UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

FACULTAD REGIONAL MULTIDISCIPLINARIA, MATAGALPA

UNAN MANAGUA - FAREM MATAGALPA

Monografía para optar al título de Ingeniería en Sistemas de Información.

Tema:

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.

Autores:

Br. Elí Josué Castillo Montenegro

Br. Norman Antonio Tercero Mendoza

Tutor:

Lic. Erick Noel Lanzas

Asesora Metodológica:

MSc. Guiselle Martínez Ramos

Matagalpa, Octubre 2016

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

FACULTAD REGIONAL MULTIDISCIPLINARIA, MATAGALPA

UNAN MANAGUA - FAREM MATAGALPA

Monografía para optar al título de Ingeniería en Sistemas de Información.

Tema:

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.

Autores:

Br. Elí Josué Castillo Montenegro

Br. Norman Antonio Tercero Mendoza

Tutor:

Lic. Erick Noel Lanzas

Asesora Metodológica:

MSc. Guiselle Martínez Ramos

Matagalpa, Octubre 2016

DEDICATORIA

A Dios:

Ser Supremo por excelencia, dador de la vida, sabiduría y oportunidades. Siempre estuvo conmigo y me fortaleció hasta el último momento de mi formación profesional.

A mi madre:

Por su constante motivación, apoyo incondicional y entrega plena. Siempre fue una fuente de inspiración, ayudándome día a día a crecer como un ser humano con valores morales, espirituales y con un alto espíritu de superación.

A los docentes:

Por ser personas genuinas y responsables en mi formación. Con entereza me facilitaron los conocimientos científicos y axiológicos, habilidades y destrezas inherentes en mi ser.

Elí Josué Castillo Montenegro

DEDICATORIA

A Dios:

Por ser el eje principal de mi vida, quien me dio la sabiduría necesaria en el transcurso de mi carrera, la fortaleza necesaria para afrontar y vencer cada obstáculo que se me presentó y así poder coronar mi carrera universitaria.

A mi familia:

Por ser mi principal apoyo en transcurso de mi carrera, brindándome las condiciones necesarias para poder estudiar y motivarme a ser mejor cada día, por su amor incondicional y formación fundamental para ser un profesional con principios morales y espirituales en la sociedad.

A los docentes:

Por impartirme el pan del saber, trasmitirme el conocimiento necesario y la ética profesional para formarme en mi carrera.

Norman Antonio Tercero Mendoza

AGRADECIMIENTO

A nuestro tutor Lic. Erick Lanzas, por orientarnos y corregirnos durante el desarrollo de la investigación.

A nuestra asesora metodológica MSc. Guiselle Martínez Ramos por su orientación y guía en el principio y formulación de la investigación.

A todos los docentes que influyeron y nos trasmitieron el conocimiento necesario para interesarnos en la línea de investigación, en especial a la MSc. Indiana Delgado por impartimos el conocimiento de Auditoria Informática.

De igual manera agradecemos a la Alcaldía Municipal de San Ramón, Matagalpa, por brindarnos la confianza y oportunidad de realizar dicha investigación, en especial a la Ing. Meylin Machado López por su amistad y transmitirnos la información necesaria para el desarrollo de esta investigación.

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 ***Norman Antonio Tercero Mendoza*** *(Carné 11064834) y* ***Elí Josué Castillo Montenegro*** *(Carné 11060687)*, dado que el informe final titulado: "*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*", cumple los requisitos establecidos para su defensa ante el tribunal examinador.

Dado en la ciudad de Matagalpa, a los veintiséis días del mes de octubre del año dos mil dieciséis.

_____

Lic. Erick Noel Lanzas Martínez

Tutor de Monografía

RESUMEN

Esta investigación tiene como objetivo principal evaluar la infraestructura de red LAN, de la Alcaldía Municipal de San Ramón, Matagalpa, bajo la norma ISO/IEC 27002:2013 en el primer semestre 2016.

La investigación se estructuró y desarrolló de acuerdo a los objetivos específicos, de los cuales se definen las variables de estudio que fueron desarrolladas en el marco teórico para aportar la cientificidad necesaria a la investigación. También se elaboró el diseño metodológico como base de la metodología de investigación aplicada, el cual comprende el enfoque investigativo, el universo de estudio y las técnicas de recolección de información.

Para la recolección de la información, se elaboraron los instrumentos necesarios a partir de la operacionalización de variables, la cual fue guiada a través del marco teórico, dichos instrumentos consistieron en entrevistas dirigidas a la directora de informática y una guía de observación a objetivos específicos.

Los resultados obtenidos de esta investigación demuestra que en la institución no se cumplen buenas prácticas para la seguridad de la información en las redes, además que el personal de informática no está capacitado para dar la atención y mantenimiento necesario a la infraestructura física y lógica de la red, tampoco existe un área de TI estructurada, no existen normativas y políticas de seguridad lógicas y físicas implementadas, el cableado no está estructurado, además no existen estándares internacionales implementados en la estructuración de la red, cabe señalar que no hay documentación necesaria de la red. Para dar solución a estas problemáticas se propone una guía de soluciones para mitigar las debilidades y mejorar la infraestructura de red.

ÍNDICE

ÍNDICE DE ANEXOS

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICO

I. INTRODUCCIÓN

Las infraestructuras de red forman parte del proceso de automatización de los recursos TIC, dado que permiten la disponibilidad y el transporte de datos de información de empresas e instituciones, es por eso que también busca la implementación de mecanismos de seguridad con el fin de que la información viaje segura y llegue de forma íntegra a su destino.

La seguridad de la información juega un papel muy importante en los procesos automatizados de las TIC, porque tiene como fin mantener segura e íntegra la información de las empresas o instituciones. Para lograr esto el estándar internacional ISO/IEC 27002-2013 propone 35 objetivos de control y 114 controles, agrupados en 14 dominios, los cuales permiten aplicar buenas prácticas para velar por el cumplimiento de la confidencialidad, seguridad, integridad y disponibilidad de la información.

En Nicaragua, las empresas e instituciones poseen infraestructuras de red que permiten compartir información y mantener comunicados a los usuarios de dicha red. Tal es el caso de la Alcaldía Municipal de San Ramón, Matagalpa, la cual forma parte de las instituciones del estado de Nicaragua, la cual posee una infraestructura de red para comunicar y difundir información entre los usuarios de la red, así como interconectar sus sistemas automatizados que se encuentran en las distintas áreas de la institución.

Por lo anterior descrito el objetivo de esta investigación, se basa en la evaluación de la infraestructura de red de la Alcaldía Municipal de San Ramón, Matagalpa, aplicando los criterios del estándar ISO/IEC 27002:2013, durante el primer semestre 2016, esto nos permitirá indagar cuáles son las deficiencias de la red y proponer mejoras para mitigar las dificultades encontradas.

Por lo tanto en este documento se describió el estado actual de la infraestructura de red, las dificultades encontradas y de esta manera se presentó la guía de soluciones para mejorar la seguridad de la información y la red.

En esta investigación, los objetivos específicos son parte fundamental de la estructura, donde cada variable se ve respaldada mediante la cientificidad del contenido del marco teórico. La metodología se arraiga con la información fundamentada que parte del diseño metodológico, el cual indica el tipo y enfoque de la investigación, así como las técnicas de recopilación de información con sus instrumentos y variables que se aplicaron.

II. ANTECEDENTES

Europa

En Cataluña España, Cepa (2011), llevó a cabo un proyecto de carrera en la Universidad Politécnica de Cataluña, donde destaca su trabajo bajo el título de "Auditoría de una red de comunicaciones", investigó el estado general de la red en aspectos de futura ampliación de la red, migración y cambios tecnológicos, de igual manera revisó el estado general de la red para detectar posibles fallas, estudió la calidad de los servicios de red para así poder solucionar problemas existentes en la red y elaborar la documentación técnica de esta. Encontró que la red está basada en tecnologías y equipos obsoletos, existen un grave problema de flooding, no existe segmentación de red VLAN, los equipos no emplean las recomendaciones básicas de seguridad para entornos LAN, por lo que recomendó; minimizar el tráfico multicast utilizando técnicas IGMP snooping, optimizar la segmentación de red mediante VLAN y actualizar las versiones de software de los equipos. Con esta investigación se logró encontrar múltiples riesgos en la red, y así poder recomendar las mejores para minimizar dichos riesgos.

Sudamérica

En Venezuela, Mayol (2006), realizó una investigación del "Modelo para la auditoría de la seguridad informática en la red de datos de la Universidad de los Andes", su objetivo fue diseñar un modelo para realizar auditorías de seguridad informática en ambientes universitarios y aplicar dicho modelo a la Universidad de los Andes. Encontró dificultades en cuanto a la infraestructura física de la red e inalámbrica, riesgo en la revisión de: políticas de seguridad y en servidores basados en Unix y Windows, por lo cual recomendó utilizar el modelo de auditoría informática actualmente propuesta, debido a que esta facilita procedimientos y salidas para corregir los riesgos detectados, así también implementar funciones necesarias para la seguridad informática de la Universidad de los Andes. Con este proyecto se logró crear e implementar un nuevo modelo para aplicar auditorías de seguridad informática, basada en el uso de mejores técnicas y mecanismos para la mejorar la seguridad informática.

En Ecuador, Arce Cuesta & Tacuri Japa (2010), optan por el título de Ingeniero en Sistemas, mediante una tesis bajo el título “Auditoría física y lógica a las redes de comunicaciones de computadores de la fábrica PASAMANERIA S.A”, dicha auditoría comprendió el estado de toda la red, es decir la infraestructura física y lógica, problemas y rendimiento de la misma. Se encontraron dificultades en cuanto al diseño físico de la red, por lo cual se propuso un nuevo esquema físico de red.

Centroamérica

En El Salvador, Orellana Benavides (2003), opta 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.

En la Universidad de San Carlos, Guatemala, Lobos Barrera (2005), llevó a cabo una auditoría, bajo el nombre “Auditoría de empresas en el área de telecomunicaciones”. Se investigaron los aspectos críticos que no se pueden descuidar en la seguridad de las redes y el adecuado control interno sobre las áreas de las empresas, por lo cual se recomendó realizar evaluaciones periódicas sobre el nivel de cumplimento de los procesos relacionados con la administración de los sistemas e implementar las recomendaciones planteadas en la auditorías y aplicar políticas y normas de seguridad de las telecomunicaciones.

Matagalpa, Nicaragua

En Matagalpa, Mendoza (2012), realizó la evaluación de la red de computadores de la FAREM Matagalpa, con el título “Evaluación de la red de computadores de UNAN Managua FAREM Matagalpa” donde el autor expuso las fortalezas y debilidades de dicha red. Las debilidades encontradas se reflejan tanto en la infraestructura física como lógica, en el diseño físico se encontró con la mala organización de la red y el uso de dispositivos obsoletos, así también se encontraron múltiples fallas en la red lógica, ya que no existía segmentación de la red y no se aplicaban políticas de seguridad, por lo cual se recomendó un nuevo diseño físico de la red, y el uso de mecanismo de seguridad y políticas de seguridad.

En la Universidad Nacional Autónoma de Nicaragua, Managua, Facultad Regional Multidisciplinaria, Matagalpa, Blandon & Galdámez (2016), realizaron una evaluacion 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 podrian implementar a la infraestructura de red para mejorar y minimizar los riesgos encontrados en la seguridad.

III. JUSTIFICACIÓN

La investigación consiste en la evaluación de la infraestructura de red en la Alcaldía Municipal de San Ramón, Matagalpa, bajo la norma ISO/IEC 27002:2013, la cual ayudará a analizar y brindar una guía con los controles necesarios para la seguridad de la información y un mejor desempeño de la red.

Se apreció la necesidad de evaluar la infraestructura de red de la institución, debido a que esta no se encuentra estructurada correctamente y no se realizan buenas prácticas, las cuales permitan mejorar el desempeño de la red, cabe señalar que la gerencia no está consciente del grado de importancia que presenta el área informática en los procesos claves que se realizan en la institución.

La importancia de esta evaluación centra como objetivo fundamental obtener información detallada sobre la infraestructura de red, para poder determinar el grado de cumplimento de buenas prácticas en la seguridad de la información, de esta manera mediante el análisis de la información se podrán aplicar mejoras que permitan optimizar la red.

La investigación tendrá un impacto positivo en la institución e indirecto para la sociedad, puesto que actualmente la red es deficiente y los servicios automatizados que la alcaldía ofrece a la población se ven afectados, además no se cuenta con el suficiente personal informático que de soporte a los servicios de TI, por esta razón la evaluación permitirá establecer controles de buenas prácticas en la seguridad de la información y la administración de la red, de esta manera se podrán mejorar los servicios en red, mitigar las vulnerabilidades y amenazas existentes.

El resultado de esta evaluación permite aportar las recomendaciones necesarias para mejorar el funcionamiento de la red, la seguridad de la información y optimización de los servicios en red, proporcionando beneficios directos a la directora de informática para la correcta administración de las redes y la institución en general que hace uso de red LAN e indirectamente a la población que acude a los servicios brindados por la institución.

IV. PLANTEAMIENTO DEL PROBLEMA

La Alcaldía Municipal de San Ramón, Matagalpa, posee una infraestructura de red, donde es notable que la red se encuentra de manera desorganizada, ocasionando una saturación en el tráfico de datos, lo que provoca que los sistemas colapsen en múltiples ocasiones.

De forma exploratoria, se puede observar que los trabajadores se encuentran insatisfechos con el rendimiento de la infraestructura de red en cuanto a calidad, disponibilidad y confiabilidad se refiere, lo que conlleva a pensar que es necesaria una evaluación para detectar fallas y proponer mejoras en el diseño lógico y físico de la red.

Por lo anterior descrito se plantea la siguiente problemática:

¿Cumple la infraestructura de red de la Alcaldía Municipal de San Ramón, Matagalpa, los criterios de la norma ISO/IEC 27002:2013, primer semestre 2016?

V. OBJETIVOS

Objetivo General

Evaluar la infraestructura de red LAN, bajo la norma ISO/IEC 27002:2013, en la Alcaldía Municipal de San Ramón, Matagalpa, primer semestre 2016.

Objetivos Específicos

1. Describir la condición lógica y física de la red actual.
2. Identificar las debilidades y fortalezas de la red, tomando en cuenta la norma ISO/IEC 27002:2013.
3. Proponer guía de soluciones ante las debilidades físicas y lógicas encontradas en la red, tomando en cuenta la norma ISO/IEC 27002:2013.

VI. MARCO TEÓRICO

6.1 Redes

6.1.1 Definición

Según ([1]Cisco systems, 2007), una red son múltiples computadoras conectadas entre ellas que utilizan un sistema de comunicaciones. El objetivo de una red es que las computadoras se comuniquen y compartan archivos.

Para que exista el término red de computadoras siempre deben de haber más de dos computadoras conectadas unas a otras, esto con el fin de intercambiar información de cualquier índole, recursos o servicios.

En la actualidad las redes de computadoras se han vuelto muy usadas en hogares, universidades, empresas, porque vivimos en la época de la globalización y este es un término muy usado en estos tiempos. La globalización se lleva a cabo principalmente gracias a las redes de computadoras, debido a que con ellas es posible comunicarse en cuestión de segundos a cualquier país del mundo e intercambiar información sin tener que levantarse de tu asiento. También son muy importantes porque la tecnología avanza con rapidez, te puedes informar de todo lo que está pasando en el mundo.

6.1.2 Arquitectura de red

Según (Alvarez, 2012), “Lo primero que tenemos que saber es, a que nos referimos cuando hablamos de arquitectura de red, bien pues nos referimos a las tecnologías que admiten la infraestructura, servicios y protocolos que transmiten los mensajes a través de la red, para que esta sea fiable y funcione perfectamente”.

[1] **Cisco systems:** es la empresa líder mundial en TI que se dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones y permite a las empresas aprovechar las oportunidades del futuro. Para más información ver: http://www.cisco.com/c/es_ni/index.html.

La arquitectura de red se basa en la implementación de tecnologías que permitan ofrecer servicios de calidad, donde la información se transmita de manera segura y confiable.

Hoy en día las empresas presenciaron cambios masivos, pero una sola cosa se conservó: la red empresarial. Y aunque los dispositivos de red se volvieron más rápidos, más potentes y más inteligentes, la arquitectura fundamental de la red (y la manera en que usted la suministra y la opera) sigue siendo la misma en gran parte.

6.1.2.1 La tolerancia de fallas

[2]CIBERTEC (2012), menciona que el hecho de que Internet esté siempre disponible para los millones de usuarios que dependen de ella, requiere de una arquitectura de red que se ha diseñado y construido para ser tolerantes a errores. El concepto de tolerancia a fallos de red limita la posibilidad de que un fallo de hardware o software se dé y si este se da, que la red se pueda recuperar rápidamente. Estas redes dependen de los enlaces o rutas redundantes, entre la fuente y el destino de un mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes puedan ser enrutados al instante entre los usuarios de cualquiera de los extremos.

Una red tolerante a fallos es aquella que limita el impacto de un error de software o hardware y que además puede recuperarse de dicho error rápidamente, para que se entienda mejor, si nosotros enviamos un mensaje y nos da un error de enrutamiento, la red lo que tendría que hacer es mandar inmediatamente el mismo mensaje pero por otra ruta distinta, de tal manera que el destinatario no conoce dicho error y puede recibir el mensaje sin ningún problema. Para aplicar este sistema utilizamos lo que se llama redundancia, y es simplemente implementar

[2] CIBERTEC: es una institución educativa que cuenta con más de **33 años de experiencia** (autorizado mediante Resolución Ministerial 1451-83-ED con fecha 10 de noviembre de 1983) en la formación y capacitación de profesionales en diferentes áreas de Tecnologías de la Información, Gestión y Negocios, Diseño, Comunicaciones e Ingeniería. Para más información ver: http://www.cibertec.edu.pe/acerca-de-cibertec.

varios caminos, soluciones por si uno falla, tengamos más opciones y el mensaje siempre llegue a su destinatario.

Hoy en día los proveedores de servicios de Internet utilizan conexiones redundantes, porque permiten usar rutas alternativas cuando falla un dispositivo o un enlace sin verse afectada, garantizando que los mensajes pueden enrutarse en forma instantánea en un enlace diferente y transparente para los usuarios en cada extremo.

6.1.2.2 Escalabilidad

Para CIBERTEC (2012), una red escalable puede crecer rápidamente para apoyar a nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio que se entrega a los usuarios existentes. Miles de nuevos usuarios se conectan a Internet cada semana. La capacidad de la red de apoyar a estas nuevas interconexiones depende de una concepción jerárquica en capas subyacentes de la infraestructura de la arquitectura física y lógica.

La red debe poder aumentar de tamaño, es decir, el diseño general debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño original y rendimiento de la red, como un ejemplo de esto, cada semana se conectan miles de usuarios nuevos y proveedores de Internet, para que esto no cree problemas de rendimiento se ha creado un diseño jerárquico de capas para la estructura física y la arquitectura lógica.

En la actualidad para los proveedores de servicio de internet es un tema muy importante, dado que día a día millones de redes y usuarios se conectan a internet, sus redes deben admitir nuevas interconexiones para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio dado a los usuarios actuales.

6.1.2.3 Calidad de Servicio (QoS)

CIBERTEC (2012), afirma que el internet actualmente proporciona un nivel aceptable de tolerancia a fallos y escalabilidad para sus usuarios. Sin embargo,

las nuevas aplicaciones a disposición de los usuarios generan mayores expectativas por la calidad de los servicios entregados. Las transmisiones de voz y video en directo exigen un nivel alto de calidad de la transmisión y la certeza de una transmisión ininterrumpida. Las redes tradicionales de voz y de video están diseñadas para apoyar a un solo tipo de transmisión, y por lo tanto son capaces de producir un nivel aceptable de calidad. Los nuevos requisitos para apoyar esta calidad de los servicios convergentes sobre una red están cambiando la forma en que las arquitecturas de red se están diseñando y aplicando.

Para que una red suministre una buena calidad de servicio, crea lo que se denominan prioridades, para que así, de esta forma, por ejemplo, se da más prioridad a un streaming de video que a una página web, ya que esta última no requiere tantos servicios para funcionar correctamente.

Hoy en día los dispositivos que entregan los proveedores de servicio de internet como Claro, traen una configuración que se llama QoS lo que indica que al activarla les dará más prioridad a una llamada de VoIP que a una página web, es decir le proporciona mayor ancho de banda a una llamada o video que la página web, la página se cargará pero de manera más lenta.

6.1.2.4 Seguridad

CIBERTEC (2012), añade que la Internet ha evolucionado de ser una internetwork estrictamente controlada por las organizaciones gubernamentales y orientada a la educación hacia una red que permite servir como medio de transmisión de comunicaciones personales y de negocios. Como resultado de ello, las necesidades de seguridad de la red han cambiado. La seguridad y la privacidad de las comunicaciones requieren altos estándares para ofrecer seguridad a los interlocutores del proceso de comunicación. Como resultado de ello, muchos esfuerzos se están dedicando a esta área de investigación y desarrollo. Entre tanto, muchas herramientas y procedimientos se están aplicando para luchar contra fallas de seguridad inherentes en la arquitectura de red.

La seguridad de redes es una parte integral de las redes de computadoras, independientemente si la red está limitada a un entorno doméstico con una única conexión a Internet o si es tan extensa como una empresa con miles de usuarios, podemos utilizar sistemas de seguridad como : contraseñas cifradas, firewall, encriptadores de datos, entre otros, sin embargo no es lo suficientemente seguro puesto que existen miles de atacantes en la red interceptando paquetes, con el objetivo de robar información valiosa o realizar ataques desde afuera hacia las intranet.

En la actualidad muchas empresas se preocupan con el tema de seguridad, por lo que se encuentran muy estrictos en sus políticas de seguridad, por ejemplo, es el caso de INVERCASA que usa un firewall para filtrar los datos y detectar amenazas que vienen desde el exterior y puedan ocasionar robos de información valiosa.

6.1.3 Tipos de Redes

6.1.3.1 Redes de área local (LAN)

“Las redes de área local (generalmente conocidas como LANs) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos e intercambiar información” (Tanembaum, 2003, p.891).

Son las redes más comunes que existen que por lo general conecta los ordenadores en un área relativamente pequeña y determinada, por ejemplo, una habitación, un edificio, un hogar, esta red alcanza una velocidad de transferencia de datos de hasta 10 Mbps o 1 Gbps.

Hoy en día estas son las redes que más encontramos, y pequeñas empresas o instituciones optan por crear este tipo de red, con el objetivo de compartir algún recurso o servicio, otro ejemplo de LAN que se aplica en la actualidad es la red que posee la Facultad Regional Multidisciplinaria de Matagalpa, una LAN bien estructurada.

