralizados en el RACK de datos.
¿Los cables de red están aislados de otros cables?	NO
¿Qué tipo de mantenimiento se les suministra a los dispositivos de red y al servidor?	El mantenimiento preventivo cada 6 meses y el correctivo cada vez que es necesario.
¿Existen controles de seguridad que permitan la detección y mitigación de malware?	SI
¿Realiza copias de seguridad del servidor y la información vital de la institución, y cada cuánto tiempo?	SI se realizan copias de seguridad y estas se realizan semanalmente.
¿Las copias de seguridad son guardadas en un lugar seguro?	NO
¿Se realizan auditorías de sistemas de información y redes?	NO
¿Hace uso de herramientas de monitoreo de red?	NO
¿Implementa mecanismos de seguridad emplea para proteger los servicios que ofrece la red?	NO

¿Existen redes virtuales locales en la institución?	NO
¿Intercambia información con entidades externas? ¿Utiliza políticas y procedimientos para realizar intercambios de información?	NO NO

¿Intercambia información con entidades externas? ¿Utiliza políticas y procedimientos para realizar intercambios de información?	NO NO
¿Utiliza mecanismos de seguridad para enviar información, por ejemplo: ¿el uso de correo electrónico?	Si, Mozilla Thunderbird con protocolo IMAP, POP3
¿La institución monitorea el cumplimiento prestado por los proveedores de servicio de internet (ISP)?	NO
¿Están establecidos los procedimientos para dar respuesta a los incidentes de seguridad de la información de la red?	NO
¿Se notifica a la administración de los eventos asociados a la seguridad de la información?	NO
¿Se documenta y notifica a la administración las sospechas de puntos débiles en la seguridad de la información que viaja por la red?	NO
¿Existe un plan de continuidad y recuperación de los procesos de seguridad de la información ante desastres?	NO
¿Existen dispositivos de red que permitan la redundancia en la infraestructura de red?	NO

Anexo 9.
Organigrama actual SILAIS - Matagalpa



Anexo 10.

Carta dirigida a responsable del área de Informática SILAIS Matagalpa

06 de abril de 2019

Cro. Oscar Danilo Mendoza

Responsable de Informática de SILAIS-MATAGALPA.

Por este medio adjudicamos el resultado de la Red de Área Local (LAN), en el Sistema Local de Atención Integral (SILAIS-MATAGALPA), periodo 2019. El informe de la investigación contiene las conclusiones y la propuesta de guía de mejoras respecto al estado actual de la infraestructura de red LAN, bajo la normativa para la seguridad de la información, ISO/IEC 27002:2013.

Br. Álvaro F Muñiz Zapata.
Responsable de evaluación

Br. Juan P Pravia Valdivia.
Responsable de evaluación.