6.1.3.2 Redes de área metropolitana (MAN)

“Las redes de área metropolitana se caracterizan por tener velocidades de acceso muy elevadas (de 30 a 150 Mbit/s y en la actualidad hasta los 10 Gbit/s), distancias cubiertas medianas (10 a 50 km, las correspondientes a una ciudad y su área de influencia) y propiedad/explotación a medio camino entre lo público y lo privado” (Hesselbach Serra & Bosch, 2002, p186).

Una red MAN es aquella que a través de una conexión de alta velocidad, ofrece cobertura en una zona geográfica extensa como una ciudad o un municipio, con esta red es posible compartir e intercambiar todo tipo de datos mediante fibra óptica o cable de par trenzado, esta red puede ser pública o privada.

En la actualidad muchas empresas corporativas que tienen cierta cantidad de sucursales dispersos en áreas dentro de una ciudad, forman una MAN con el objetivo de compartir su información de manera rápida.

6.1.3.3 Redes de área amplia (WAN)

Para Tanembaum (2003), una red de área amplia (WAN), abarca una gran área geográfica, con frecuencia un país o un continente. Contiene un conjunto de máquinas diseñados para programas (es decir, aplicaciones) de usuario.

Las redes WAN por lo general se extienden en una gran franja de territorio, ya sea a través de una ciudad, un país e incluso a nivel mundial, este tipo de red generalmente cubre unos 100 o hasta 1000 kilómetros, lo que permite cubrir varias ciudades e incluso un país entero. Su velocidad oscila entre 1 Mbps y 1 Gbps.

Este tipo de red usan las grandes corporaciones como Claro que posee sucursales en casi todo el país e incluso en algunos países del continente americano.

6.1.4 Topologías de Red

6.1.4.1 Topología de Estrella

Según Rodríguez (2007), es la estructura clásica de red y la más antigua, es la de estrella. El centro de la estrella lo forma el servidor, o una gran computadora central. Cada estación de trabajo, que en tiempos pasados estaba formada por una terminal sin inteligencia propia, que se conecta al ordenador central a través del cable.

Consiste en que todos los equipos finales de la red se conectan a uno intermedio que encamina la información al destinatario.

En la actualidad ya casi no existe esta topología, puesto que no aportan ninguna ventaja sobre el resto y sí muchos inconvenientes.

6.1.4.2 Topología de Bus

Heredero (2004), mencionó que la red no tiene equipos intermedios. Todos los equipos finales se encuentran conectados a un mismo medio físico que típicamente es un cable (aunque se puede emplear tecnología inalámbrica o Wireless). Este medio físico se encuentra interrumpido por los dos extremos y terminado por elementos eléctricos que aseguran sus características de transmisión.

En esta topología se pueden conectar una gran cantidad de computadores al bus, si un computador falla, la comunicación se mantiene, mientras que si el bus es el que falla, la comunicación se cae inmediatamente. La información viaja por el cable en ambos sentidos a una velocidad bastante buena y posee en sus dos extremos una resistencia.

La topología de bus hoy en día ya no es usada porque presenta muchos problemas como por ejemplo:

- ✓ Hay un límite de equipos dependiendo de la calidad de la señal.
- ✓ Puede producirse degradación de la señal.
- ✓ Limitación de las longitudes físicas del canal.
- ✓ El desempeño se disminuye a medida que la red crece.
- ✓ El canal requiere ser correctamente cerrado (caminos cerrados).
- ✓ Altas pérdidas en la transmisión debido a colisiones entre mensajes.
- ✓ Es una red que ocupa mucho espacio.

6.1.4.3 Topología de anillo

Para Higuera & García (2007), la topologia en anillo consiste en un circulo de conexiones punto a punto que se conectan mediante una unidad de acceso y un repetidor. En esta topologia no existe un nodo principal y el control de la red queda distribuido entre los nodos.

En esta topología, las estaciones de trabajo que están de manera individual hacen la forma de un anillo y la información pasa de un ordenador a otro hasta que llega al destinatario al que va dirigida.

En la actualidad no se conoce de entidades que usan esta red porque es muy complicado mantenerla y ampliarla: cuando falla un cable o una conexión, la red entera deja de funcionar, y no es sencillo localizar el punto exacto donde se encuentra el fallo.

6.1.4.4 Topología de árbol

Rodríguez (2007), añade que este tipo de topología de red es una de las más sencillas. Como su nombre lo indica, las conexiones entre los nodos (terminales o computadoras) están dispuestas en forma de árbol, con una punta y una base.

Si un nodo falla, no se presentan problemas entre los nodos subsiguientes. Cuenta con un cable principal llamado backbone, que lleva la comunicación a todos los nodos de la red, compartiendo un mismo canal de comunicación.

La topología en árbol puede verse como una combinación de varias topologías en estrella y la información se propaga hacia todas las estaciones, si el cable principal falla se cae la red de comunicación puesto que este es el principal canal de conexión.

La topología en árbol es un poco más usada en la actualidad a pesar que se requiere mucho cable, la medida de cada segmento viene determinada por el tipo de cable utilizado, si se viene abajo el segmento principal todo el segmento se viene abajo con él y es más difícil su configuración.

6.1.4.5 Topología de malla

Para Vázquez, Baeza, & Herías, (2010), una topologia en malla es una configuración en la que cada dispositivo tiene un enlace punto a punto dedicado con cualquier otro dispositivo. El término dedicado indica que el enlace solo conduce el flujo de datos entre los dispositivos que interconecta. En la topología en malla, los dispositivos que forman la red puedes ser nodos de reenvio o enrutamiento (router) o equipos finales (PC).

En el uso de esta topología los equipos finales como son (PC) se conectan a equipos intermedios (switch) en forma de estrella, mientras que los últimos se conectan entre si todos con todos. Esta configuración que se realiza asegura la disponibilidad de la red en un dado caso que un dispositivo intermediario falle.

Hoy en día esta topología es usada en redes WAN o de área amplia. Su importancia radica en que la información puede viajar en diferentes caminos, de manera que si llegara a fallar un nodo, se puede seguir intercambiando información sin inconveniente alguno entre los nodos.

6.1.5 Elementos de una red

6.1.5.1 Mensajes

Para Cisco Systems (2007) 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.

En esta parte se utiliza la palabra mensaje para referirse por ejemplo, a páginas web, correos electrónicos, llamadas telefónicas, videollamadas, documentos, entre otros, sin importar lo que sea estos se transmiten en la red, pero antes tienen que ser convertidos a su respectivo formato para su transporte.

En la actualidad la mayoría de personas hace uso de su correo electrónico, visitar páginas web, descargas de videos por lo que esto se transforma en bits y después en binarios para su envío a través de la red.

6.1.5.2 Dispositivos

Según Cisco Systems (2007), 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 componentes que hacen posible que nuestros mensajes instantáneos sean direccionados a través de kilómetros de cables, cables subterráneos, ondas aéreas y estaciones de satélites que puedan existir entre los dispositivos de origen y de destino. Uno de los componentes

críticos en una red de cualquier tamaño es el router. Un router une dos o más redes, como una red doméstica e Internet, y pasa información de una red a otra.

Los routers en una red funcionan para asegurar que el mensaje llegue al destino de la manera más rápida y eficaz.

Es un dispositivo muy esencial, programado para que este sea quien elija la mejor ruta para enviar los datos y su trabajo principal es de enviar o encaminar los paquetes de datos de una red a otra, hasta que este sea entregado o haya llegado al destino seleccionado.

Actualmente las empresas de telecomunicaciones poseen un sinnúmero de dispositivos, esto con el fin de ofrecer una mejor eficiencia y rapidez de envío de determinados archivos.

6.1.5.3 Medio de transmisión

Para Cisco Systems (2007), 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.

Hoy en día en la mayoría de hogares y empresas se cuenta con conexión de red inalámbrica o cableada, así que por la red inalámbrica se puede enviar un correo electrónico o conectando el ordenador con un cable al dispositivo (router o switch), esto indica que se puede enviar de igual manera un correo electrónico con cualquiera de los dos medios, puesto que los datos pueden viajar sin importar el medio.

6.1.5.4 Servicios

Cisco Systems (2007), afirma que 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 e-mails, 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.

Estos servicios por lo general son instalados en uno o más servidores para compartir recursos o servicios a otras computadoras clientes, son una gran variedad de servicios que presta la red, como son: servicios de archivos, base de datos, fax, backup, website, email, chat, video, entre otros.

En la actualidad estos servicios son muy usados desde que se usa de un servidor de descarga de archivos, revisar el correo electrónico, consultas en línea de facturas, transferencia de dinero, videoconferencias e incluso llamadas internacionales usando VoIP de Skype.

6.1.5.5 Reglas

Cisco Systems (2007), 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.

6.1.6 Calidad de las comunicaciones

6.1.6.1 Factores externos

Según Cisco systems (2007), los factores externos que afectan la comunicación están relacionados con la complejidad de la red y el número de dispositivos que debe atravesar un mensaje para llegar al destino final.

Los factores externos que afectan el éxito de las comunicaciones son:

- ✓ La calidad de la ruta entre el emisor y el receptor.
- ✓ La cantidad de veces que el mensaje tiene que cambiar la forma.
- ✓ La cantidad de veces que el mensaje tiene que ser redireccionado o redirigido.
- ✓ La cantidad de mensajes adicionales que se transmiten simultáneamente en la red de comunicación.
- ✓ La cantidad de tiempo asignado para una comunicación exitosa.

En la red un mensaje al ser enviado pasa por redes extensas y un sinnúmero de dispositivos de red, de estos factores principales depende que el mensaje pueda llegar de manera exitosa al destino seleccionado.

Las empresas de dispositivos de red hoy en día están fabricando dispositivos de red y cables con capacidades de transmisión realmente altas, esto para evitar retrasos en las redes mientras se transportan los mensajes.

6.1.6.2 Factores internos

Cisco systems (2007), afirma que diferentes tipos de mensajes pueden variar en complejidad e importancia. Los mensajes claros y concisos son generalmente más fáciles de entender que los mensajes complejos. Las comunicaciones importantes requieren de más atención para asegurarse de que el receptor las comprenda correctamente.

Los factores internos que afectan la comunicación exitosa en la red son:

- El tamaño del mensaje.
- La complejidad del mensaje.
- La importancia del mensaje.

Los factores internos que interfieren en la comunicación en redes están relacionados con la naturaleza del mensaje, como son el tamaño, complejidad e importancia del mensaje, factores importantes ya que de estos depende la comunicación exitosa de la red.

El ancho de banda de internet en la actualidad permite que los mensajes un poco más pesados puedan adjuntarse y entregarse de manera rápida, aunque es más difícil entregar un paquete más grande y rápido, que pequeños paquetes a la vez.

6.1.7 Infraestructura física

6.1.7.1 Dispositivos de red

6.1.7.1.1 Repetidor

Gallego (2010), el repetidor es uno de los elementos de electrónica de red más simples. Su función es captar la señal y enviarla, sin darle ningún tratamiento más allá de la amplificación. Por este motivo, el repetidor trabaja en la capa 1 del modelo OSI.

El repetidor surge por la necesidad de cubrir distancias más grandes de las que podían alcanzar los cables, siendo su trabajo recibir señal y enviarla.

El repetidor en la actualidad sigue siendo utilizado, por ejemplo en las interconexiones submarinas de extremo a extremo y una de las desventajas de estos dispositivos era que se extendían en longitud pero solo podían conectar una computadora porque solo tenía una entrada y una salida.

6.1.7.1.2 Concentrador (hub)

Para Cisco systems (2007), los hubs son conocidos como repetidores multipuesto. La diferencia entre ellos y el repetidor está dada por el número de puertos que posee cada uno de ellos.

Los hubs realizan la misma función que el repetidor con la única diferencia que este puede tener hasta 24 puertos y el repetidor solo 2.

Hoy en día el hub es un dispositivo que se está quedando obsoleto. Sin embargo, en muchas instalaciones se lo utiliza como enlace entre redes locales.

6.1.7.1.3 Conmutador (Switch)

Según Cisco systems (2007), un switch recibe una trama y regenera cada bit de la trama en el puerto de destino adecuado. Este dispositivo se utiliza para segmentar una red en múltiples dominios de colisiones. A diferencia del hub, un switch reduce las colisiones en una LAN. Cada puerto del switch crea un dominio de colisiones individual. Esto crea una topología lógica punto a punto en el dispositivo de cada puerto. Además, un switch proporciona ancho de banda dedicado en cada puerto y así aumenta el rendimiento de una LAN. El switch de una LAN también puede utilizarse para interconectar segmentos de red de diferentes velocidades.

El switch tiene como función principal recibir y enviar paquetes únicamente a los dispositivos seleccionados, si bien un switch es más costoso que un hub resulta económico al considerar su confiabilidad y rendimiento mejorados, además que posee gran ancho de banda en sus puertos.

Hoy en día en muchas empresas usan los switch, puesto que son fácil de montar en una red, poseen gran velocidad en sus puertos, y dirigen el paquete al dispositivo seleccionado evitando congestión de datos en los cables.

El switch administrable permite una mejor administración en la red.

6.1.7.1.4 Enrutador (Router)

Concejero et al., (2014), mencionan que los routers son dispositivos de nivel 3 (Nivel de red en el modelo OSI) que permiten segmentar la red y elegir la ruta optima que deben elegir los mensajes enviados desde un equipo a otro. Los routers dividen la red en segmentos, denominados subredes.

El router posee una de las funciones principales en una red, como es conocer las redes de otros dispositivos, filtrar el tráfico, determinar la mejor ruta para alcanzar la red de destino y reenviar el tráfico hacia la interfaz que corresponde.

En la actualidad las empresas medianas, grandes y pequeñas han comenzado a buscar un mayor grado de la integración en tecnología aplicada a redes. Es común que las organizaciones necesiten utilizar tecnologías como router para comunicarse, permitiendo el acceso seguro a recursos corporativos.

6.1.7.1.5 Punto de acceso (AP)

Para Gallego (2010), el punto de acceso (acces point, o AP), es un elemento inalámbrico de la red que se usa para extender la red cableada, ofreciendo conexión a la misma a través de medio inalámbrico.

Es un intermediario de la comunicación en una red inalámbrica que se comunica por ondas de radio. Es decir, actúa como puente o bridge e intermediario entre redes cableadas e inalámbricas.

Hoy en día es muy común encontrarse con un acces point en muchas empresas, universidades e incluso parques en Nicaragua, esto evita la molestia de estar conectado a un cable que restringa tu movilidad.

6.1.7.1.6 Modem

Moya & Huidobro (2006), agregan que el servicio telefónico básico es, técnicamente, un servicio analógico y orientado a la tranmisión de voz empleando la conmutación de circuitos. Puesto que los enlaces de transmisión y centrales de conmutación no están completamente digitalizados, para la transmisión de datos se requiere el empleo de modems que conviertan la senal digital en analógica (modulación) y viceversa (demodulación)"

El módem convierte las señales digitales del ordenador en señales analógicas que pueden transmitirse a través del cable telefónico y esto permite enviar datos a otra computadora con módem.

La empresa Claro actualmente ofrece este tipo de tecnología para los clientes que poseen conexión a través de un cable de línea telefónica.

6.1.7.1.7 Cortafuegos (firewall)

Para López (2010), es un dispositivo, o conjunto de ellos, que esta configurado para impedir el acceso no autorizado a una determinada zona de una red o dispositivo pero que al mismo tiempo permite el paso a aquellas comunicaciones autorizadas.

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Hoy en día las empresas son muy cuidadosos con su información por lo que algunas inmediatamente implementan firewall, pero algunas debido a los costos altos de éste no lo hacen, por lo que están desprotegidos por intrusos que quieran realizar ataques desde el exterior.

6.1.7.2 Medios de transmisión

6.1.7.2.1 Cableados o guiados

6.1.7.2.1.1 Cable de par trenzado

Para Tanenbaum (2003), 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. Esto se hace porque dos alambres paralelos constituyen una antena simple. Cuando se trenzan los alambres, las ondas de diferentes vueltas se cancelan, por lo que la radiación del cable es menos efectiva.

Sus categorias 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 Ethernet 100Base-TX.
- ✓ Categoría 5e: hasta 622 Mbits/seg. Utilizado para Gigabit Ethernet.
- ✓ 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.

En la actualidad es el cable más usado en la mayoría de redes LAN (universidades, hogares, edificios) debido a sus velocidades de transferencias de datos realmente altas.

6.1.7.2.1.2 Cable coaxial

Según Gómez (2011), el cable coaxial transporta senales 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 prácticamente consiste en un alambre de cobre rígido grueso, rodeado por un material aislante, una malla conductiva de tejido fuertemente trenzado.

Hoy en día la empresa de telecomunicaciones Claro, usa este cable para la transmisión analógica y la televisión por cable, además que ofrece el servicio de internet con este tipo de cable.

6.1.7.2.1.3 Cable de fibra óptica

Gómez (2011), 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 LED.

La fibra óptica es una nueva tecnología de cable que se utiliza para la instalación de redes locales. Consiste en un núcleo central de vidrio con un índice alto de refracción y con un revestimiento de vidrio pero con una refracción más baja.

En la actualidad pocas entidades hacen uso de este cable debido a sus altos costos, además que usa transmisores y receptores más caros.

6.1.7.2.2 Medio de transmisión inalámbrica

6.1.7.2.2.1 Ondas de radio

Para Gómez (2011), son ondas omnidireccionales, es decir, emiten y reciben en los 360 grados, por lo que son necesarias antenas parabólicas. Las frecuencias de estas ondas oscíla entre los 3 Hz y los 3,000 MHz. Entre las ventajas está el que

son ondas fáciles de generar, pueden recorrer distancias muy largas, pudiendo incluso penetrar edificios.

Las ondas de radio son ondas electromagnéticas de radiofrecuencia (RF) que transportan información.

En Nicaragua algunas empresas de televisión, radio y telefonía celular usan este tipo de medio inalámbricos para comunicarse.

6.1.7.2.2.2 WiFi

Gómez (2011), agrega que son un conjunto de espeficaciones 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 conjunto de redes que no requieren de cables y que funcionan en base a ciertos protocolos previamente establecidos y su mecanismo de conexión de dispositivos electrónicos es de forma inalámbrica.

En la actualidad muchos de los dispositivos vienen con esta tecnología, que permiten alcances de territorio realmente grandes y velocidades de aceración realmente altas.

6.1.7.3 Estación de Trabajo

Para Alcocer, Gómez, Prat, & Albareda (2006), son computadoras que normalmente sirven para conectarse a otra computadora de mayor tamaño a través de la red, con gran capacidad de procesamiento.

En redes, la palabra “workstation” o “estación de trabajo” se utiliza para referirse a cualquier computadora que está conectada a una red.

Es un ordenador que facilita a los usuarios el acceso a los servidores y periféricos de la red. Las estaciones de trabajo usualmente ofrecen más alto rendimiento que en las computadoras personales, especialmente con lo que respecta a gráficos, poder de procesamiento y habilidades multi-tareas.

En la mayoría de entidades que poseen una infraestructura de red, tienen al menos un servidor con excelentes requerimientos quien es el que provee servicios a otros ordenadores más pequeños.

6.1.7.4 Políticas de seguridad físicas

Para Castro Gil, Díaz Orueta, Alzórriz Alemendarez, & Ruiz (2014), son una serie de procedimientos relacionados con las seguridad física, tanto en el aspecto de control de acceso fisico a equipos, como el de tener planes de contingencia y emergencia, así como de recuperación frente a desastres.

Las políticas de seguridad físicas de una entidad, son normas que los trabajadores de dicha entidad deben respetar y cumplir para la protección física de todos los equipos que posee la institución.

En la actualidad la mayoría de empresas cuentan con sus políticas de seguridad físicas definidas, ya que estos son activos caros que posee la institución y los protege muy bien, pero no toda las instituciones poseen políticas de seguridad.

6.1.7.4.1 Amenazas físicas

Para Cisco systems (2007), una clase de amenaza menos glamorosa, pero no menos importante, es la seguridad física de los dispositivos.

Las cuatro clases de amenzas físicas son:

1. Amenazas al hardware: daño físico a los servidores, routers, switch, planta de cableado y estaciones de trabajo.
2. Amenazas ambientales: temperaturas extremas (calor o frios extremos) o condiciones extremas de humedad (humedad o sequedad extremas).

3. Amenazas electricas: picos de voltaje, voltaje suministrado insuficiente (apagones), alimentacion ilimitada (ruido) y perdida total de alimentacion.
4. Amenazas al mantenimiento: manejo deficiente de los componentes electricos clave (descarga electrostatica), falta de repuestos fundamentales, cableado insuficiente y rotulado incorrecto.

Las amenazas físicas son aquellas que atentan e involucran danos físicos a los dispositivos o equipos.

El centro de datos de ENACAL central, ubicado en la ciudad de Managua, posee unas políticas de seguridad físicas altamente estrictas, políticas de seguridad que benefician al hardware, en casos de amenazas ambientales, amenazas eléctricas e incluso en el mantenimiento, estas políticas son las que lo mantienen que el data center siga funcionando de manera continua.

6.1.8 Infraestructura lógica

6.1.8.1 Servidor

Según cisco systems (2007), 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 tratado como elemento físico también es una unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red.

En la Alcaldía Municipal de Matagalpa, actualmente cuenta con un servidor, el cual es encargado de brindar servicios a las computadoras que están conectadas en esa red, servicios como: DHCP, Servidor Proxy, Servidor Web, Servidor de almacenamiento, e incluso algunos de sus sistemas se encuentran ejecutando en red.

6.1.8.2 Direccionamiento IP

Esteller (2012), para identificar un dispositivo dentro de una red es necesario que tenga un identificador único en la red que lo diferencie de otro dispositivo. Este indicador de red es su dirección IP.

El protocolo IP define un esquema de direccionamiento jerárquico que permite que las direcciones individuales se asocien de forma conjunta y sean tratados como dispositivos de una misma red de area local, independiente de otras redes.

La dirección IP es un identificador lógico único e irrepetible que se le asigna a cada host ya sea (ordenador, TV, cámaras, tableta, teatro en casa, teléfono inteligente).

Hoy en día los administradores de redes toman direcciones IP, las dividen en partes más pequeñas, de acuerdo a las direcciones IP que necesitan y las agregan a los host con el objetivo de tener una administración más ordenada y eficiente de direcciones IP.

6.1.8.2.1 Direcciones privadas

Para Cisco systems (2007), 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 que no sale a internet, es decir estas direcciones IP no son usadas para Internet.

En las empresas que tienen administradores de redes, por lo general utilizan un rango de direcciones IP privadas para agregarlas a los host dentro de una red,

distribuyéndolas de manera ordenadas en la mayoría de los casos, pero en otros de manera muy desorganizada.

Los dispositivos de Internet que entrega Claro, en su servicio DHCP nos asignan incluso direcciones IP que están en el rango privado.

6.1.8.2.2 Direcciones públicas

Según cisco systems (2007), las direcciones públicas son asignadas por InterNic y estan 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 y alquiladas por nuestro proveedor de servicio 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 los ISP o proveedor de servicio de internet alquilan 1, 2, 3 o más direcciones IP públicas, las que la empresa pueda pagar para ser usada en internet, las direcciones IP públicas son únicas.

6.1.8.3 Servicios en red

6.1.8.3.1 DHCP (Dynamic Host Configuration Protocol)

Andreu (2010), 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 parametros de configuracion automaticamente.

El servidor DHCP asigna direcciones IP automáticamente a los host que están conectados a él, en el rango de direcciones que se ha especificado.

Hoy en día en universidades, empresas, colegios, este servicio está implementado en servidores en red y dispositivos de capa 2, agregando direcciones IP automáticamente a los dispositivos que se conectan a él, evitando el trabajo tedioso de estar agregando direcciones IP estáticamente a los dispositivos que se conectan.

6.1.8.3.2 DNS (Domain Name System)

Para Joaquín (2011), el Domain Name System o DNS es el servicio encargado de esta gestión, traduce un nombre en una dirección IP consultando la base de datos distribuida, conformada todos por todos los servidores DNS.

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

En la actualidad los servidores DNS han sido de mucha ayuda desde el hecho que buscamos en el navegador una sola palabra como ejemplo “a”, si no existiera tendríamos que buscar en los navegadores mediante direcciones IP para ver la página que queremos.

6.1.8.3.3 FTP (File Transfer Protocol)

Andreu (2011), el servicio FTP está basado en el protocolo FTP, del ingles File Transfer Protocol o Protocolo de Transferencia de Ficheros en redes tipo TCP/IP. El nombre se presta a confusión en tanto en cuanto no es un servicio exclusivo de transferencia de ficheros entre cliente y servidor en forma bidireccional, sino que mas bien es un servicio de administración de ficheros que permite multitud de acciones (subirlos, bajarlos, borrarlos, renombrarlos, moverlos, crear carpetas, borrar carpetas).

FTP es otro de los servicios que nos ofrece la red en la cual podemos subir archivos, descargar, usando la arquitectura de cliente servidor.

En la actualidad hacemos mucho uso de servidores como mega, 4shared, google drive, que nos permite subir archivos a la nube y podes hacer lo que nos plazca con ello.

6.1.8.3.4 Servicio de accesos remoto (TELNET)

Herrera Peréz (2003), afirma que el servicio de acceso remoto de internet se conoce como TELNET. Este es un protocolo estándar cuyas especificaciones son parte de la documentación TCP/IP. Para utilizarlo se debe llamar a un programa

de aplicación local y especificar una máquina remota. El programa permite que el usuario accese a la computadora remota como si el teclado o monitor de dicho usuario estuvieran directamente conectados a ella. El usuario puede entonces ejecutar cualquier comando o programa de aplicación.

Telnet permite controlar totalmente otra máquina desde largas distancias a través de internet, la máquina remota debe estar ejecutando el mismo programa que reciba y gestione las conexiones.

Muchas empresas en la actualidad que ofrecen servicios a sus clientes utilizan este servicio de acceso remoto para dar soporte desde largas distancias. Un ejemplo de telnet tenemos teamviewer, una herramienta muy conocida.

6.1.8.3.5 Voz IP

Para Andreu (2011), voz sobre ip o tambien conocido como VoIP (Voice Over Internet Protocol) es un servicio que permite trasnmitir voz usando el protocolo IP. En concreto se refiere a la capacidad de transmitir voz a traves de Internet. Pero no se trata de una radio por internet, sino algo mas complejo.

Voz sobre IP se refiere a la transmisión del tráfico de voz sobre redes basadas en Internet en lugar de las redes telefónicas tradicionales.

En la actualidad en Nicaragua, muchas empresas optan por el servicio de telefonía IP, ahorrándose en otro pago por servicio de telefonía, porque únicamente pagan el servicio de Internet y realizan las llamadas con muchísima duración.

6.1.8.3.6 Servidor Web

Colobran Huguet, Arqués Soldevila, & Galindo (2008), afirman que el servidor web es un recurso con el cual la organización da acceso a la informacion que quiere publicar. Este servidor web, por ejemplo, podría dar servicios solo a usuarios de una red local, o quizás una intranet, o como en la mayoría de los casos, dar una puerta de acceso libre para cualquier usuario conectado a la red internet.

Este servidor permite alojar las páginas web y mostrarlas a usuarios dentro de la red o incluso cualquier usuario externo con acceso a Internet.

Hoy en día pequeñas, medianas y grandes empresas en Nicaragua poseen su servidor web para brindar información de cualquier índole.

6.1.8.3.7 Servicio de correo electronico

Según Carmona Romera (2014), el correo electrónico es un servicio de red que permite el envío y recepción de mensajes mediante un sistema de comunicación.

El servicio de correo electrónico, es otro servicio que permite el intercambio de mensajes a través de sistemas de comunicación en red.

En la actualidad las empresas optan por su servidor de correo electrónico interno para aprovechar la red que tienen implementada, ya que los beneficios obtenidos son innumerables, como su uso muy fácil e intuitivo.

6.1.8.3.8 VLAN

Cisco Systems (2007), LAN virtual, grupo de dispositivos en una LAN que se configuran (usando software de administracion) de modo que se pueda comunicar como si estuvieran conectados al mismo cable cuando, de hecho, están ubicados en una segmentación de LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son muy flexibles.

Las VLANs son redes de área local que agrupa un conjunto de equipos de manera lógica y no física.

La importancia de las VLANs en la actualidad es que las pequeñas, medianas y grandes empresas que cuentan con muchas áreas, permitan organizar de manera lógica y ordenada sus VLANs para una mejor administración, como lo es en el caso de la UNAN, Managua FAREM- Matagalpa.

6.1.8.3.9 Ancho de banda

Para Cisco systems (2007), es la cantidad de datos que se puede trasmitir en una cantidad de tiempo determinada. En el caso de ancho de banda digital, en general se expresa en bit por segundo (bps). En el caso de ancho de banda analógica, se expresa en ciclos por segundo, o Hertz (HZ).

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 un ancho de banda regular de hasta 20 Mbps de descargar, en comparación a otros países desarrollados como Estados Unidos con google fiber que ofrece velocidades de descarga hasta de 1 Gbps.

6.1.8.3.10 Firewall

Cisco systems (2007), es un dispositivo de hardware o una conexión de software disenado para proteger los dispositivos de red de los usuarios externos de la red y/o de aplicaciones y archivos maliciosos.

Es un dispositivo tanto lógico como físico que filtra el tráfico que viene desde el exterior hacia el interior, evitando ataques o archivos maliciosos.

Muchas entidades en la actualidad son tan cuidadosas con su información que para evitar ataques o robos de información, instalan un firewall en su red.

6.1.8.3.11 VPN (Virtual Private Network)

Para López (2010), las Redes Privadas Virtuales son conocidas a menudo como conexiones VPN (Virtual Private Network). A través de una red VPN los datos viajan cifrados y solamente podran ser descifrados por el destinatario y, por supuesto, por el emisor, por lo cual todo el proceso resulta transparente para ambas partes. De este modo no quedan expuestos a la captacion fraudulenta en su camino por la red.

El VPN permite crear una conexión segura a otra red a través del Internet. Cuando conectas cualquier dispositivo a un VPN, este actúa como si estuviese en la misma red que la que tiene el VPN y todo el tráfico de datos se envía de forma segura a través del VPN.

Hoy en día las empresas que manejan grandes flujos de información como sus ganancias, información confidencial que no puede ser vista por cualquiera, antes de evitar cualquier robo de información en la red usan VPN para transportar su información de forma segura y sin ningún riesgo.

6.1.8.3.12 Central VoIP

Según Moya & Huidobro (2006), una centralita IP o una IP-PBX es una centralita telefónica que trabaja internamente con el protocolo IP. De esta manera, utiliza la infraestructura de comunicaciones de datos (LAN y WAN) para realizar sus funciones. Las centralitas IP pueden por tanto conectarse a servicios públicos VoIP, pero también tienen la capacidad de trabajar con líneas convencionales de teléfono analógicas o digitales (RDSI).

Es una central telefónica que utiliza dispositivos especiales para VoIP, que funcionan como un teléfono normal y pueden trabajar de igual manera con teléfonos convencionales.

En los bancos y universidades de Nicaragua, en la actualidad poseen centrales telefónicas de VoIP para evitar gastos en pago de servicio de teléfono, usando solamente su infraestructura de red y dispositivos especiales para esto.

6.1.8.4 Políticas de seguridad lógicas

López (2010), consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Las políticas de seguridad lógicas de una entidad, son normas que los trabajadores de dicha entidad deben respetar y cumplir para la protección total de su información.

En la actualidad la mayoría de empresas como: bancos, universidades, empresas privadas, cuentan con sus políticas de seguridad lógicas definidas, con el objetivo de proteger su información de manera directa y más cuando esta se encuentra en red.

6.1.8.5 Amenazas lógicas

Según cisco (2007), algunas amenazas lógicas son:

- ✓ Ingeniería social: enganar a las personas con páginas engañosas para que proporcionen información valiosa.
- ✓ Ataques de reconocimientos: Es el descubrimiento y la asignación no autorizados de sistemas, servicios o vulnerabilidades.
- ✓ Ataques de acceso: Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios de FTP y los servicios Web para obtener acceso a cuentas Web, bases de datos confidenciales y otra información confidencial.
- ✓ Ataques a las contraseñas: Los ataques a las contraseñas pueden implementarse mediante un programa detector de paquetes para proporcionar cuentas de usuarios y contraseñas que se transmiten como texto sin cifrar
- ✓ Explotación de confianza: El objetivo de un ataque de explotación de confianza es comprometer un host de confianza, mediante su uso, con el fin de llevar a cabo ataques en otros hosts de una red.
- ✓ Ataque man-in-the-middle: Los ataques man-in-the-middle (MITM) son realizados por agresores que logran ubicarse entre dos hosts legítimos. El agresor puede permitir que se realicen transacciones normales entre hosts, y manipular la conversación entre ambos sólo periódicamente.

- ✓ Ataques de DoS: En definitiva, impiden que las personas autorizadas utilicen un servicio consumiendo recursos del sistema.
- ✓ Ping de la muerte: Estos ataques modificaron la parte IP de un encabezado de paquete de ping para indicar que hay más datos en el paquete de los que realmente había.
- ✓ Ataques DDos: Los ataques de DoS distribuida (DDoS) están diseñados para saturar los enlaces de la red con datos legítimos.
- ✓ Los ataques Smurf: utilizan mensajes ping de broadcast suplantados para saturar un sistema objetivo.
- ✓ Ataques de código malicioso: Las principales vulnerabilidades de las estaciones de trabajo de los usuarios finales son los ataques de gusanos, virus y caballos de Troya.

Las redes de datos son atacadas principalmente por personas, quienes intencionalmente o no, pueden afectar a los elementos o recursos interconectados. No se puede descartar a aquellas amenazas lógicas que fueron creadas para dañar (software malicioso o malware) o incluso fallas en la programación de las aplicaciones (bugs o agujeros), que aun no siendo su fin, pueden ocasionar daños o perdidas.

Las empresas u organizaciones en la actualidad, no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente, sin embargo los administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas, pero estas amenazas no pueden ser eliminadas en su totalidad ya que existen muchos atacantes en la red que quieren tratar de robar información o hacer danos en las redes o sistemas informáticos

6.2 ISO/IEC 27002:2013

“ISO/IEC 27002:2013 se refiere a una serie de aspectos sobre la seguridad de las tecnologías de información. Este Estándar Internacional va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las

probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo". (Chacón, Erazo, España, Montoya, & Portillo, 2008)

La ISO/IEC 27002:2013 se trata de una serie de pasos que se establecen para dar cumplimento a buenas prácticas de controles de seguridad de la información, para mantener seguro e íntegro el patrimonio de las empresas.

En la actualidad el estándar ISO/IEC 27002:2013 aporta controles y técnicas que permiten a las empresas aplicar buenas prácticas para mantener su información segura e integra.

6.2.1 Concepto

Según [3]nimbosystems (2013), ISO/IEC 27002:2013 publicada en 2012, 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 39 objetivos de control y 133 controles los cuales están agrupados en 11 dominios.

La ISO/IEC 27002:2013 no es para fines de certificación, esta brinda una muy buena guía para la administración de la seguridad de la información de una institución, permitiéndole adoptar buenas prácticas que ayuden a mantener la integridad y disponibilidad de los datos.

Actualmente ISO/IEC 27002:2013 no permite que una empresa sea certificada mediante este estándar, pero otorga una serie de controles que permiten aplicar buenas prácticas en cuanto a seguridad de la información se refiere.

6.2.2 Controles

"Control consiste en la medición y corrección del desempeño con la finalidad de asegurarse de que se cumplan los objetivos de la empresa y los planes para lograrlo". (Koontz & Weihrich, 2007)

[3] **Nimbosystems:** es una empresa orientada a suplir las necesidades de información de nuestros clientes por medio de diversos servicios innovadores, nuestra experiencia en implementaciones de proyectos, nuestro conocimiento de buenas prácticas y estándares nos permiten ofrecerle servicios de calidad, que cumplan las expectativas de los clientes en los plazos acordados.

Los controles son un proceso que ayudan a verificar si los planes se están cumpliendo o no, esto permite controlar si existen avances en cuanto al cumplimiento de los objetivos y permite corregir desviaciones a tiempo.

Hoy en día todas las empresas e instituciones, poseen como una actividad principal y administrativa el control que les permita verificar el desempeño de las distintas áreas y funciones de la organización.

6.2.2.1 Políticas de Seguridad

Según (ISO, 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.

Las políticas de seguridad están basadas en contextos en el que opera una organización, institución o empresa, estas se redactan bajo los fines y objetivos de la organización.

Actualmente las empresas, instituciones, organizaciones, etc. Adoptan este tipo de documentos para alcanzar y cumplir sus objetivos, donde reflejan los controles necesarios que fundamenten las políticas creadas de acuerdo a su estructura organizativa.

6.2.2.1.1 Directrices de la dirección en seguridad de la información

Según (ISO, 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.

Las líneas de las políticas deben estar alineadas de acuerdo a sus objetivos, de tal manera que son aprobadas desde el más alto nivel directivo y son comunicadas a toda la organización de una manera comprensible. Estas líneas de políticas de seguridad deben contemplar de manera esencial aspectos importantes de la

seguridad de la información como son: confidencialidad, integridad, disponibilidad y autenticidad.

Hoy en día grandes instituciones u organizaciones actualizan de manera periódica sus líneas de políticas de seguridad, esto en función del análisis de riesgos, cambios estructurales o como el fruto de la misma experiencia.

6.2.2.1.1.1 Conjunto de Políticas para la Seguridad de la Información

Para (ISO, 2012), se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.

Las empresas o instituciones deben crear un documento de carácter público, donde reflejen su conjunto de políticas de acuerdo a sus objetivos, permitiendo a los empleados conocer dichas políticas a las que están sujetos.

Toda empresa o institución actual da a conocer a cada uno de sus trabajadores las políticas de trabajo de la institución a la cual todos ellos están sujetos.

6.2.2.2 Aspectos organizativos de la seguridad de la información

Según (ISO, 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.

Para lograr este objetivo la organización debe definir formalmente su ámbito de gestión para efectuar tareas tales como la aprobación de políticas de seguridad, coordinación de la implementación de seguridad y asignación de funciones y responsabilidades a cada uno de sus miembros.

Al día de hoy toda organización con objetivos serios y bien definidos, organiza de forma eficaz y correcta sus aspectos enfocados a la seguridad de la información, por lo cual les permite cumplir forma eficiente sus objetivos.

6.2.2.2.1 Organización interna

Para (ISO, 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.

Es importante que en toda institución la alta gerencia se preocupe por establecer y mantener políticas de seguridad de la información, contemplando los elementos claves de seguridad tales como: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad.

Actualmente en las mayorías de instituciones se cuentan con estrictas políticas de seguridad, esto con el fin de darle una mayor protección a su información.

6.2.2.2.1.1 Segregación de tareas

Para (ISO, 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 deben de asignar tareas y responsabilidades a cada área de trabajo, para poder controlar la información de forma más eficiente, garantizando así un mayor nivel de seguridad de los datos, evitando así la violación de la integridad de los datos.

En la actualidad las instituciones asignan responsabilidades a cada área de trabajo, esto con el fin de llevar un control más riguroso de la información, para así evitar manipulaciones no autorizadas de esta.

6.2.2.3 Seguridad ligada a los recursos humanos

Según (ISO, 2012), el objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al

desarrollo de sus funciones y de las expectativas depositadas en ellos en materia 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 instituciones deben de explicar cuáles son las responsabilidades en materia de la seguridad de la información en la etapa de contratación de nuevo personal, así como garantizar que el personal esté capacitado sobre cuáles son los mecanismos de seguridad de la información y las responsabilidades que esta conlleva.

Actualmente las instituciones ejercen planes de capacitación al nuevo personal contratado y el personal antiguo, logrando así reducir riesgos que pongan en peligro la integridad de la información.

6.2.2.3.1 Antes de la contratación

Para (ISO, 2012), las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo. Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles.

Es importante que antes de la contratación de un personal para un trabajo, este conozca cuales son las responsabilidades en cuanto a seguridad de información se refiere, con el fin de evitar fugas de información o daños que afecte a la entidad.

Hoy en día las instituciones cuidan mucho su información, por consiguiente, empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.

6.2.2.3.1.1 Investigación de antecedentes

Según (ISO, 2012), se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Las empresas deben realizar revisiones de los antecedentes del nuevo personal que aplica a las vacantes de trabajo, esto permite controlar y administrar el recurso humano, logrando evitar riesgos de índole humano en cuanto a la seguridad de la información se refiere.

Hoy en día toda persona natural que aplica para una vacante de trabajo debe de demostrar su profesionalismo y ética mediante sus antecedentes de trabajo, esto le permite a la organización contratante controlar el dominio y correcto uso de la información.

6.2.2.3.1.2 Términos y condiciones de contratación

Según (ISO, 2012), como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

Las empresas poseen un documento formal donde exponen sus términos y condiciones para la contratación de nuevo personal, toda persona que aplique a la plaza de trabajo debe de cumplir con esto parámetros para así poder competir por el puesto de trabajo.

En la actualidad toda institución posee un documento donde detalla sus términos y condiciones de contratación, en este se estipulan cuáles son las responsabilidad y pautas que deben cumplir los nuevos aspirantes de una plaza de trabajo.

6.2.2.3.1.3 Durante la contratación

Para (ISO, 2012), se debería definir las responsabilidades de la dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.

En la contratación todos los usuarios empleados, contratistas y terceras personas se les deberían proporcionar capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

En la actualidad la mayoría de entidades les brindan capacitaciones continuas a sus empleados con el fin de minimizar posibles riesgos de seguridad en su información.

6.2.2.3.1.4 Concienciación, educación y capacitación en seguridad de la información

Según (ISO, 2012), todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Toda empleado de una institución debe de estar capacitado en seguridad de la información de acuerdo a su área de trabajo, dado que esto le permitirá velar por el cumplimento de la integridad de los datos.

Hoy en día las instituciones están sujetas a dar capacitaciones constantes a los empleados en cuanto a seguridad de la información se refiere.

6.2.2.4 Gestión de activos

Según (ISO, 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 debe de clasificar su información, de acuerdo a la sensibilidad que esta contiene, con el objetivo de explicar cómo será procesada y protegida la información.

Actualmente las instituciones gestionan sus activos empleando mecanismo que le permiten asegurar la información y reducir los riesgos.

6.2.2.4.1 Responsabilidad sobre los activos

Para (ISO, 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 término “propietario” identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona disponga de los derechos de propiedad reales del activo.

En la actualidad en las instituciones se hacen usos de códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados.

6.2.2.4.1.1 Inventario de activos

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

Todos los recursos con los cuenta la organización deben de ser claramente identificados en un inventario donde debe estar contenido todo los activos que posee la organización.

En las instituciones o empresas de hoy en día, el inventario es uno de los más importante recursos de información con lo que se cuenta, esto debido a que contiene la información de los recursos con los que se cuenta, para poder subsistir.

6.2.2.4.1.2 Uso aceptable de los activos

Según (ISO, 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.

Existe una normativa donde se estipula cual y como debe de ser el uso de cada activo que posee la institución, esto con el fin de salvaguardar la información.

Actualmente las instituciones velan porque se haga un correcto uso de sus activos, considerando que esto les permite administrar de forma correcta sus recursos y mantener segura su información.

6.2.2.4.2 Manejo de los soportes de almacenamiento

Para (ISO, 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.

El objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.

Actualmente algunas entidades desechan equipos de cómputo con soportes de almacenamiento que aun poseen información, descuidando información de mucha importancia que puede ser usada por otros.

6.2.2.5 Control de accesos

Según (ISO, 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 información debe de estar protegida mediante técnicas de control que permitan mantener la integridad de los datos y evitar que esta sea manipulada de forma no autorizada.

En la actualidad las organización cuentan con medidas que restringen el acceso a la información por entes no autorizados, esto ayuda a evitar que la integridad de los datos sean alterados, para lograr mantener la confiabilidad de la información.

6.2.2.5.1 Requisitos de negocio para el control de accesos

Según (ISO, 2012), se deberían controlar los accesos a 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.

El objetivo esencial es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.

Actualmente en grandes instituciones u organizaciones usan sistemas de control de accesos, como lo es en ENACAL, Managua, Nicaragua, usa tarjetas magnéticas para acceder al centro de datos, además de una autenticación de usuario y contraseña.

6.2.2.5.1.1 Política de control de acceso

Para (ISO, 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 establecer con el fin de dar solución a las necesidades de mantener la seguridad de los datos.

Al día de hoy toda institución implementa sus propias políticas de seguridad, en dependencia de las necesidades que esta posee, en cuanto a seguridad de la información se refiere.

6.2.2.5.1.2 Control de acceso a las redes y servicios asociados

Según (ISO, 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.

El control de acceso a las redes tiene como objetivo asegurar que todos los usuarios que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información, entre otras.

Actualmente para muchas empresas, la información y tecnologías que la soportan representan sus más valiosos activos, por lo tanto el control de acceso a las redes es de suma importancia puesto que cada vez las empresas tienen redes más distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas.

6.2.2.5.2 Gestión de acceso de usuarios

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

Los procedimientos de acceso a los sistemas y servicio se deben definir como controles que permitan controlar la manipulación de la información.

Actualmente las empresas poseen procedimientos de gestión de usuarios que les permiten controlar el acceso y manipulación de los sistemas por parte de ellos, ya sea mediante controles de usuarios como lo son los login, bitácoras del sistema.

6.2.2.5.2.1 Gestión de altas/bajas en el registro de usuarios

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

Debe de existir un procedimiento de seguridad en el cual se especifique que se deben de dar de baja todos aquellos usuarios del sistema que ya no laboran

dentro de la institución y dar prioridad de dar alta a todos aquellos usuarios que deben poseer privilegios de acceso a los sistemas.

Actualmente las organizaciones implementan sus propios procedimientos de control, que permite organizar el acceso a la información, permitiendo así que solo usuarios activos y autorizados tengan acceso a la información.

6.2.2.5.2.2 Gestión de los derechos de acceso con privilegios especiales

Para (ISO, 2012), la asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

La asignación y uso de derechos de acceso con privilegios especiales debe ser restringido y controlado, para poder administrar correctamente la asignación de privilegios.

Actualmente se el control de la información se otorga mediante privilegios, donde usuarios especiales poseen privilegios especiales en cuanto a la manipulación general de la información se refiere, por ejemplo un privilegio puede ser el control total para manipular la información de los sistemas.

6.2.2.5.3 Control de acceso a sistemas y aplicaciones

Según (ISO, 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.

El objetivo esencial es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

Actualmente en instituciones se llevan a cabos muchos procedimientos para descartar activos que contengan información valiosa de la institución.

6.2.2.5.3.1 Restricciones de acceso a la información

Para (ISO, 2012), se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

Es decir se debe de implementar una política de control de acceso a información, donde solo los usuarios autorizados puedan tener acceso la información de los sistemas.

En la actualidad la organización se rigen mediante políticas que permiten controlar el acceso a la información de los sistemas, logrando así llevar un control específico sobre las normativas de acceso definidas.

6.2.2.5.3.2 Gestión de contraseñas de usuarios

Según (ISO, 2012), los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

Se debe de capacitar a los usuarios, para que estos implementen contraseñas que contengan un formato fuerte de seguridad, para evitar así que terceras personas se adueñen de sus credenciales de acceso al sistema.

Hoy en día la gestión de contraseñas está muy ligada a la seguridad de la información, ya que las organizaciones deben de incluir dentro de sus políticas de seguridad un formato estándar de implementación de contraseña, que les permita asegurar que las credenciales de los usuarios no sean violentadas.

6.2.2.6 Cifrado

Según (ISO, 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.

El cifrado de la información es uno de los elementos más importantes de seguridad, ya que permite que esta no sea modificada y permite que esta viaje por la red de forma segura.

Actualmente las instituciones implementan cifrado en la transmisión de su información, esto con el fin de que riegos que atenten contra la integridad de esta se sinteticen.

6.2.2.6.1 Controles criptográficos

Para (ISO, 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 garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Actualmente algunas organizaciones utilizan controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

6.2.2.6.1.1 Políticas de uso de controles criptográficos

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

Mediante las políticas de seguridad de la información, se deben de establecer el uso de cifrado de la información para permitirá la administración de este tipo de control.

Actualmente dentro de las políticas de seguridad de las instituciones se implementa el uso del cifrado de los datos, para evitar que la información sea alterada y modificada cuando esta es compartida en el medio.

6.2.2.6.1.2 Gestión de claves

Para (ISO, 2012), se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

Debe de existir una política donde se establezca el ciclo de cambio del tipo de cifrado utilizado cada cierto tiempo, esto con el fin de evitar que este control sea violentado.

En la actualidad las organizaciones que implementan cifrado para mantener la seguridad de la información, deben de contar con una política que les indique cada cuanto tiempo se debe de cambiar el tipo de criptografía implementada.

6.2.2.7 Seguridad física y ambiental

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

Deben de existir políticas que permitan minimizar los riesgos de la seguridad física y del entorno ambiental, con el fin de evitar que los medios físico que contienen la información sean alterados ya sea por factores humanos o factores ambientales.

Actualmente las instituciones implementan políticas de seguridad que les permiten salvaguardar la información de factores ambientales y humanos, permitiéndoles estar preparadas en caso de que algo salga mal, esto también lo cumplen mediante planes de contingencia previamente estipulados.

6.2.2.7.1 Áreas seguras

Para (ISO, 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. Los

medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

La finalidad de áreas seguras es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

En la actualidad organizaciones que cuidan la información y las TI tienen búnker contra incendios, temblores u otros desastres naturales o daños que puedan ocasionar el mismo hombre.

6.2.2.7.1.1 Controles físicos de entrada

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

Se debe contar con un control estricto a los medios físicos que contienen la información, donde solo el personal autorizado pueda tener acceso a manipular la información.

En la actualidad las organizaciones implementan controles que regulan el acceso físico a los sistemas que contienen y controlan la información, esto les permite evitar que la información pueda ser controlada por personas no autorizadas.

6.2.2.7.1.2 Seguridad de oficinas, despachos y recursos

Según (ISO, 2012), se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.

Las instalaciones físicas deben de contar con las medidas de seguridad necesarias que permitan mantener la información segura e integra.

Las instituciones hoy en día deben de implementar normativas en el diseño y construcción de sus instalaciones, tomando en cuanta niveles de seguridad en dependencia del recurso estipulado, es decir existirán áreas con niveles de

seguridad más altas que otras, por ejemplo el centro de datos de la empresa es uno de lugares con más políticas de seguridad física implementadas para asegurar la seguridad y calidad de la información

6.2.2.7.1.3 Protección contra amenazas externas y ambientales

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

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

Actualmente las organizaciones cuentan con medidas de seguridad y planes de contingencia que les permiten minimizar riesgos y tomar decisiones cuando se presentan algún evento con índole ambiental o ataque lógicos desde fuera de la red.

6.2.2.7.2 Seguridad de los equipos

Según (ISO, 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.

La finalidad de este objetivo es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

Hoy en día es prácticamente imposible considerar a los equipos informáticos como entes aislados, si consideramos al ordenador como un elemento individual hay sólo tres elementos sobre los que tendremos que incidir para evitar agujeros de seguridad:

- Evitar accesos locales al equipo por parte de personas no deseadas.
- Evitar la contaminación del equipo por parte de elementos perniciosos que puedan dañar o ralentizar el funcionamiento del mismo, y que se aprovechan fundamentalmente de los sistemas de almacenamiento portátiles (llaves USB, tarjetas SD, discos duros portátiles) y/o de los sistemas de comunicación.
- Evitar agujeros de seguridad mediante el mantenimiento actualizado del equipo informático, su sistema operativo y los programas que utilicemos.

6.2.2.7.2.1 Seguridad del cableado

Para (ISO, 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 implementado y que cumple todos los parámetros para la seguridad de la información.

Actualmente las empresas se rigen mediante normas internacionales de seguridad del cableado, para dar cumplimiento con parámetros de seguridad y calidad en las comunicaciones y trasmisión de la información.

6.2.2.7.2.2 Mantenimiento de los equipos

Según (ISO, 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.

Hoy en día las instituciones dan soporte técnico a sus equipos informáticos cada cierto tiempo, por lo general se hace cada seis meses, con el fin de garantizar la integridad, continuidad y disponibilidad de estos.

6.2.2.7.2.3 Seguridad de equipos y activos fuera de las instalaciones

Para (ISO, 2012), se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

Si la institución posee activos fuera de las instalaciones físicas de esta, debe de velar también por el cumplimiento de políticas de seguridad y garantizar la integridad de los datos en dichos activos.

Muchas empresas hoy en día, poseen activos fuera de la organización física de esta, es decir pueden estar fuera de sus instalaciones pero siguen siendo parte esencial de ella misma, es decir no siempre todos los recursos de una institución están centralizados en un mismo lugar.

6.2.2.8 Seguridad Operativa

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

La seguridad operativa aplica procedimientos que permiten el desarrollo y documentación de los procesos que se llevan a cabo con la información de la institución.

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

6.2.2.8.1 Responsabilidades y procedimientos de operación

Para (ISO, 2012), se debe asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados. Se deberían establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Se debería implantar la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

Las empresas e instituciones se deben encargar de implementar operaciones apropiadas para que permitan un correcto procesamiento de su información, esto con el fin de reducir los riesgos que ponen el peligro la integridad de la información, debido al mal uso de la información.

Hoy en día las empresas e instituciones están implementando buenas prácticas en la operación y manipulación de la información, ya que están consiente de la importancia de mantener en todo momento la integridad de la información.

6.2.2.8.1.1 Documentación de procedimientos de operación

Según (ISO, 2012), se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

Se deben documentar todos los procedimientos operativos que se llevan a cabo en la institución, con el objetivo de servir como guía para los usuarios que necesiten capacitarse en dichos procesos.

Las empresas de hoy en día documentan sus procedimientos de operación, para que sirvan como guía a aquellos usuarios que necesitan controlar un proceso, aplicando las normativas necesarias para dar cumplimiento a la seguridad de la información.

6.2.2.8.1.2 Gestión de cambios

Para (ISO, 2012), se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.

Las instituciones deben de controlar y documentar todos los cambios que se implementan y afectan a la seguridad de la información.

Actualmente en las instituciones se debería cumplir con este control, ya que permite conocer cómo se comporta la información cuando se implementan nuevos cambios y así poder construir una infraestructura más sólida que permita asegurar la información.

6.2.2.8.1.3 Gestión de capacidades

Según (ISO, 2012), se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

Se deben implementar monitoreos que permitan establecer pautas que definan los futuros crecimientos a largo plazo, esto con el fin de ajustar y garantizar el correcto rendimiento de los recursos.

Actualmente se implementan planes de gestión que permiten especular sobre el crecimiento a corto y largo plazo, que sirven como guía para medir las inversiones y proyecciones futuras.

6.2.2.8.2 Protección contra código malicioso

Para (ISO, 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 malware se refiere específicamente a software malicioso, pero el código malicioso incluye además scripts de sitios web (applets de Java, controles de ActiveX, contenido insertado, plug-ins, lenguajes de scripts u otros lenguajes de programación en páginas web y correo electrónico) que pueden aprovechar vulnerabilidades con el fin de descargar un malware.

Los códigos maliciosos son la causa número uno de robo de información y violación de la integridad de los datos, es por eso que se deben de implementar mecanismos que permitan identificar y contrarrestas ataques que pongan en peligro la seguridad de la los datos de información.

En la actualidad se implementan mecanismos de seguridad que permiten identificar códigos maliciosos que se mueven mediante los medios de transmisión o se ejecutan en los equipos, tal como es el uso de software antimalware, antivirus, servidor proxy, firewalls entre otros.

6.2.2.8.2.1 Controles contra código malicioso

Según (ISO, 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 controles que minimicen el riesgo que conllevan los códigos maliciosos, para asegurar que la información este integra y disponible en todo momento.

Actualmente existen múltiples controles tales como antivirus, firewalls, antimalware, etc, que permiten a la institución evitar que códigos maliciosos pongan en riesgo la integridad de los datos de información.

6.2.2.8.3 Copias de seguridad

Para (ISO, 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.

Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes.

Aplique técnicas de cifrado a copias de seguridad y archivos que contengan datos sensibles o valiosos (en realidad, serán prácticamente todos porque, si no, ¿para qué hacer copias de seguridad?).

Se deben definir e implementar mecanismos de recuperación que permitan salvaguardar la información y establecer la continuidad del negocio. La identificación de los datos más sensibles es el primer procedimiento a realizar, ya que estos son el rubro más importante de toda empresa o institución.

Hoy en día existen múltiples mecanismo de recuperación de datos, las copias de seguridad son el principal eje en la continuidad de las empresas e instituciones, es por eso que se implementan respaldos de información mediante servidores internos o externos que permiten salvaguardar los datos de información más sensibles.

6.2.2.8.3.1 Copias de seguridad de la información

Para (ISO, 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.

Las copias de seguridad son un elemento fundamental en la continuidad de los procesos de una institución en caso de que algo falle.

Actualmente toda institución debe de contar con respaldo físicos y lógicos de su información, tanto de forma interna a ella como externa, es decir deben poseer respaldos fuera de las instalaciones físicas, en caso de que algo falle existirá un respaldo de la información.

6.2.2.8.4 Registro de actividad y supervisión

Según (ISO, 2012), los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.

El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información.

La organización debería cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades. El monitoreo del sistema debería ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad del modelo de política de acceso.

El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información.

La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico.

Se debe analizar la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información.

6.2.2.8.4.1 Registro y gestión de eventos de actividad

Para (ISO, 2012), se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.

Es necesario poseer un registro de la actividad de la información ya que estos permitirán identificar el origen de los eventos de seguridad de la información.

En la actualidad se implementan servidores que permiten monitorear y controlar la actividad del uso de la información, registrando la actividad de cada uno de los

usuarios que manipulan los datos, por lo cual ayuda a prevenir e identifica los eventos que ponen en riesgos la información.

6.2.2.8.5 Consideraciones de las auditorías de los sistemas de información

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

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

Limitar las verificaciones (p.ej. a un acceso de "sólo lectura" en software y datos de producción) y/o tomar las medidas necesarias a efectos de aislar y contrarrestar los efectos de modificaciones realizadas al finalizar la auditoría (eliminar archivos transitorios, entidades ficticias y datos incorporados en archivos maestros; revertir transacciones; revocar privilegios otorgados).

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 deben documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

6.2.2.8.5.1 Controles de auditoria de los sistemas de información

Según (ISO, 2012), 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.

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.

En la actualidad toda institución está sujeta a constantes controles de auditorías de los sistemas de información, esto ayuda a minimizar riesgos mediante las recomendaciones que se establecen al concluir cada auditoria.

6.2.2.9 Seguridad en las telecomunicaciones

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

Se debe implementar controles adicionales que permitan la protección de la información que se transmite a través de las redes.

En la actualidad las organizaciones implementan mecanismos de seguridad lógica que permiten que la información viaje segura a través del medio de transmisión, protegiéndola contra las amenazas que atentan contra la integridad y manipulación de los datos.

6.2.2.9.1 Gestión de la seguridad en las redes

Para (ISO, 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 si se garantizan:

a) Que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones.

b) Que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos.

c) El cumplimiento del control de los accesos de los usuarios a los servicios de información.

Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).

Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

6.2.2.9.1.1 Controles de Red

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

Se deben controlar los accesos a los servicios internos y externos conectados en red, con el propósito de administrar de forma eficiente el acceso a la información.

Hoy en día toda organización que hace uso de redes, implementa controles que le permiten mantener una administración rigurosa y detallada sobre la información que es accedida y se manipula mediante la red, ya sea desde adentro o desde afuera.

6.2.2.9.1.2 Mecanismos de seguridad asociados a servicios de red

De acuerdo a (ISO, 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.

6.2.2.9.1.3 Segregación de redes

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

La segmentación de las redes permite establecer grupos red específicos que sean independientes a los demás grupos, es decir permite crear distintas áreas de comunicación de datos todas interdependientes entre ellas.

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 es decir, permite organizar la información de acuerdo a su fin y solo da acceso a los usuarios autorizados a manipular dicha información.

6.2.2.9.2 Intercambio de información con partes externas

Según (ISO, 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.

Estudie canales de comunicaciones alternativos y "pre-autorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes.

El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.

6.2.2.9.2.1 Políticas y procedimientos de intercambio de información

Conforme a (ISO, 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 todo los medios por donde se mueve, es decir desde que se emite, se trasmite y se recepciona.

Las instituciones en la actualidad aplican estas políticas y procedimientos, porque su fin en el de asegurar que la información se mueva se transmita de forma íntegra.

6.2.2.9.2.2 Acuerdos de intercambio

De acuerdo a (ISO, 2012), los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

Se deben implementar acuerdos que den prioridad a la confidencialidad e integridad de la información, con el fin de evitar que esta sea manipulada y corrompida.

Las empresas e instituciones tienen el deber de estableces y cumplir los acuerdos de intercambio.

6.2.2.9.2.3 Mensajería electrónica

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

Se deben aplicar mecanismo 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.

Actualmente muchas empresas posees su propio servicio de correo electrónico, por lo cual implementan técnicas y mecanismo de seguridad que eviten ataques tales como Ddos, spam, physing, etc.

6.2.2.9.2.4 Acuerdos de confidencialidad y secreto

Para (ISO, 2012), se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

Toda institución sabe que su mayor y más importante activo es su información, es por eso que se deben de crear normas de acuerdos de confidencialidad y sigilo, a las cuales los usuarios deben de dar cumplimiento.

Actualmente las instituciones están siempre en la búsqueda e implementación de nuevas técnicas que permitan mantener la confidencialidad de su información, es por es que implementan normativas en las cuales se estipula como se debe de dar cumplimiento a la confidencialidad de la información y el grado de sigilo que esta conlleva.

6.2.2.10 Relaciones con suministradores

De acuerdo con (ISO, 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 deben de verificar el cumplimiento de los acuerdos de los servicios contratados a terceros, con el objetivo de verla por el cumplimiento de un servicio de calidad.

6.2.2.10.1 Gestión de la prestación del servicio por suministradores

Según (ISO, 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.

6.2.2.10.1.1 Supervisión y revisión de los servicios prestados por terceros

Para (ISO, 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.

Por lo general, se controla que el proveedor cumpla con los requisitos del contrato, y brinde un servicio de calidad.

6.2.2.11 Gestión de incidentes en la seguridad de la información

Según (ISO, 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 organizaciones cuentan con muchos activos, y cada de uno de ellos están expuestos a sufrir incidentes que atenten contra su seguridad.

Actualmente las empresas deben de contar con la capacidad de gestión contra incidentes, para que puedan detectar y tratar dichos incidentes y prevenir futuros incidentes de la misma índole.

6.2.2.11.1 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-incidente 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, contratistas y terceros deberían estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales.

Se les debería exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado.

6.2.2.11.1.1 Responsabilidades y procedimientos

Para (ISO, 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.

Es necesario establecer tanto las responsabilidades de cada parte como los procedimientos a seguir en dependencia de los incidentes asociados a la seguridad de los datos.

En la actualidad las empresas e instituciones deben de aplicar procedimientos para gestionar de manera adecuada los incidentes de seguridad, con el fin de obtener una solución rápida y viable ante cualquier incidente materializado.

6.2.2.11.1.2 Notificación de eventos de seguridad de la información

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

Los incidente de la seguridad de la información se deben de informar enseguida que se detecten riesgos o se concreticen, esto con el fin mantener informada a la institución sobre los que pasa con su información y tomar medidas de seguridad.

Actualmente si una empresa no cuenta con la organización necesaria para notificar el evento que ocurre con la seguridad de la información, no le permitirá adecuar los mecanismos necesarios para darse cuenta si la información mantiene en su estado integro.

6.2.2.11.1.3 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 informar inmediatamente que se encuentre un punto débil, para así poder aplicar lo mecanismo necesarios para fortalecer la seguridad y así evitar que la integridad de la información sea violada.

Actualmente existen miles de mecanismos de ataque que buscan penetrar en los sistemas de las instituciones para poder manipular la información, si no se notifican los puntos débiles de seguridad tendrá como consecuencia que alguno de estos mecanismo lograra encontrar la puerta para violentar la seguridad de los datos, es por eso que las instituciones deben de notificas cada mínimo detalle que ponga en peligro a la información.

6.2.2.11.1.4 Valoración de eventos de seguridad de la información y toma de decisiones

Conforme a (ISO, 2012), se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.

Los incidentes se deben clasificar en dependencia el grado de peligro e impacto que representa para la seguridad de la información.

Es una obligación de las empresas o instituciones revisar los eventos y proponer soluciones para minimizar el impacto de estos.

6.2.2.11.1.5 Aprendizaje de los incidentes de la seguridad de la información

Según (ISO, 2012), se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.

Cuando se materialicen incidentes que atenten contra la seguridad se deben de documentar para poder aplicar mecanismo de seguridad y así poder reducir la probabilidad de que en un futuro se materialice nuevamente.

En la actualidad las organizaciones deben de aprender a documentar todo aquel incidente que atente contra la seguridad de la información, ya que esto les permitirá evitar que en un futuro vuelva a ocurrir el mismo incidente.

6.2.2.11.1.6 Recopilación de evidencias

Para (ISO, 2012), la organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Recopilar evidencias sobre los incidentes que atentan contra la seguridad de la información, permitirá evitar que se materialicen nuevos incidentes de la misma índole a largo plazo, por lo cual permite que la institución conserve su información integra.

En la actualidad las organizaciones que cumplen con este control, logran minimizar los riesgos de seguridad que poseen sus sistemas, por lo cual permiten que sean una organización con sistemas más seguros y robustos.

6.2.2.12 Aspectos de seguridad de la información en la gestión de la continuidad de negocio

Según (ISO, 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 dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativas y/o que estén dispuestos de un modo distinto a la operativa habitual.

Actualmente las instituciones elaboran planes de continuidad que les permitan asegurar la disponibilidad de los procesos críticos ante cualquier incidente relacionado a la seguridad y continuidad de la información.

6.2.2.12.1 Continuidad de la seguridad de la información

De acuerdo a (ISO, 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 debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

Las organizaciones deberían verificar la validez y la efectividad de las medidas de continuidad de la seguridad de la información regularmente, especialmente cuando cambian los sistemas de información, los procesos, los procedimientos y

los controles de seguridad de la información, o los procesos y soluciones establecidas para la gestión de la continuidad de negocio.

6.2.2.12.1.1 Planificación de la continuidad de la seguridad de la información

Para (ISO, 2012), la organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

En todo momento se debe planificar cuales son los requisitos que permitirán mantener la información de manera íntegra ante cualquier situación que ponga en peligro dicha información.

Las empresas deben implementar y planificar la continuidad de la seguridad de la información en cualquier circunstancia, ya que esto permitirá que aunque existan situaciones de riesgo materializadas, la seguridad de la información prevalecerá.

6.2.2.12.1.2 Implantación de la continuidad de la seguridad de la información

Según (ISO, 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 procesos de continuidad que permitan mantener la integridad de la información, es una estrategia muy positiva que permitirá garantizar la continuidad de la empresa o institución.

Para que se puedan mantener un nivel necesario de seguridad, las instituciones y empresas deben de garantizar la implementación de los proceso de seguridad que se deben llevar a cabo durante situaciones que atenten contra la información.

6.2.2.12.2 Redundancias

Para (ISO, 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 comprobar los sistemas de información redundantes, para garantizar la disponibilidad de los dispositivos intermediarios y que estos siempre funcionen adecuadamente.

Toda institución que hace uso de tecnologías de la información, debe garantizar la implementación de dispositivos redundantes que permitan mantener la información disponible en todo momento.

6.2.2.12.2.1 Disponibilidad de instalaciones para el procesamiento de la información

Conforme a (ISO, 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 suma importancia contar con enlaces redundantes que permitan mantener los datos en movimiento, es decir si un enlace cae, deberían existir enlaces alternativos que permitan mantener la continuidad de estos.

Es necesaria la implementación de mecanismos de redundancia en todas las instalaciones que procesan la información, para asegurar la disponibilidad de esta en todo momento.

6.2.2.13 Cumplimiento

Según (ISO, 2012), el diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales. Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Actualmente las organizaciones implementan normativas y políticas con el fin de que sean cumplidas, el objetivo de dicho cumplimiento, es el de evitar que la organización o su empleados caigan en sanciones administrativas de índole civil o penal. Cada organización posee sus normativas de acuerdo al fin de esta.

6.2.2.13.1 Cumplimiento de los requisitos legales y contractuales

De acuerdo a (ISO, 2012), el diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.

Las instituciones deben de velar por que existan requisitos legales y contractuales que regulen los sistemas, esto permitirá que estos se operen de manera correcta.

6.2.2.13.1.1 Identificación de la legislación aplicable

Para (ISO, 2012), se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

Se deben tener pleno conocimiento de las condiciones contractuales de los sistemas empleados por las organizaciones e instituciones, de esta manera se podrá mantener al tanto de cuáles son las normativas aplicables en caso de que se viole algún elemento de los sistemas que estén regidos mediante sus normas.

Es de suma importancia que las instituciones documenten y actualicen las normativas que rigen los sistemas de información.

6.2.2.13.1.2 Derechos de propiedad intelectual (DPI)

Según (ISO, 2012), se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y

contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.

Se debe conocer y estar consiente en todo momento, cuales son las normativas que rigen la propiedad de derechos intelectuales de cada sistema empleado, para evitar caer en violación de dichas normativas.

Las instituciones deben crear e implementar un plan de procedimientos, el cual les permita verificar que no se infringe las normativas de derechos intelectuales.

6.2.2.13.1.3 Protección de los registros de la organización

Conforme a (ISO, 2012), los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

Se deben establecer las políticas y normas que permitan proteger a la información, ante cualquier situación que ponga en riesgo la integridad, disponibilidad y confidencialidad de esta.

Se debe contar en todo momento con mecanismos que permitan a las instituciones salvaguardar la información ante cualquier riesgo.

6.2.2.13.1.4 Protección de datos y privacidad de la información personal

Según (ISO, 2012), se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

Las instituciones deben de garantizar que los datos de los usuarios estarán protegidos e íntegros, mediante los mecanismos establecidos para la seguridad de la información. Además se debe de asegurar que las normativas estén bien definidas y documentadas.

Hoy en día toda organización, debe de dar prioridad a la seguridad de los datos con información personal, aplicando las políticas y mecanismos necesarios que

permitan evitar el control y manipulación no autorizado sobre este tipo de información. Debe de revisar periódicamente la seguridad de la información a efecto de garantizar la adecuada aplicación de las políticas, normativas y procedimientos de seguridad.

6.2.2.13.1.5 Regulación de controles criptográficos

Para (ISO, 2012), se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

Se debe velar por que se estén cumpliendo las normativas con los controles y obtener asesoramiento legal competente.

En la actualidad las organizaciones identifican y documentan los controles necesarios para implementar procedimientos adecuados a garantizar el cumplimiento de los requisitos normativos.

6.2.2.13.2 Revisiones de la seguridad de la información

Según (ISO, 2012), se deberían realizar revisiones regulares de la seguridad de los sistemas de información.

Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.

Actualmente las instituciones y empresas invierten en auditoría TI cualificada que utilice ISO 27001, COBIT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación, para mejorar los

6.2.2.13.2.1 Revisión independiente de la seguridad de la información

Para (ISO, 2012), se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.

En cada momento que se ocurran cambios en la planificación u organización de la institución, se debe realizar una exhaustiva revisión, para verificar que se están cumpliendo con las políticas y protocolos de la seguridad de la información.

Las instituciones deben de planificar la revisión de los mecanismos de seguridad a corto y largo plazo, además en cada momento que existan cambios relevantes en esta.

6.2.2.13.2.2 Cumplimiento de las políticas y normas de seguridad

De acuerdo a (ISO, 2012), los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.

Se debe verificar periódicamente el cumplimiento de las políticas de seguridad de la información, para constatar que estos se estén cumpliendo en tiempo y forma, para que la información esté segura en todo momento.

Es importante que la gerencia de la institución se preocupe por velar por el cumplimiento de normas y procedimientos establecidos para el procesamiento y seguridad de la información.

6.2.2.13.2.3 Comprobación del cumplimiento

Conforme a (ISO, 2012), los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Se deben de realizar revisiones regulares de la seguridad de la información, aplicando las políticas de seguridad apropiadas, para así poder identificar si se está cumpliendo con los controles para proteger la información.

Actualmente las organizaciones, organizan la revisión regular del cumplimiento de los procesos de procedimientos de la información en dependencia de sus áreas, esto respecto a las políticas y normas de requisito de seguridad de la información.

VII. PREGUNTAS DIRECTRICES

a) ¿Cuál es el estado actual de la infraestructura lógica y física de la red LAN de la Alcaldía Municipal de San Ramón, Matagalpa, en el primer semestre 2016?

b) ¿Cuáles son las debilidades y fortalezas de la infraestructura lógica y física de la red LAN de la Alcaldía Municipal de San Ramón, Matagalpa, tomando en cuenta la norma ISO/IEC 27002:2013 en el primer semestre 2016?

c) ¿Cuáles serán las soluciones para mitigar las debilidades encontradas en la infraestructura lógica y física de la red LAN de la Alcaldía Municipal de San Ramón, Matagalpa, tomando en cuenta la norma ISO/IEC 27002:2013 en el primer semestre 2016?

VIII. DISEÑO METODOLÓGICO

- **Enfoque de Investigación**

La presente investigación se basó en el análisis del enfoque conceptual y objetivo de los controles de la norma ISO/IEC 270002:2013.

Se aplicó el razonamiento deductivo, comenzando con la teoría y se analizó la información que se obtuvo mediante los instrumentos, es una investigación objetiva puesto que no afecta el proceso que se estudió, por tal razón el enfoque de investigación es cualitativa con elementos cuantitativos, donde se usaron técnicas de recolección de información (entrevistas y observación).

- **Tipo de investigación según su alcance, diseño y corte**

Según su alcance, esta investigación es descriptiva porque se describió la condición actual de la infraestructura de red lógica y física.

Según el diseño, es no experimental porque no se manipularon variables y se describió de forma real lo que está sucediendo en el caso de estudio.

Según el corte, es transversal porque el estudio ocurrió durante un periodo de tiempo determinado, en el primer semestre 2016.

- **Universo de Estudio**

El área de estudio comprendió a la Alcaldía Municipal de San Ramón, Matagalpa.

El universo de estudio es el área de informática.

Se utilizó una muestra por conveniencia no probabilística, ya que el área de investigación es específica y se tomara directamente, en este caso el área informática.

Según (Explorable.com, 2009), “El muestreo por conveniencia es una técnica de muestreo no probabilístico donde los sujetos son seleccionados dada la conveniente accesibilidad y proximidad de los sujetos para el investigador”.

- **Análisis y Recolección de datos**

Las técnicas que se utilizaron para la recolección de la información son:

a. Entrevistas dirigidas a la directora de informática (Anexos 3, 4, 5, 6)

b. Guía de Observación (Anexo 7)

Para dar cientificidad a la investigación, se utilizó el método teórico para la redacción del marco teórico y el análisis y discusión de resultados. Se utilizaron herramientas empíricas y tecnológicas para la recolección de la información, como: entrevistas, guía de observación, lápices, libreta de apuntes, tablet y smartphone.

La información se analizó a través de los métodos deductivo e inductivo, la información se analizó, comparó y trianguló.

La información recolectada se procesó a través de la paquetería ofimática y herramientas informáticas: Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010 y Cisco Packet Tracert.

Los materiales que se utilizaron para el desarrollo, análisis y elaboración del informe final son: computadoras, impresora, fotocopiadora, encuadernado y papel bond.

- **Variables de estudio** (Ver Anexo 2)
  - Infraestructura de red LAN
  - ISO/IEC 27002:2013

IX. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

La finalidad de esta investigación es evaluar la infraestructura de red LAN de la alcaldía municipal de San Ramón, Matagalpa, bajo la guía de buenas prácticas de la seguridad de la información ISO/IEC 27002:2013 en el primer semestre 2016. Para cumplir dicho propósito se plasmaron objetivos específicos, los cuales se orientan a describir la condición actual física y lógica de la infraestructura de red LAN de la institución y de esta manera identificar las debilidades y fortalezas de esta.

La información sustancial obtenida se recolectó mediante entrevistas dirigidas a la directora de informática de la alcaldía (Ver Anexo 3, 4, 5, 6), también se aplicó un formato de observación (Ver Anexo 7).

Para procesar la información se realizó la matriz de datos para las entrevistas que se realizaron (Ver Anexo 8, 9) y se complementó mediante la guía de observación aplicada.

Descripción de ámbito

La Alcaldía Municipal de San Ramón, Matagalpa es una institución estatal, que brinda a la población diversos servicios con el objetivo de contribuir a mejorar la calidad de vida de los ciudadanos.

Esta institución actualmente cuenta con una infraestructura de red deficiente, debido a que los recursos implementados en la red no están distribuidos de la manera adecuada para un óptimo funcionamiento, además el personal a cargo no está debidamente capacitado para operar y dar el mantenimiento necesario.

Condición actual de la red LAN de la alcaldía municipal de San Ramón, Matagalpa, primer semestre 2016

La infraestructura actual de la red LAN de la alcaldía municipal de San Ramón, Matagalpa, está compuesta por 61 computadoras personales, 3 servidores, 14 impresoras, 17 teléfonos analógicos, 56 baterías de respaldo, 4 enrutadores, 7 conmutadores, 1 panel de conexiones y con un ancho de banda de 15 Megabytes.

La red LAN es utilizada por el personal, mediante el uso de los equipos conectados a través del cableado distribuido entre las 22 áreas, con el fin de utilizar los servicios que se ofrecen en la red tales como: sistemas en red, base de datos, impresiones, videoconferencias y acceso a internet.

La red cuenta con un servidor que ofrece únicamente el servicio de proxy SQUID, también existe un servidor de sistema contable llamado Sistema Integrado de Administración Financiera Municipal (SIAFM), el cual lleva a cabo todos los procesos de los módulos contables y un servidor dedicado para la sala de videoconferencias.

Imagen 1. Servidores de las redes de la alcaldía



Fuente: Propia a partir de la observación realizada

Mediante la red se transportan datos de información confidencial que se comparten mediante las múltiples computadoras conectadas a la red y que forman parte de los activos más importantes para la institución, como lo es, los datos de los módulos contables del Sistema Integrado de Administración Financiera Municipal (SIAFM).

Arquitectura de red

En la institución existen dos redes LAN con conexión a internet independientes, pero no son tolerante a fallos, debido a que solo existe un proveedor de servicio de internet por cada red, además no hay enlaces redundantes y servidores de respaldo por lo que si algunos de estos falla, la redes colapsan de manera inmediata.

La arquitectura de red de la sala de video conferencias se ha implementado de manera eficiente puesto que ofrece sus servicios de manera óptima, además es independiente a la red principal, cabe señalar que esta última es ineficiente, aunque soporta de manera estable los servicios que se ofrecen, esta se encuentra estructurada de manera incorrecta.

Según la directora de informática la red principal es escalable, pero se ha observado que la arquitectura actual crece de manera desorganizada por lo que la demanda de más usuarios conllevaría un impacto negativo en el rendimiento de esta, lo que provocaría que los servicios se ejecuten de manera ineficiente, mientras que la red de la sala de video conferencias se encuentra organizada y estructurada correctamente.

Se desconoce si en las redes está implementada la calidad de servicios (QoS), debido a que la directora de informática no maneja esta información y no posee las credenciales necesarias para acceder a la configuración de los servidores de ambas redes.

La seguridad de la red principal de la institución no refleja que existan procedimientos y herramientas óptimas que permitan mitigar fallas de seguridad en la arquitectura de red implementada, en cambio la red de la sala de video conferencias refleja una estructura más robusta.

Tipos de Red

La institución cuenta con dos redes LAN independientes (red de la sala de video conferencias y la red principal) que interconectan en dependencia de la red en la que se encuentran las estaciones de trabajo ubicadas en las diferentes áreas. No existe una red MAN debido a que no hay nodos conectados fuera de la localidad donde se encuentra la institución, además se hace uso de la red WAN (internet) solo para acceso a servicios web.

Topología de Red

La directora de informática desconoce el tipo de topología lógica y física implementada en las dos redes LAN, tampoco posee documentación de las topologías físicas actualmente implementadas, sin embargo mediante la observación se pudo identificar que estas se asemejan a la topología de árbol (Ver Anexo 11, 12, 13, 14).

Calidad de las comunicaciones

La estructura de red principal de la institución presenta un cierto grado de complejidad que impacta en la calidad de las comunicaciones, debido a que dicha estructura de red se encuentra desorganizada y sin documentación, por lo tanto existen factores externos que afectan la calidad, por ejemplo: las veces que el mensaje debe de cambiar de forma, las veces que este es redirigido y la cantidad de mensajes que se trasmiten de manera simultánea.

Imagen 2. Estructura de la red principal desorganizada

Fuente: Propia a partir de la observación realizada

En cambio la red de la sala de video conferencias está organizada, pero la directora de informática desconoce si esta se encuentra documentada y mediante la observación se determinó que no existe documentación.

Imagen 3. Estructura de red sala video conferencias

Fuente: Propia a partir de la observación realizada

En la red principal no existen factores internos relevantes que afecten la calidad de las comunicaciones, puesto que no se mueven grandes volúmenes de información, esto debido a las restricciones de red que únicamente permite las conexiones a sistemas en red, bases de datos y consultas a páginas web específicas. Sin embargo según la directora de informática algunos usuarios, logran saltar dichas restricciones utilizando programas VPN, afectando la calidad de las comunicaciones, en cambio en la red de la sala de videoconferencias se cuenta con ancho de banda dedicado y dispositivos capaces de soportar la transmisión de video y voz eficientemente, por lo tanto la calidad de las comunicaciones no se ve afectada.

Infraestructura Física

Dispositivos de red

La tabla 1 muestra los componentes de la infraestructura de red principal la cual cuenta con enrutadores, conmutadores, panel de conexión, central telefónica y servidores.

Tabla1. Dispositivos de la red principal

Dispositivo	Cantidad	Observación
Módem	1	Claro A7600A1 (Propiedad del ISP)
Enrutador	1	D-Link
	1	Thompson ST585
Conmutador	4	Encore de 8 puertos
	1	Nexxt de 8 puertos
	1	Nexxt de 24 puertos
Central Telefónica	1	Panasonic Tem824
Servidores	1	Hp Proliant
	1	Clon
Computadoras	31	Clon
	5	Dell
	2	HP
	1	Lenovo
	1	Gateway
	1	Compaq
Panel de Conexiones	1	Nexxt 24 puertos

Fuente. Elaboración propia a partir de la observación aplicada.

La tabla 2 refleja los componentes de red implementados en la sala de video conferencias.

Tabla 2. Dispositivos de la red de la sala de video conferencias

Dispositivo	Cantidad	Observación
Módem Inalámbrico	1	Mikrotik (Propiedad del ISP)
Conmutador	1	Tp-link 8 puertos
Servidor	1	Lenovo
Computadoras	20	Dell Optiplex 3020

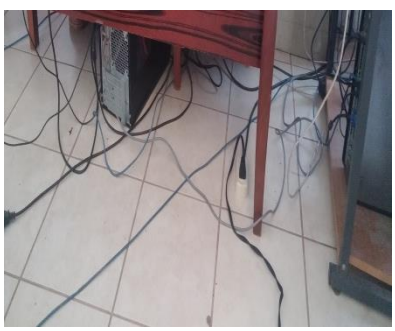
Fuente. Elaboración propia a partir de la observación aplicada.

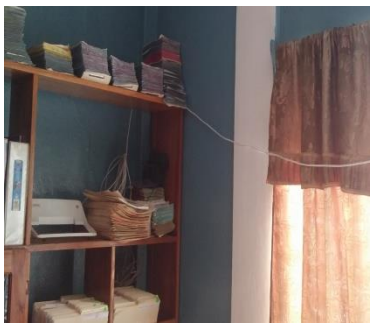
De igual manera se observó que en ambas redes no existen dispositivos firewall físico.

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. Cabe señalar que el cableado se encuentra desorganizado y no está debidamente protegido, mientras que en la sala de videoconferencia solo existe el cableo para la conexión del módem al enlace del ISP. No existe cableado coaxial ni fibra óptica.

Imagen 4. Cableado de red principal desorganizado





Fuente: Propia a partir de observación realizada

Medios de transmisión inalámbricos

Se utilizan el medio de conexión inalámbrica en la sala de conferencias, para conectar las terminales a la red. La tecnología implementada es IEEE 802.11b/g/n.

Estación de trabajo

Se preguntó a la directora de informática por la cantidad de computadoras por área, la tabla 3 refleja esta información.

Tabla 3. Cantidad de computadoras por área

Área	Cantidad de computadoras	Área	Cantidad de computadoras
Contabilidad	7	Registro	1
Informática	1	Escuela de Oficio	2
Administración	1	Divulgación	3
Adquisición	2	Catastro	3
Proyecto	6	UMAS	1
Turismo	1	Medio ambiente / Poder ciudadano	1
Auditor Interno	1	Promotoría social	1
Gerencia	1	Secretaria de alcalde	1
Asistente del Alcalde	1	Recepción	1
Tributario	4	Sala de Videoconferencia	20
Servicios Municipales	1	Recursos Humanos	1
Total		61	

Fuente. Elaboración propia a partir de la entrevista aplicada.

Políticas de seguridad físicas

No existen políticas de seguridad físicas implementadas en la infraestructura de ambas redes, esto conlleva una gran amenaza a la seguridad de los dispositivos, en consecuencia esta no se encuentra respaldada mediante un plan de contingencia que permita la recuperación inmediata ante un desastre.

No se cuenta con procedimiento de seguridad que permitan prevenir la manipulación y acceso no autorizado a la información, cabe señalar que el personal no está en constante capacitación sobre las reglas y procedimientos establecidos sobre la seguridad de la red.

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

Imagen 5. Dispositivos desprotegidos, fuera de la oficina de informática

Fuente: Propia a partir de observación aplicada

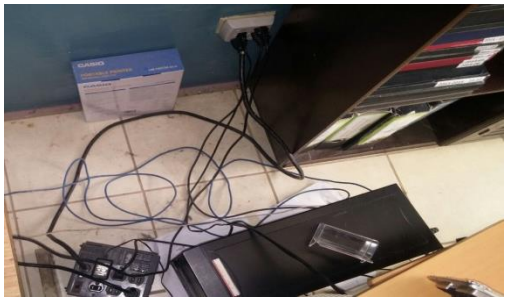
Sólo se encuentran climatizados los dispositivos que están dentro de la oficina de informática y en la sala de video conferencias.

Imagen 6. Climatización en oficina de informática y sala de video conferencias

Fuente: Propia a partir de observación aplicada

Los dispositivos se encuentran conectados a baterías de respaldo, que ayudan a estabilizar la energía para evitar daños por cambios de voltaje y apagones.

Imagen 7. Baterías de respaldo



Fuente: Propia a partir de observación aplicada

No existen antecedentes documentados de riesgos y amenazas hacia la seguridad de la infraestructura física.

Infraestructura Lógica

Servidores

En la red principal existe un servidor de red configurado con Debian 5, el cual ofrece el servicio de proxy SQUID. También se cuenta con un servidor basado en Windows Server 2007 que ejecuta el Sistema Integrado de Administración Financiera Municipal (SIAFM) de la institución.

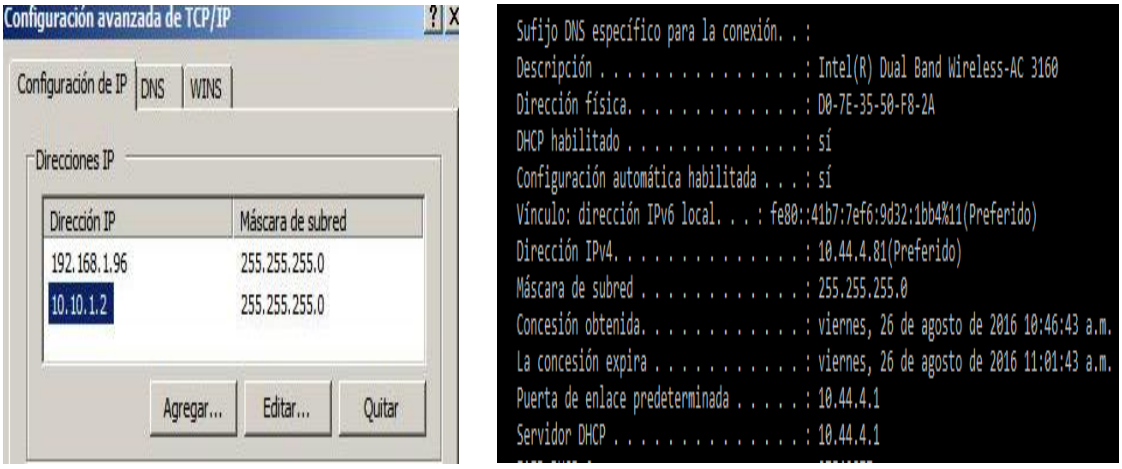
En la sala de video conferencias una computadora principal con sistema operativo Windows 8 ejerce el papel de servidor, donde está instalado el programa SKYPE para videoconferencias.

Direccionamiento IP

El rango de IP privado implementado en la red principal es 10.10.1.0/24, las direcciones IP son asignadas de manera manual a cada computadora cabe señalar que el servidor del Sistema Integrado de Administración Financiera Municipal (SIAFM) utiliza el direccionamiento 192.168.1.0/24 con el fin de comunicarse solo con las computadoras que hacen uso del sistema.

En la sala de video conferencias el rango implementado es 10.44.4.0/24 y las IP se reciben de manera dinámica.

Imagen 8. Direccionamiento red principal y sala de video conferencias



Fuente: Propia a partir de la observación realizada

Ambas redes cuentan con direcciones IP públicas dinámicas para salir a internet.

Servicios de Red

Las redes de la institución ofrecen los siguientes servicios.

- ✓ Proxy
- ✓ Bases de datos
- ✓ Chat interno
- ✓ Impresiones en red
- ✓ Videoconferencias

Segmentación de red

La institución no implementa en sus redes tecnologías de LAN virtuales (VLANs), por lo tanto no existe segmentación de red.

Ancho de banda

La red principal cuenta con un ancho de banda de 10 Mb brindado por el proveedor CLARO, mientras que la red de la sala de conferencias posee 5 Mb asignados por ENATREL.

Imagen 9. Prueba de Ancho de banda Red Principal y Sala Video conferencia

Fuente: Propia a partir de observación aplicada

Cabe destacar que el ancho de banda suministrado a la red principal cubre las necesidades de esta, para brindar un óptimo servicio.

Firewall

Sólo se utilizan firewall lógicos que traen por defecto los sistemas operativos de las computadoras y los servidores.

VPN

No se hace uso de este tipo de tecnología en ambas redes.

Central Telefónica

Existe una central telefónica análoga que brinda la cantidad suficiente de extensiones telefónicas para el uso de los usuarios de la institución, cabe destacar que esta no es administrada debido a que no existe documentación técnica de la misma y la encargada de informática no posee los conocimientos técnicos para administrarla.

Imagen 10. Central Telefónica

Fuente: Propia a partir de observación aplicada a la red principal.

Políticas de seguridad Lógicas

En la institución no se encuentran establecidas ni documentadas las políticas de seguridad lógicas.

Amenazas lógicas

Para mitigar las amenazas en la red se implementa como mecanismo de seguridad el antivirus KASPERSKY (KASPERSKY Lab, 2016) con licencia de 1 año para 20 en video conferencia y 10 para red principal, las de más maquinas utilizan AVAST Internet Security sin licencia original y se actualiza de manera manual.

ISO/IEC 270002-2013

Concepto

La ISO/IEC 27002:2013 es una guía de buenas prácticas enfocada a la seguridad de la información.

Según NimboSystems (2013), ISO 27002:2013 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.

Se le preguntó a la directora de informática si tenía conocimiento acerca de normativas que regulan la seguridad de la información a lo que ella respondió no tener conocimiento. También se enfatizó la importancia de implementar normativas internacionales, a lo cual ella argumentó que es muy importante porque de esta manera se evitaría la pérdida de información.

De la misma manera se cuestionó acerca del conocimiento de la Norma ISO/IEC 27002:2013, a lo cual respondió que no.

Es importante que la directora de informática conozca acerca de normativas que ayudan a regir la seguridad de la información, dado que esta es el principal y más importante activo de la institución. Esto ayudará a poder aplicar eficazmente controles de seguridad para el manejo y gestión adecuada de los recursos disponibles.

Políticas de Seguridad

Conjunto de políticas

Para (ISO, 2012), se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.

Se preguntó a la entrevistada, si se encuentran definidas las políticas de seguridad en la red de la institución, a lo cual ella respondió que no están definidas.

La institución no ha establecido los requisitos de seguridad para desarrollar normativas y reglas que administren la protección de la información, por lo tanto al no aplicar estos parámetro de seguridad, es evidente que no se cumple con el objetivo planteado por ISO/IEC 27002:2013.

Aspectos organizativos de la seguridad de la información

Segregación de tareas

Para (ISO, 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.

Se cuestionó a la directora de informática acerca de que, si se encuentran definidas sus tareas respecto a la seguridad de la red, ella mencionó que no se encuentran definidas, también se preguntó que si encuentra definida el área de ti a lo que respondió que no se encuentra definida, esta información se complementó mediante la observación ya que en el organigrama de la institución no se encuentra definida un área de TI (Ver Anexo 10).

Debido a que no se encuentran definidas y documentadas las tareas de seguridad que debe de ejercer la directora de informática y no existe un área de TI, no se cumple el objetivo propuesto por ISO/IEC 27002:2013.

Seguridad ligada al recurso humano

Antes de la contratación

Para (ISO, 2012), las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo. Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles.

Se preguntó a la entrevistada, si antes de su contratación se le dieron a conocer cuáles eran los términos y condiciones para el puesto de trabajo, a lo cual contestó que sí.

La directora de informática conoció formalmente los términos y condiciones del empleo antes de su contratación, por lo cual este objetivo de control que propone ISO 27002:2013 se cumple por parte de la institución.

Investigación de antecedentes

Según (ISO, 2012), se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Se preguntó a la entrevistada, si la institución indagó acerca de sus antecedentes en otros empleos, a lo cual hizo mención que solo se le pidieron cartas de recomendación.

La institución no aplica técnicas de revisión de antecedentes con el fin de conocer a los aspirantes al puesto, solo pidió cartas de recomendación personal, por lo consiguiente al realizar este proceso de verificación, cumple parcialmente con el objetivo propuesto por ISO 27002:2013.

Términos y condiciones de contratación

Según (ISO, 2012), como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

Se preguntó a la entrevistada sobre, cuáles son los términos y condiciones de su trabajo, a lo cual respondió que no están definidos.

La institución no ha definido y documentado los términos y condiciones de contratación por lo tanto el objetivo de control de ISO 27002:2013 no se cumple.

Durante la contratación

Para (ISO, 2012), se debería definir las responsabilidades de la dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.

Se preguntó a la entrevistada si la gerencia se encarga de velar por el cumplimiento de la seguridad en las redes, a lo que respondió que únicamente se preocupan cuando ocurre una falla y pregunta que ha pasado con la red y porque ha sucedido.

No están definidas las responsabilidades para garantizar la seguridad en los puestos de trabajo y la gerencia no está atenta a la seguridad de la red en todo momento, solo si ocurre un incidente, además no posee un plan para velar por cumplimiento de la seguridad de la información en todas las áreas, en especial en informática, por lo tanto según lo planteado por el objetivo de control de ISO 27002:2013, este no se cumple.

Concienciación, educación y capacitación en seguridad de la información

Según (ISO, 2012), todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Se cuestionó a la encargada de informática si la institución le brinda capacitaciones relevantes en su área y si le da a conocer los cambios en las políticas y procedimientos organizacionales, a lo que respondió que únicamente recibe capacitaciones por parte del Instituto Nicaragüense de Fomento Municipal (INIFOM) y que la institución si le da a conocer los cambios de las políticas y procedimientos organizacionales relevantes.

La institución se encarga de dar a conocer a la directora de informática cada cambio que se realizan en las políticas y procedimientos organizacionales, además le brinda capacitaciones para el manejo y administración del sistema financiero, pero no brinda capacitaciones relevantes a las tecnologías de la información, por lo tanto se cumple parcialmente con el objetivo propuesto por ISO/IEC 27002:2013.

Gestión de activos

Responsabilidades sobre los activos

Para (ISO, 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.

Se preguntó a la entrevistada que cuales son sus responsabilidades en el mantenimiento adecuado de los activos asignados a informática, a lo que respondió que su responsabilidad es cumplir con los controles que la dirección le indique.

La institución define a la responsable de informática cuáles son sus responsabilidades y los controles del mantenimiento de los activos que debe

aplicar, pero no existe un documento formal en donde estén reflejadas, por lo tanto el control que propone ISO/IEC 27002:2013 se cumple parcialmente.

Inventario de activos

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

Se preguntó a la directora de informática, si lleva a cabo el inventario de los equipos informáticos y cada cuanto tiempo se realiza, a lo cual respondió que se lleva a cabo de manera anual.

El inventario se realiza de manera muy general y no se describe de manera detallada los datos de los equipos informáticos, de manera que la información obtenida es superficial, es evidente que el control propuesto por ISO/IEC 27002:2013 se cumple parcialmente.

Uso aceptable de los activos

Para (ISO, 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.

Se cuestionó a la directora de informática sobre cuáles eran los procedimientos empleados para el uso adecuado de los activos del área de redes, a lo cual respondió de que no existen procedimientos.

La institución no documenta ni implementa las regulaciones necesarias para regir el uso adecuado de la información y los activos, por ende no cumple el objetivo de control propuesto por ISO/IEC 27002:2013.

Manejo de los soportes de almacenamiento

Para (ISO, 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.

Se consultó a la directora de informática, sobre los controles y procedimientos que se aplican para proteger los medios de almacenamiento, a lo que contestó que no existen.

La institución no aplica regulaciones de seguridad que permitan proteger los dispositivos de almacenamiento, por lo que incumple con el objetivo de control de ISO/IEC 27002:2013.

Control de accesos

Requisitos de negocio para el control de accesos

Para (ISO, 2012), se deberían controlar los accesos a 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.

Se cuestionó a la directora de informática si se controla el acceso a la información y de qué manera, a lo que respondió que no se controla.

La institución no implementa controles de acceso a los recursos de información, por esta razón no cumple con el objetivo de control contenido en ISO/IEC 27002:2013.

Política de control de acceso

Para (ISO, 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.

Se preguntó a la entrevistada si están establecidas y documentadas las políticas de control de acceso, a lo que contesto no existen políticas ni documentación de estas.

La institución no ha definido ni documentado las políticas de control de acceso que permitan establecer niveles de seguridad en la información, por lo cual no cumple el objetivo de control de ISO/IEC 27002:2013.

Control de acceso a las redes y servicios asociados

Según (ISO, 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.

Se cuestionó a la directora de informática que si existen controles de acceso de usuarios, para permitir que estos solo utilicen los servicios de red a los que ha sido autorizados, a lo que respondió que se implementa este control el área de contabilidad a través del servidor de red y el servidor de sistemas.

La institución cumple de manera parcial con este objetivo propuesto por ISO/IEC 27002:2013, puesto que solo aplica este control en el área de contabilidad.

Gestión de acceso de usuarios

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

Se cuestionó a la directora de informática, sobre la existencia de procedimientos formales que le permitan determinar los parámetros necesarios para asignar los permisos de acceso a la red, a lo respondió que no tiene definidos estos parámetros dado que estos los regula el Instituto Nicaragüense de fomento Municipal (INIFOM).

La directora 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.

Gestión de altas/bajas en el registro de usuarios

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

Se interrogó a la entrevistada que si aplica procedimientos formales al momento de dar de alta o baja a un usuario de la red, a lo cual menciono que no realiza procedimientos.

En la institución no se aplican procedimientos formales para realizar altas y bajas de usuarios en el acceso a los sistema y red, por consiguiente el objetivo de ISO/IEC 27002:2013 no se cumple.

Gestión de los derechos de acceso con privilegios especiales

Para (ISO, 2012), la asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

Se preguntó a la directora de informática, por el control de usuarios con privilegios especiales en la red, a lo que respondió de que si se controlan y que el privilegio es tener total acceso a la red sin ninguna restricción.

La directora de informática controla la asignación de los privilegios especiales que poseen algunos usuarios, por lo cual es evidente que se cumple con el objetivo de control que plantea ISO/IEC 27002:2013.

Control de acceso a sistemas y aplicaciones

Según (ISO, 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.

Se preguntó a la entrevistada sobre que procedimientos de seguridad están implementados para evitar que los usuarios manipulen los sistemas, datos y dispositivos restringidos, a lo cual hizo mención que cambia la contraseña del servidor cada dos meses, controla la entrada a la oficina de informática e implementa el uso de proxy en las computadoras, también menciono que a los dispositivos que se encuentran fuera de la oficina de informática no se le aplican procedimientos de seguridad.

La institución no aplica procedimientos de seguridad a todos recursos que conforman la red, ya que existen dispositivos que están fuera de áreas seguras y no poseen ningún tipo de seguridad implementado, por lo cual el objetivo de control de ISO/IEC 27002:2013 se cumple parcialmente.

Restricciones de acceso a la información

Para (ISO, 2012), se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

Se cuestionó a la entrevistada sobre qué mecanismos de seguridad implementa para restringir el acceso a la información por parte de usuarios no autorizados, a lo cual respondió que no todos los sistemas están en red y que estos están restringidos mediante el acceso por contraseñas que solo ella conoce.

La directora de informática implementa ciertos mecanismo para restringir el acceso no autorizado al sistema en red, pero estas no están relacionadas a políticas de control de acceso ya que no se encuentran definidas, por lo tanto el objetivo de control de ISO/IEC 27002:2013 se cumple de manera parcial.

Gestión de contraseñas de usuarios

Según (ISO, 2012), los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

Se cuestionó a la directora de informática, de qué manera se gestionan las contraseñas de usuarios, a lo que respondió que no existen parámetros definidos y no se gestionan las contraseñas de los usuarios.

En la institución no existe la gestión de las contraseñas, esto quiere decir que no se aplican estándares de seguridad de las credenciales de los usuarios, por lo cual no se cumple el objetivo de control de ISO/IEC 27002:2013.

Cifrado

Controles criptográficos

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

Se cuestionó a la directora de informática si se aplican mecanismos de encriptamiento a la información, a lo que respondió que no.

La institución no implementa métodos de seguridad que respalde la confiabilidad e integridad de la información, por ende no cumple con el objetivo de control propuesto por ISO/IEC 270022:2013.

Políticas de uso de controles criptográficos

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

Se preguntó a la entrevistada que si existen políticas de seguridad que regulen los controles criptográficos a lo que respondió que no.

La institución al no aplicar mecanismo de cifrado a la información, no tiene definida las políticas del uso de este control de seguridad, por lo tanto no cumple el objetivo de control de ISO/IEC 27002:2013.

Gestión de claves

Para (ISO, 2012), se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

Se cuestionó a la entrevistada sobre la gestión de las claves de encriptamiento a lo que respondió que no se gestionan.

En la institución no existen mecanismo ni políticas de encriptamiento por lo tanto tampoco se gestionan claves de cifrado y descifrado, esto indica que no se cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Seguridad física y ambiental

Áreas seguras

Para (López, 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. Los medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Se preguntó a la directora de informática si los dispositivos de las redes se encuentran en áreas debidamente protegidas ante la manipulación y acceso no autorizado, a lo que respondió que solamente algunos dispositivos, 50% están en área protegida y 50% en área no protegida.

En la institución los dispositivos de red que se encuentran en áreas con cierto grado de seguridad son los que se encuentran en la sala de video conferencia y en la oficina de informática, por lo tanto el objetivo de control de ISO 27002:2013 se cumple de manera parcial.

Controles físicos de entrada

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

Se cuestionó a la directora de informática si existen medidas de control físico en las áreas donde se encuentran los dispositivos de red, a lo que respondió que solo en la oficina de informática y sala de video conferencia se aplica este control, mediante el uso de puerta bajo llave.

En la institución no se aplican controles de acceso físico en todas las áreas, por lo que los dispositivos de red que están fuera de la área de informática y sala de video conferencias se encuentran es riesgos ya que donde están ubicados cualquier persona tiene acceso a ellos, por esta razón el objetivo de control de ISO/IEC 27002:2013 se cumple parcialmente.

Seguridad de oficinas, despachos y recursos

Según (ISO, 2012), se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.

Se le preguntó a la directora de informática que medida de seguridad de acceso físico implementa en la oficina de informática y sala de video conferencias, a lo cual menciono que únicamente hace uso de la puerta con llave y que solo ella tiene acceso a esta.

La institución no ha diseñado y aplicado un sistema de seguridad física que permita mantener los dispositivos de red íntegros, ya que solo implementa un mecanismo de seguridad como puerta con llave en dos áreas relevantes como lo son la sala de video conferencia y oficina de informática, cabe señalar que se hace uso de otros mecanismo de seguridad física como lo son cámaras de seguridad, detectores de movimiento, entre otros, por lo tanto este objetivo de control de ISO/IEC 27002:2013 se cumple parcialmente.

Protección contra amenazas externas y ambientales

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

Se le preguntó a la directora de informática si los dispositivos de red se encuentran en un lugar capaz de protegerlos antes desastres naturales e incidentes malintencionados, a lo que contesto que contra desastre naturales no es seguro que están protegidos los dispositivos y solamente están protegidos la mitad de los dispositivos contra ataques malintencionados.

La institución no cuenta con una infraestructura física que sea capaz de soportar de manera adecuada desastres naturales, además pese a que algunas áreas estén protegidas para evitar ataque maliciosos, esto no asegura la protección de todos los dispositivos de red, por lo tanto se cumple parcialmente el control de ISO/IEC 27002:2013.

Seguridad de los equipos

Según (ISO, 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.

Se preguntó a la entrevistada que si los dispositivos de red se encuentran debidamente climatizados y conectados a fuentes de energía de respaldo, además si estos se encuentran ubicados en un rack, a lo que respondió que solo los equipos que se encuentran en la oficina de informática y sala de video conferencias se encuentran climatizados, además que todos los dispositivos están conectado a fuentes de energía de respaldo y no están ubicados en rack.

La entidad cumple de manera parcial el objetivo propuesto por ISO/IEC 27002:2013 ya que no cuenta con una infraestructura física organizada que proteja de manera adecuada los dispositivos de red.

Seguridad del cableado

Para (ISO, 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 le preguntó a la directora de informática que si el cableado se encuentra canaleteado y debidamente protegido para evitar la manipulación no autorizada de estos, a lo que respondió que no están canaleteados y estos pueden ser manipulados fácilmente.

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.

Mantenimiento de los equipos

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

Se le preguntó a la entrevistada acerca del tipo de mantenimiento que se le da a los dispositivos de red y cada cuanto tiempo se realiza, a lo que respondió que se realiza mantenimiento preventivo y correctivo cada 3 a 5 meses.

La institución cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Seguridad de equipos y activos fuera de las instalaciones

Para (ISO, 2012), se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

Se le preguntó a la directora de informática que si existen dispositivos de red fuera de las instalaciones de la institución, a lo que respondió que si existen pero no se aplican mecanismos de seguridad.

La institución cuenta con dispositivos de red a su cargo que están fuera de sus instalaciones, estos se encuentran en la escuela de oficio y biblioteca, pero no se le aplican los mecanismos necesarios de seguridad a los equipos, por lo que no se cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Seguridad Operativa

Documentación de procedimientos de operación

Según (ISO, 2012), se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

Se le pregunto a la directora de informática si existe documentación de los procedimientos de operación para los recursos de red, a lo que respondió que no.

La institución no documenta los procedimientos necesarios para operar los dispositivos de red, por lo cual no cumple con el objetivo propuesto por ISO/IEC 27002:2013.

Gestión de cambios

Para (ISO, 2012), se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.

Se cuestionó a la entrevistada si controla los cambios que afectan a la infraestructura de red, a lo que ella respondió que no.

No se cumple con el objetivo planteado por ISO/IEC 27002:2013, debido a que no se gestionan los cambio que afecten a la seguridad de la información en la red.

Gestión de capacidades

Según (ISO, 2012), se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

Se le preguntó a la directora de informática si lo recursos actualmente implementados ofrecen las condiciones necesarias para operar de manera óptima en un futuro, a lo que respondió que sí.

Los recursos de red actuales, aunque no estén estructurados de manera adecuada, brindan las condiciones necesarias para operar de manera estable, según la directora de informática estas condiciones son suficientes para que en el futuro la red siga operando de manera óptima, mediante la observación se pudo constatar esta afirmación, la red aunque esta desorganizada, si brinda, las capacidades para operar en el futuro, por lo tanto se cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Protección contra código malicioso

Para (ISO, 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.

Se cuestionó a la entrevistada si actualiza el antivirus en todas las computadoras que hacen uso de la red, a lo que respondió que, las maquinas que poseen la licencia del antivirus Kaspersky se actualizan automáticamente cada día y las demás que utilizan el antivirus Avast sin licencia, ella se encarga de actualizarlos manualmente cada 20 días.

La institución brinda la protección adecuada en algunas computadoras, puesto que tiene un número limitado de equipos con licencias genuinas, por lo que las demás computadoras suponen un riesgo a la protección de la información, debido a que

no cuentan con antivirus que posea licencias originales que respalden la actualización correcta de la base de datos del antivirus, por lo tanto se cumple parcialmente con el objetivo de control de ISO/IEC 27002:2013.

Controles contra código malicioso

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

Se preguntó a la entrevistada si existen controles de seguridad que permitan la detección y mitigación del malware, a lo que ella respondió que solo implementa como control de seguridad 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.

Copias de Seguridad

Copias de seguridad de la información

Para (ISO, 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.

Se interrogó a la directora de informática si realiza copias de seguridad de los servidores, si se almacenan en un lugar seguro y cada cuento tiempo se realiza esta acción, a lo que respondió que solo realiza copias de seguridad del sistema contable todos los días y que en el servidor del proxy no puede realizar copias de seguridad porque no tiene acceso, también menciono que las copias de seguridad se almacenan en un lugar seguro.

El objetivo de control propuesto por ISO/IEC 27002:2013 se cumple parcialmente debido a que no se realizan copias de seguridad en uno de los servidores.

Registro de actividad y supervisión

Según (ISO, 2012), los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.

Se cuestionó a la directora de informática si monitorea continuamente los sistemas y de qué manera lo realiza, a lo que respondió que no realiza monitoreo continuo, solo únicamente cuando los sistemas presentan alguna falla.

La institución no monitorea en todo momento los sistemas, por lo que no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Registro y gestión de eventos de actividad

Para (ISO, 2012), se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.

Se le preguntó a la directora de informática si monitorea y controla el uso de información en cada uno de los usuarios que manipulan los datos, a lo que ella respondió que no monitorea la actividad de los usuarios.

La institución no implementa mecanismo de monitoreo para el uso de la información por parte de los usuarios, por consiguiente no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Consideraciones de las auditorías de los sistemas de información

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

Se cuestionó a la directora 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.

Controles de auditoria de los sistemas de información

Según (ISO, 2012), 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.

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

Seguridad en las telecomunicaciones

Gestión de la seguridad en las redes

Controles de Red

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

Se cuestionó a la directora de informática que si hace uso de herramientas de monitoreo de red que le permitan observar intrusiones no autorizada en la red, a lo que respondió que no.

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.

Mecanismos de seguridad asociados a servicios de red

De acuerdo a (ISO, 2012), se deberían identificar e incluir en los acuerdos de nivel 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 preguntó a la directora de informática acerca de qué mecanismos de seguridad emplea para proteger los servicios de red, a lo que respondió que solo utiliza el proxy.

La institución no identifica los niveles de servicio y requisitos de información de todos los servicios de red que se ofrecen, además únicamente emplea como mecanismo de seguridad para la protección el proxy, por consiguiente cumple parcialmente con el objetivo de control propuesto por ISO/IEC 27002:2013.

Segregación de redes

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

Se cuestionó a la entrevistada que si existen redes virtuales locales, a lo que respondió que no.

La institución no implementa VLAN, por lo que supone un riesgo a la información sensible que se mueven en ciertas áreas de la institución, ya que todas las máquinas están conectadas en la misma red, por consiguiente no se cumple el objetivo de control de ISO/IEC 27002:2013.

Intercambio de información con partes externas

Según (ISO, 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 le pregunto a la directora de informática si existe intercambio de información con entidades externas mediante la red, a lo que 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.

Políticas y procedimientos de intercambio de información

Conforme a (ISO, 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.

Se preguntó a la directora de informática si existen políticas y procedimientos de intercambio, a lo que respondió que no.

Puesto que no se realiza intercambio de información con entidades externas, no existen políticas y procedimientos de intercambio empleados por la institución, por esta razón no se cumple el objetivo de control de ISO/IEC 27002:2013.

Acuerdos de intercambio

De acuerdo a (ISO, 2012), los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

Se cuestionó a la directora de informática acerca de que si se establecen los acuerdos de intercambio a lo que respondió que no.

La institución no establece acuerdos de intercambio, por lo tanto no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Mensajería electrónica

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

Se cuestionó a la entrevistada sobre qué mecanismos de seguridad emplea para el uso de correo electrónico, a lo que respondió que no existe ningún mecanismo empleado.

La institución no implementa mecanismo de seguridad que ayude a evitar amenazas que puedan ocurrir mediante el uso de correo electrónico, por lo tanto no se cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Acuerdos de confidencialidad y secreto

Para (ISO, 2012), se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

Se preguntó a la directora de informática si se documentan y actualizan los acuerdos de confidencialidad, con el fin de evitar fugas de información a lo que respondió que no existen acuerdos de confidencialidad.

La institución no ha definido ni documentado acuerdos de confidencialidad que permitan mantener la información segura por parte de los usuarios, por lo que supone un alto riesgo al sigilo de la información más sensible, por lo anterior descrito no se cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Relaciones con suministradores

Gestión de la prestación del servicio por suministradores

Según (ISO, 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 prestan cumplen con todos los requerimientos acordados con los terceros.

Se cuestionó a la directora de informática si se verifica el cumplimiento de los acuerdos de servicio por parte de los proveedores de servicio de internet (ISP) de la red, a lo que respondió que realiza pruebas de velocidad del ancho de banda para verificar que se está recibiendo la cantidad acordada en el contrato.

La institución no cumple con el objetivo de control de ISO/IEC 27002:2013, puesto que no estipula e implementa acuerdos que permitan gestionar y monitorear el cumplimiento de los acuerdos con terceros.

Supervisión y revisión de los servicios prestados por terceros

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

Se preguntó a la directora de informática que si se monitorea el cumplimiento de los servicios prestados por el proveedor de internet, a lo que respondió que no.

La institución no supervisa ni revisa el cumplimiento del servicio prestado por el proveedor de internet, por lo tanto no se cumple el objetivo de control de ISO/IEC 27002:2013.

Gestión de incidentes en la seguridad de la información

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.

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 con el objetivo de control de ISO/IEC 27002:2013.

Responsabilidades y procedimientos

Para (ISO, 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 le preguntó a la entrevistada 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 ISO 27002:2013.

Notificación de eventos de seguridad de la información

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

Se le preguntó a la directora 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.

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 preguntó a la entrevistada si documenta y notifica a la administración, las sospechas de puntos débiles en la seguridad de la información tanto en la red como sistemas internos, a lo que respondió que no.

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.

Valoración de eventos de seguridad de la información y toma de decisiones

Conforme a (ISO, 2012), se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.

Se preguntó a la directora de informática si se evalúan y clasifican los incidentes de seguridad de la red, a lo que respondió que no.

La institución no cuenta con un plan que les permita la evaluación y clasificación de los eventos ocurridos en la red, esto con el fin de mejorar la toma de decisiones ante cualquier incidente ocurrido, por lo tanto no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

Aprendizaje de los incidentes de la seguridad de la información

Según (ISO, 2012), se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.

Se cuestionó a la entrevistada si se realiza análisis de incidentes de la seguridad de la información y si estos aportan conocimientos para reducir la probabilidad de futuros incidentes a lo que ella respondió que a veces porque no se efectúa un análisis detallado de los incidentes y tampoco estos son documentados.

La institución al no analizar y documentar los incidentes, no profundiza las causas probables de los eventos ocurridos, el cual les permitirá mitigar el impacto de futuros incidentes en la seguridad de la información, por esta razón no se cumple el objetivo de control de ISO/IEC 27002:2013.

Recopilación de evidencias

Para (ISO, 2012), la organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Se le pregunto a la directora de informática si se recopilan evidencias de los incidentes relacionado a la seguridad de la información en la red, a lo que respondo que no.

La institución no aplica procedimientos para la recopilación de evidencias, que le permita identificar los incidentes para preservar la información antes riesgos materializados, por lo tanto no cumple con el objetivo de control propuesto por ISO/IEC 27002:2013.

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

Continuidad de la seguridad de la información

De acuerdo a (ISO, 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.

Se cuestionó a la entrevistada si existen un plan de continuidad y recuperación de los procesos de seguridad de la información ante desastres a lo que ella 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.

Planificación de la continuidad de la seguridad de la información

Para (ISO, 2012), la organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

Se le preguntó a la directora de informática si se determinan cuáles son los requisitos de la seguridad de la información para su gestión durante situaciones críticas, a lo que respondió que no.

La institución no planifica la continuidad de la seguridad de la información, por lo tanto no cumple con el objetivo de control de ISO/IEC 27002:2013.

Implantación de la continuidad de la seguridad de la información

Según (ISO, 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.

Se interrogó a la entrevistada si se ha 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.

Redundancias

Para (ISO, 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 cuando los sistemas existentes se demuestren insuficientes.

Se preguntó a la directora de informática si existen dispositivos de red que permitan la redundancia en la infraestructura de red, a lo que respondió que no.

En la infraestructura de red de la institución no se implementan enlaces redundantes, por tanto esto hace inexistente la disponibilidad de la información ante un desastre, puesto que si los enlaces existentes caen automáticamente se pierde la comunicación de la información mediante la red, por consiguiente no se cumple con el objetivo de control de ISO/IEC 27002:2013.

Disponibilidad de instalaciones para el procesamiento de la información

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

Se cuestionó a la entrevistada, si los dispositivos redundantes ofrecen disponibilidad de la red en todo momento, a lo que respondió que no existen dispositivos que permitan la redundancia en la red.

No existen redundancias en la infraestructura de red, por lo tanto este objetivo de control de ISO/IEC 27002:2013 no se cumple.

Cumplimiento

Cumplimiento de los requisitos legales y contractuales

De acuerdo a (ISO, 2012), el diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

Se le preguntó a la directora de informática si están definidos los requisitos para la operación, uso y gestión de los recursos de red, a lo que respondió que no.

La institución no cuenta con una documentación que defina los requisitos para gestionar y operar de manera adecuada los recursos de red, por lo tanto no cumple con el objetivo de ISO/IEC 27002:2013.

Identificación de la legislación aplicable

Para (ISO, 2012), se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

Se interrogó a la entrevistada si existe la documentación con normativas legislativas que regulen los requisitos para el uso de los recursos de red, a lo que respondió que no.

En la institución no existen normativas legislativas que permita establecer requisitos estatuarios para la gestión de los sistemas de información, por lo tanto no se cumple el objetivo de control de ISO/IEC 27002:2013.

Derechos de propiedad intelectual (DPI)

Según (ISO, 2012), se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.

Se le cuestionó a la entrevistada si existen procedimientos aplicados para asegurar que se usen recursos originales tal como el uso de software con licencia, a lo que respondió que no.

La institución no aplica procedimientos que permitan asegurar el cumplimiento de los derechos de propiedad intelectual y el uso de software original, por ende no se cumple el objetivo de control de ISO/IEC 27002:2013.

Protección de los registros de la organización

Conforme a (ISO, 2012), los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

Se cuestionó a la directora de informática si los registros de información de la institución que se mueven mediante la red, están protegidos contra destrucción, falsificación, acceso y publicación, a lo que respondió que sí porque solo ella tiene acceso a los respaldos de información.

La institución no implementa mecanismos de seguridad que protejan adecuadamente los registros de información de la entidad, aunque los respaldos son resguardados por la directora de informática en la oficina, esto no garantiza la seguridad de estos datos en su totalidad, por lo tanto el objetivo de control de ISO/IEC 27002:2013 no se cumple.

Protección de datos y privacidad de la información personal

Según (ISO, 2012), se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

Se le preguntó a la directora de informática, si existen normativas legales aplicadas a la privacidad y protección de la información personal, a lo cual respondió que no.

En la institución no existen normativas legislativas que garanticen la protección y privacidad de la información personal, por lo tanto no se cumple objetivo de control propuesto por ISO/IEC 27002:2013.

Regulación de controles criptográficos

Para (ISO, 2012), se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

Se cuestionó a la entrevistada si se implementa controles de cifrado de la información que viaja en la red, a lo que respondió que no.

La institución no implementa mecanismo de codificación a la información, para asegurar la protección de los datos ante manipulación no autorizada, por lo tanto no se cumple el objetivo de control de ISO/IEC 27002:2013.

Revisiones de la seguridad de la información

Según (ISO, 2012), se deberían realizar revisiones regulares de la seguridad de los sistemas de información.

Se le preguntó a la directora de informática si revisa con regularidad la seguridad de los sistemas de información y de red, a lo que respondió que solo cuando estos presentan una falla.

En la institución solo lleva a cabo revisiones esporádicas en la seguridad de los sistemas de información, solo se realiza cuando estos presentan alguna falla, por lo tanto no se cumple el objetivo de ISO/IEC 27002:2013.

Revisión independiente de la seguridad de la información

Para (ISO, 2012), se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.

Se le preguntó a la entrevistada si se revisa el enfoque organizacional de la institución para la implementación de controles, políticas, procesos y procedimientos para la seguridad de la información en la red, a lo que respondió que no.

En la institución no están implementados procedimientos con enfoque organizacional que permitan la seguridad de la información, por lo tanto no se cumple el objetivo de control de ISO/IEC 27002:2013.

Cumplimiento de las políticas y normas de seguridad

De acuerdo a (ISO, 2012), los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisitos de seguridad correspondiente.

Se cuestionó a la entrevistada, si se revisan de manera regular el cumplimiento de las políticas y normas de seguridad de la información en la red, a lo que respondió que no.

Al no estar definidas e implementadas las políticas y normas de seguridad de la información en la institución no existe revisión de estas, por lo tanto no se cumple con el objetivo de control de ISO/IEC 27002:2013.

Comprobación del cumplimiento

Conforme (ISO, 2012), los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Se cuestionó a la directora de informática si se revisan de manera regular los recursos de red para verificar su óptimo funcionamiento para el cumplimiento con las políticas y normas de seguridad, a lo que respondió que no.

La institución no verifica que los sistemas de información y recursos de red cumplan con políticas y normas de seguridad, por ende no se cumple el objetivo de control de ISO/IEC 27002:2013.

Se realizó la tabla de cumplimiento de la norma ISO/IEC 27002:2013 mediante el análisis de la situación actual en la institución. Donde se evaluaron los dominios: políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad ligada al recurso humano, gestión de activos, control de acceso, cifrado, seguridad física y ambiental, seguridad operativa, seguridad en las telecomunicaciones, relaciones con suministradores, gestión de incidentes en la seguridad de la información, aspectos de seguridad de la información en la gestión de la continuidad del negocio y cumplimiento, para cada uno de ellos se toma una escala basada en el cien por ciento como el valor máximo de cumplimiento, así mismo los resultados pueden ser apreciados mediante la gráfica.

Tabla 4. Análisis para determinar el cumplimiento de la Norma ISO/IEC 27002:2013

Alcaldía Municipal de San Ramón, Matagalpa

Cumplimiento de ISO/IEC 27002:2013 en la Alcaldía Municipal de San Ramón, Matagalpa (Escala de medición en base al 100%)				
Dominio	Objetivo de control	Controles	Cumplimiento	%
Políticas de seguridad				0.0
	Directrices de la dirección en seguridad de la información	Conjunto de políticas	no se cumple	0.0
Aspectos organizativos de la seguridad de la información				0.0
	Organización Interna	Segregación de tareas	no se cumple	0.0
Seguridad ligada al recurso humano				15.0
	Antes de la contratación	Investigación de antecedentes	se cumple parcialmente	30.0
		Términos y condiciones de contratación	no se cumple	0.0
		Durante la contratación	no se cumple	0.0
		Concienciación, educación y capacitación en seguridad de la información	se cumple parcialmente	30.0
Gestion de activos				16.7
	Responsabilidades sobre los activos	Inventario de activos	se cumple parcialmente	50.0
		Uso aceptable de los activos	no se cumple	0.0
	Manejo de los Soportes de Almacenamiento		no se cumple	0.0
Control de acceso				23.3
	Requisitos de negocio para el control de accesos	Política de control de acceso	no se cumple	0.0
		Control de acceso a las redes y servicios asociados	se cumple parcialmente	30.0
	Gestión de acceso de usuarios	Gestión altas/bajas en el registro de usuarios	no se cumple	0.0
		Gestión de los derechos de acceso con privilegios especiales	se cumple	80.0
	Control de acceso a sistemas y aplicaciones	Restricciones de acceso a la información	se cumple parcialmente	30.0
		Gestión de contraseñas de usuarios	no se cumple	0.0
Cifrado				0.0
	Controles criptográficos	Políticas de uso de controles criptográficos	no se cumple	0.0
		Gestión de claves	no se cumple	0.0

Seguridad física y ambiental				**31.7**
	Áreas seguras	Controles fisicos de entrada	se cumple parcialmente	30.0
		Seguridad de oficinas, despachos y recursos	se cumple parcialmente	30.0
		Protección contra amenazas externas y ambientales	se cumple parcialmente	30.0
	Seguridad de los equipos	Seguridad del cableado	no se cumple	0.0
		Mantenimiento de los equipos	se cumple	100.0
		Seguridad de equipos y activos fuera de las instalaciones	no se cumple	0.0
Seguridad operativa				**27.1**
	Responsabilidades y procedimientos de operación	Documentación de procedimientos de operación	no se cumple	0.0
		Gestion de cambios	no se cumple	0.0
		Gestion de capacidades	se cumple	90.0
	Protección contra código malicioso	Controles contra código malicioso	se cumple parcialmente	50.0
	Copias de seguridad	Copias de seguridad de la información	se cumple parcialmente	50.0
	Registros de actividad y supervisión	Registro y gestión de eventos de actividad	no se cumple	0.0
	Consideraciones de las autitorías de los sistemas de información	Controles de auditoría de los sistemas de información	no se cumple	0.0
Seguridad en las telecomunicaciones				**4.3**
	Gestión de la seguridad en las redes	Controles de red	no se cumple	0.0
		Mecanimos de seguridad asociados a servicios de red	se cumple parcialmente	30.0
		Segregación de redes	no se cumple	0.0
	Intercambio de información con partes externas	Políticas y procedimientos de intercambio de información	no se cumple	0.0
		Acuerdos de intercambio	no se cumple	0.0
		Mensajeria electrónica	no se cumple	0.0
		Acuerdos de confidencialidad y secreto	no se cumple	0.0
Relaciones con suministradores				**0.0**
	Gestión de la prestación del servicio por suministradores	Supervisón y revisión de los servicios prestados por terceros	no se cumple	0.0

Gestión de incidentes en la seguridad de la información				5.0
	Gestión de incidentes de seguridad de la información y mejoras	Responsabilidades y procedimientos	no se cumple	0.0
		Notificación de eventos de seguridad de la información	se cumple parcialmente	30.0
		Notificación de puntos débiles de la seguridad	no se cumple	0.0
		Valoración de eventos de seguridad de la información y toma de desiciones	no se cumple	0.0
		Aprendizaje de los incidentes de la seguridad de la información	no se cumple	0.0
		Recopilación de evidencias	no se cumple	0.0
Aspectos de seguridad de la información en la gestión de la continuidad de negocio				0.0
	Continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información	no se cumple	0.0
		Implantación de la continuidad de la seguridad de la información	no se cumple	0.0
	Redundancias	Disponibiliad de las intalaciones para el procesamiento de la información	no se cumple	0.0
Cumplimiento				0.0
	Cumplimiento de los requisitos legales y contractuales	Identificación de la legislación aplicable	no se cumple	0.0
		Derechos de propiedad intelectual (DPI)	no se cumple	0.0
		Protección de los registros de la organización	no se cumple	0.0
		Protección de los datos y privacidad de la infomación personal	no se cumple	0.0
		Regulación de los controles criptográficos	no se cumple	0.0
	Revisión de la seguridad de la información	Revisión independiente de la seguridad de la información	no se cumple	0.0
		Cumplimiento de las políticas y normas de seguridad	no se cumple	0.0
		Comprobación del cumplimiento	no se cumple	0.0

Fuente: Elaboración propia a partir de criterios de cumplimiento de la norma ISO/IEC 27002:2013

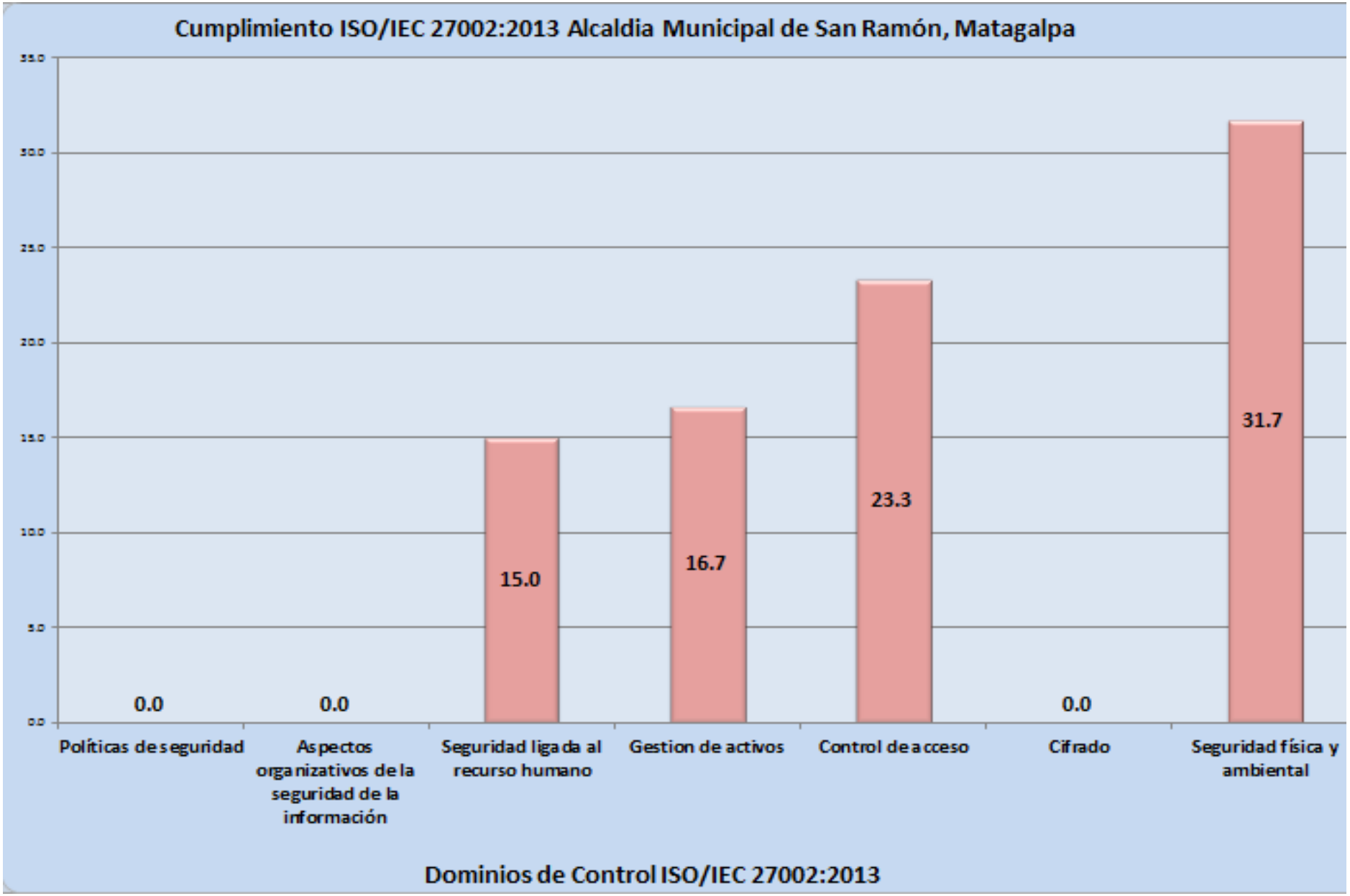
Tabla 5. Cumplimiento actual ISO/IEC 27002:2013

Dominio	% cumplimiento
Políticas de seguridad	0.0%
Aspectos organizativos de la seguridad de la informacion	0.0%
Seguridad ligada al recurso humano	15.0%
Gestion de activos	16.7%
Control de acceso	23.3%
Cifrado	0.0%
Seguridad fisica y ambiental	31.7%
Seguridad operativa	27.1%
Seguridad en las telecomunicaciones	4.3%
Relaciones con suministradores	0.0%
Gestion de incidentes en la seguridad de la información	5.0%
Aspectos de seguridad de la información en la gestión de	0.0%
Cumplimiento	0.0%

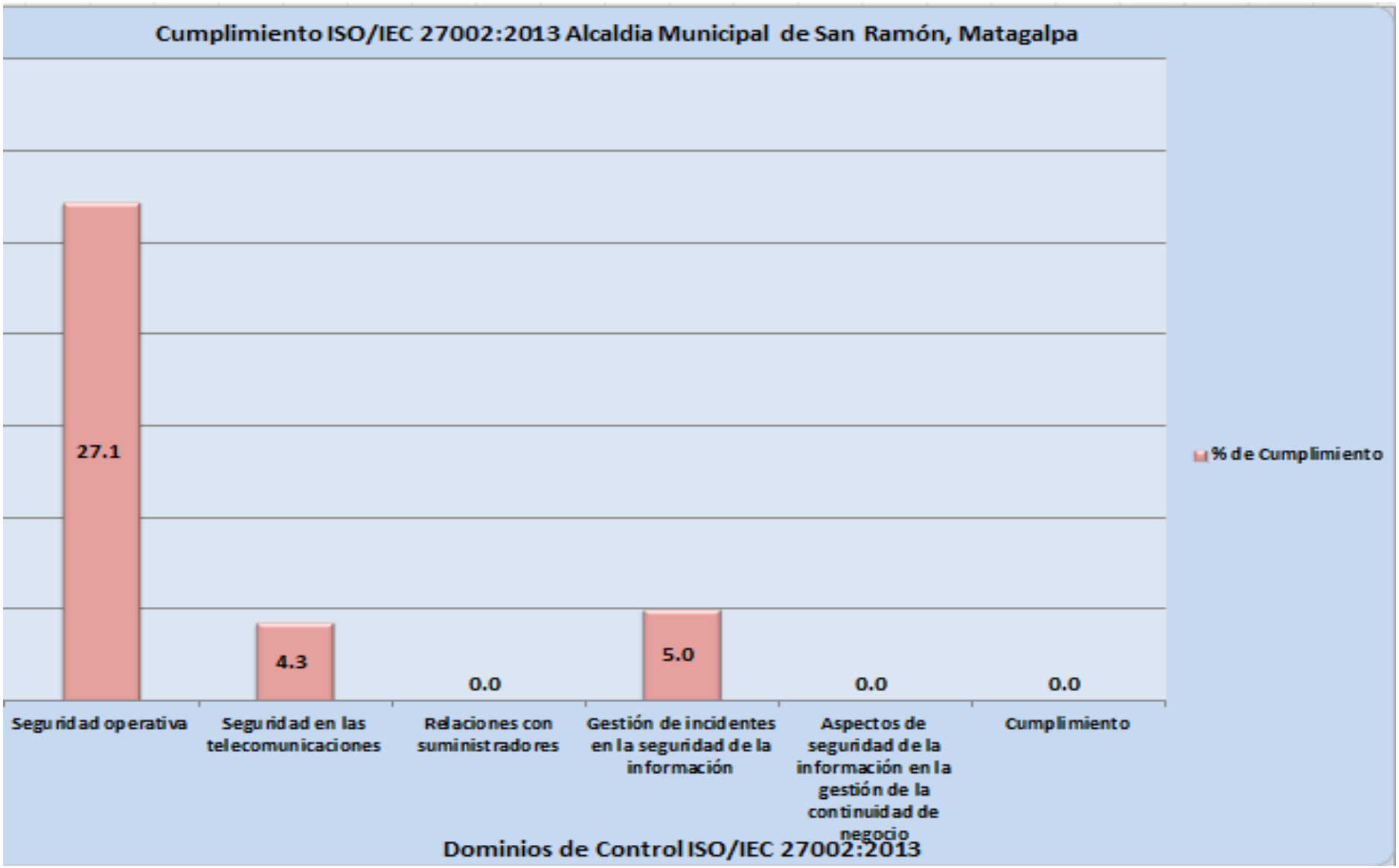
Total de cumplimiento ISO 27002:2013	**10.56 %**

Fuente: Elaboración propia a partir de criterios de cumplimiento de la norma ISO/IEC 27002:2013

Gráfico 1. Cumplimiento ISO/IEC 27002:2013



Fuente: Elaboración propia a partir de los resultados del cumplimiento de la norma ISO/IEC 27002:2013


Cumplimiento ISO/IEC 27002:2013 Alcaldia Municipal de San Ramón, Matagalpa
27.1
4.3
0.0
5.0
0.0
0.0
% de Cumplimiento
Seguridad operativa
Seguridad en las telecomunicaciones
Relaciones con suministradores
Gestión de incidentes en la seguridad de la información
Aspectos de seguridad de la información en la gestión de la continuidad de negocio
Cumplimiento
Dominios de Control ISO/IEC 27002:2013

X. CONCLUSIONES

Basados en los resultados de la 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 concluyó lo siguiente:

- Los procesos que se llevan a cabo en las redes de la institución son; el uso del Sistema Integrado de Administración Financiera Municipal (SIAFM), acceso a sitios web controlados mediante un proxy SQUID y videoconferencias, también se concluyó que no existe personal capacitado dentro de la institución, el cual este destinado a la administración, mantenimiento de los recursos de red y seguridad de la información.

- Mediante los objetivos de control de ISO/IEC 27002:2013 se determinaron deficiencias relevantes tales como:
  - ✓ No hay políticas de seguridad definidas.
  - ✓ No existe documentación de la red.
  - ✓ Recursos de red fuera de áreas seguras.
  - ✓ El cableado de red no está estructurado.
  - ✓ No se realizan auditorías a la seguridad de la información en las redes.
  - ✓ No existen plan de contingencia y plan de continuidad en la seguridad de la información.

- Se determinó el porcentaje de cumplimiento de ISO/IEC 27002:2013, donde el resultado refleja que la institución no cumple de manera recomendada los objetivos de control, políticas de seguridad 0%, aspectos organizativos de la seguridad de la información 0%, seguridad ligada al recurso humano 15%, gestión de activos 16.7%, control de acceso 23.3%, cifrado 0%, seguridad física y ambiental 31.7%, seguridad operativa 27.1%, seguridad en las telecomunicaciones 4.3%, relaciones con suministradores 0%, gestión de incidentes en la seguridad de la información 5%, aspectos de seguridad de la información en la gestión de la continuidad del negocio 0% y cumplimiento 0%, lo que demuestra la deficiencia de la infraestructura de red y de la seguridad de la información.

- A través de los resultados conseguidos se realizó la propuestas de mejoras en la cual se reflejan las deficiencias encontradas más relevantes en la institución mediante los objetivos de control de ISO/IEC 27002:2013. De igual manera se reflejan las recomendaciones adecuadas para mejorar la infraestructura de red e implementar buenas prácticas para la seguridad de la información (Ver Anexo 1).

XI. RECOMENDACIONES

Para mejorar la infraestructura de red y aplicar objetivos de control para la seguridad de la información en la Alcaldía Municipal de San Ramón, Matagalpa se sugiere lo siguiente:

A la directora de informática:

- Tomar como referencia la guía propuesta, con el fin de mejorar la infraestructura de red en la institución y la seguridad de la información.

A la gerencia:

- Tomar conciencia de la importancia del área de informática en los procesos críticos de la institución, para garantizar la calidad de los servicios y procesos claves de TI.

- Incrementar el personal en el área informática, con el fin de brindar soporte y soluciones de manera rápida.

- Brindar capacitaciones tecnológicas al personal de informática, para mejorar la administración de los recursos de TI.

- Implementar estándares para las buenas prácticas en la seguridad de la información y administración de redes.

XII. BIBLIOGRAFÍA

Alcocer, P.-P. V., Gomez, J. M., Prat, A. M., & Albareda, X. M. (2006). Programación en C++ para ingenieros. Editorial Paraninfo.

Alvarez, S. (5 de enero de 2012). Arquitectura de red. Recuperado el 15 de mayo de 2015, de DesarrolloWeb: http://www.desarrolloweb.com/articulos/arquitectura-red.html

Andreu Cepa, D. (2011). Auditoria de una red de Comunicaciones. Cataluña.

Andreu Gómez, J. (2010). Servicios en Red. Editex.

Andreu, J. (2011). Servicios FTP (Servicios en red). Editex.

Arce Cuesta, N. C., & Tacuri Japa, A. F. (2010). Auditoria física y lógica a las redes de comunicaciones de computadores de la fabrica PASAMARÍA S.A . Cuenca Ecuador.

Blandon, S., & Galdámez, S. (2016). Evaluación de la Infraestructura de la Red LAN, "Empresa CECOCAFEN", basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, Primer Semestre 2016. Matagalpa.

Carmona Romera, G. (2014). Sistema Operativo, búsqueda de información: Internet-Intranet y correo electrónico. IC Editorial.

Castro Gil, M. A., Diaz Orueta, G., Alzórriz Alemendarez, I., & Ruiz, E. (2014). Procesos y herramientas para la seguridad en las redes. Editorial UNED.

Chacón, J., Erazo, R., España, G., Montoya, J., & Portillo, K. (18 de Enero de 2008). Monografias. Recuperado el 28 de Mayo de 2015, de Estándar Internacional ISO/IEC 27002: http://www.monografias.com/trabajos67/estandar-internacional/estandar-internacional2.shtml

CIBERTEC. (2012). Arquitectura de redes y comunicaciones. Lima.

Cisco Systems, inc. (2007). Aspéctos básicos de networking. San Francisco .

Colobran Huguet, M., Arqués Soldevila, J. M., & Galindo, E. M. (2008). Administración de sistemas operativos en red. Barcelona: Editorial UOC.

Concejero, J. B., Mondejar, J. B., Romero, O. R., Ternero, M. D., Rodriguez, J. R., Anton, G. S., & Castillo, F. S. (2014). Redes locales. Ediciones Paraninfo, S.A.

Esteller Millán, J. M. (2012). Instalaciones de megafonía y sonorización. Editorial Paraninfo.

Explorable.com. (16 de septiembre de 2009). Muestreo por conveniencia. Recuperado el 25 de Mayo de 2015, de Muestreo por conveniencia: https://explorable.com/es/muestreo-por-conveniencia

Gallego, J. C. (2010). FPB - Instalación y mantenimiento de redes para transmisión de datos. Editlex.

Gómez Joaquín, A. (2011). Redes locales. Editex.

Heredero, C. d. (2004). Informática y comunicaciones en la empresa. ESIC .

Herrera Peréz, E. (2003). Tecnologías y redes de transmisión de datos. Editorial Limusa.

Hesselbach Serra, X., & Bosch, J. (2002). Análisis de redes y sistemas de comunicaciones. Barcelona: Univ. Politèc. de Catalunya.

Higuera, A. G., & García, F. J. (2007). CIM, el computador en la automatización de la producción. Univ de Castilla La Mancha.

Joaquín, A. (2011). Servicios DNS (Servicios en red). Editex.

Koontz, H., & Weihrich, H. (2007). Elementos de administración: Un enfoque internacional. En H. Koontz, & H. Weihrich, Elementos de administración: Un enfoque internacional (pág. 372). México, DF: Miembro de la camara nacional de la industria Editorial Mexicana.

Lobos Barrera, E. Y. (2005). Auditorias de Empresas en el área de Telecomunicaciones. Guatemala.

López, A. R. (2012). ISO 27002.es. Recuperado el 20 de Mayo de 2015, de El portal de ISO 27002 en Español: http://iso27000.es/iso27002.html

López, P. A. (2010). Seguridad informática. Editex.

Mayol Arnao, R. N. (2006). Modelo para la auditoría de la seguridad informática en la rede de datos de la universidad de los andes. Merida.

Mendoza, L. (2012). Evaluación de la red de computadores de UNAN Managua FAREM Matagalpa, período 2012. Matagalpa.

Misfud, E. (2012). Introducción a la seguidad informática.

Montero, I. B. (2014). Instalación y mantenimiento de redes para transmisión de datos. Ediciones Paraninfo, S.A.

Moya, J. M., & Huidobro, J. M. (2006). Redes y servicios de telecomunicaciones. Editorial Paraninfo.

NimboSystems. (3 de Mayo de 2013). NimboSystems. Recuperado el 15 de Mayo de 2015, de Áreas principales de la norma ISO 27002: http://nimbosystems.com/wp/?p=52

Orellana Benavides, L. A. (2003). Seguridad en redes de datos. Soyapango, Ciudadela Don Bosco.

Rodríguez, L. D. (2007). El gran libro del PC interno. Marcombo.

Tanenbaum, A. (2003). Redes de computadoras. México: Editorial de México.

Vázquez, P. G., Baeza, J. P., & Herías, F. A. (2010). Redes y transmisión de datos. Alicante: Universidad de Alicante.

ANEXOS

Anexo No 1

Guía de mejoras para la infraestructura de red LAN, Alcaldía Municipal de San Ramón, Matagalpa.

Primer semestre 2016

Responsables:

Br. Elí Josué Castillo Montenegro

Br. Norman Antonio Tercero Mendoza

Lugar y fecha del dictamen:

Matagalpa, Noviembre 2016

23 de Noviembre de 2016

Ing. Meylin Machado López

Directora de Informática de la Alcaldía Municipal de San Ramón, Matagalpa

Se presenta el resultado de la evaluación de la infraestructura de red LAN "Alcaldía Municipal de San Ramón, Matagalpa" comprendida en el primer semestre del año 2016. El informe de la investigación incluye las conclusiones y guía de recomendaciones respecto al estado actual de la infraestructura de red LAN, dicha investigación se llevó a cabo, bajo la guía de buenas prácticas de la seguridad de la información norma ISO/IEC 27002:2013.

Br. Elí Josué Castillo M

Responsable de evaluación

Br. Norman A Tercero M

Responsable de evaluación

CONTENIDO

ANEXOS DE GUÍA DE MEJORAS

INTRODUCCIÓN

Esta guía presenta las pautas necesarias para mejorar la infraestructura de red LAN de la Alcaldía Municipal de San Ramón, bajo la norma ISO/IEC 27002:2013, la cual brinda una sólida base para la implementación de buenas prácticas en la administración y seguridad de la red.

La guía expone las debilidades encontradas y la situación actual de la infraestructura de red, así mismo se exponen las recomendaciones necesarias para mitigar las debilidades y fortalecer la seguridad de la red.

El principal objetivo de la guía es brindar soluciones viables para la reestructuración de la infraestructura de red y esta cumpla con buenas prácticas de seguridad de la información, para brindar una mejor administración, seguridad lógica y física, documentación y organización relevante.

RESUMEN EJECUTIVO

Esta investigación consistió en conocer la infraestructura de red actual para crear la guía de mejoras, la cual permita mejorar la infraestructura de red LAN de la Alcaldía Municipal de San Ramón, Matagalpa, bajo la norma ISO/IEC 27002:2013, en el primer semestre 2016, con el fin de aplicar buenas prácticas en la administración y seguridad de la red.

La guía se ha elaborado conforme a los objetivos específicos propuestos, los cuales nos han guiado en el transcurso de la investigación. De igual manera se utilizó la norma ISO/IEC 27002:2013 como marco de trabajo para buenas prácticas en la seguridad de la información, lo cual nos permitió determinar puntos débiles en la red mediante los objetivos de control propuestos y así también poder determinar el nivel de cumplimiento.

Se realizaron los instrumentos para la recolección de la información más relevante y posteriormente esta se analizó, estos instrumentos comprendieron las entrevistas dirigidas a la directora de informática, la guía de observación y la tabla de cumplimiento donde se evaluaron cada uno de los dominios que se tomaron en cuenta a partir de la ISO.

Mediante el análisis y los resultados de la información obtenida se ha concluido, que la infraestructura de red de la institución se encuentra actualmente mal organizada y no esta optimizada adecuadamente para ofrecer el desempeño óptimo, de igual manera no se aplican buenas prácticas de administración y seguridad en la red, también se determinó el porcentaje de cumplimiento de cada dominio, dichos resultados se reflejan en la gráfica, lo que demuestra la deficiencia de la infraestructura de red y de la seguridad de la información, lo cual permite a la institución tener una visión clara de la situación actual y tomar conciencia en la importancia de aplicar buenas prácticas de administración y seguridad en su infraestructura de red.

ALCANCE DEL ESTUDIO REALIZADO

Conforme a lo acordado con la institución evaluada, se da a conocer la guía propuesta de mejoras a la infraestructura de red LAN de la Alcaldía Municipal de San Ramón, Matagalpa, en el primer semestre 2016, donde se tomó como marco de referencia los dominios de control de ISO/IEC 27002:2013 y criterios de infraestructura de red tales como:

- Arquitectura de red (tolerancia a fallas, escalabilidad, QoS, Seguridad).
- Tipos de red.
- Topología de red.
- Elementos de red (mensajes, dispositivos, medios de transmisión, servicios, reglas).
- Calidad de las comunicaciones.
- Infraestructura física (dispositivos de red, medios de transmisión, estación de trabajo, políticas de seguridad físicas).
- Infraestructura lógica (servidores, direccionamiento IP, servicios de red, amenazas lógicas, políticas de seguridad lógicas).

OBJETIVOS DE LA GUIA

General:

Mejorar la infraestructura de red LAN de la Alcaldía Municipal de San Ramón, Matagalpa, bajo la norma ISO/IEC 27002:2013, primer semestre 2016.

Específicos:

- ✓ Realizar el informe del nivel de cumplimiento la norma ISO por parte de la institución.
- ✓ Señalar los hallazgos y sugerir las recomendaciones necesarias para mitigar las debilidades y fortalecer la infraestructura de red.
- ✓ Indicar las problemáticas relevantes encontradas.

METODOLOGÍA DE LA GUÍA

Con el propósito de mejorar la infraestructura de red de la Alcaldía Municipal de San Ramón, Matagalpa, se determinó los objetivos y alcance de la guía, mediante el análisis de la información obtenida de la evaluación, que se llevó a cabo bajo los objetivos de control de ISO/IEC 27002:2013 y diversos aspectos que contemplan las redes.

En el plan de evaluación se incluyó:

Los criterios evaluados mediante las características de las infraestructuras de redes y los dominios de control de ISO/IEC 27002:2013, así como los riesgos identificados más relevantes y las sugerencias para la mitigación de estos.

La guía se estructuro mediante ISO/IEC 27002:2013, la cual es una guía de buenas prácticas de seguridad de la información que contiene criterios para la buena administración e implementación de las redes.

ISO/IEC 27002:2013 consta de 14 dominios:

- ✓ Políticas de seguridad
- ✓ Aspectos organizativos de la seguridad de la información
- ✓ Seguridad ligada a los recursos humanos
- ✓ Gestión de activos
- ✓ Control de acceso
- ✓ Cifrado
- ✓ Seguridad Física y ambiental
- ✓ Seguridad operativa
- ✓ Seguridad en las telecomunicaciones
- ✓ Adquisición, desarrollo y mantenimiento de los sistemas de información.
- ✓ Relaciones con suministradores
- ✓ Gestión de incidentes en la seguridad de la información
- ✓ Aspectos de seguridad de la información en la gestión de continuidad del negocio
- ✓ Cumplimiento

De estos 14 dominios se tomaron en cuenta 13 de ellos:

- **Políticas de seguridad**
- **Aspectos organizativos de la seguridad de la información**
- **Seguridad ligada a los recursos humanos**
- **Gestión de activos**
- **Control de acceso**
- **Cifrado**
- **Seguridad Física y ambiental**
- **Seguridad operativa**
- **Seguridad en las telecomunicaciones**
- **Relaciones con suministradores**
- **Gestión de incidentes en la seguridad de la información**
- **Aspectos de seguridad de la información en la gestión de continuidad del negocio**
- **Cumplimiento**

No se tomó en cuenta el dominio **Adquisición, desarrollo y mantenimiento de los sistemas de información,** debido a que la investigación apunto a criterios de evaluación de infraestructura de red, por lo que no se requirió evaluar el soporte y desarrollo de sistemas de información.

Cada dominio presenta objetivos de control y controles, de los cuales se evaluaron los siguientes:

- **Políticas de seguridad**
    - **Directrices de la dirección en seguridad de la información**
        - Conjunto de políticas

- **Aspectos organizativos de la seguridad de la información**
    - **Organización interna**
        - Segregación de tareas

- **Seguridad ligada a los recursos humanos**
  - **Antes de la contratación**
    - Investigación de antecedentes
    - Términos y condiciones de contratación
    - Durante la contratación
    - Concienciación, educación y capacitación en seguridad de la información

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

- **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**
    - Gestión altas/bajas en el registro de usuarios
    - Gestión de los derechos de acceso con privilegios **especiales**
  - **Control de acceso a sistemas y aplicaciones**
    - Restricción de acceso a la información
    - Gestión de contraseñas de usuario

- **Cifrado**
  - **Controles criptográficos**
    - Políticas de uso de controles criptográficos
    - Gestión de claves

- **Seguridad Física y ambiental**
  - **Áreas seguras**
    - Controles físicos de entrada
    - Seguridad de oficinas, despachos y recursos
    - Protección contra amenazas externas y ambientales
  - **Seguridad de los equipos**
    - Seguridad del cableado
    - Mantenimiento de los equipos
    - Seguridad de los equipos y activos fuera de las instalaciones

- **Seguridad operativa**
  - **Responsabilidades y procedimientos de operación**
    - Documentación de procedimientos de operación
    - Gestión de cambios
    - Gestión de capacidades
  - **Protección contra código malicioso**
    - Controles contra código malicioso
  - **Copias de seguridad**
    - Copias de seguridad de la información
  - **Registros de actividad y supervisión**
    - Registro y gestión de eventos de actividad
  - **Consideraciones de las auditorias de los sistemas de información**
    - Controles de auditoria de los sistemas de información

- **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
  - Acuerdos de intercambios
  - Mensajería electrónica
  - Acuerdos de confidencialidad y secreto

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

- **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
    - Valoración de eventos de seguridad de la información y toma de decisiones
    - Aprendizaje de los incidentes de la seguridad de la información
    - Recopilación de evidencias

- **Aspectos de seguridad de la información en la gestión de continuidad del negocio.**
  - **Continuidad de la seguridad de la información**
    - Planificación de la 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

- **Cumplimiento**
  - **Cumplimiento de los requisitos legales y contractuales**
    - Identificación de la legislación aplicable
    - Derechos de propiedad intelectual (DPI)
    - Protección de los registros de la organización
    - Protección de los datos y privacidad de la información personal
    - Regulación de los controles criptográficos
  - **Revisión de la seguridad de la información**
    - Revisión independiente de la seguridad de la información
    - Cumplimiento de las políticas y normas de seguridad
    - Comprobación de cumplimiento

HALLAZGOS Y RECOMENDACIONES

En este apartado se exponen los detalles de los riesgos relevantes encontrados en la infraestructura de red.

El análisis de los riesgos y recomendaciones están basados bajo los controles propuestos por ISO/IEC 27002:2013.

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 la institución no se han definido e implementado políticas de seguridad en las redes.

Hallazgo	No hay implementación de políticas de seguridad.
Objetivo	
Desarrollar un plan que permita definir e implementar las políticas de seguridad	
Recomendación	
Elaborar un plan de seguridad, que deberá ser aceptado y comunicado, donde se delimiten las responsabilidades en dependencia del organigrama de la institución. Definir las metodologías de seguridad con sus respectivos procesos y políticas destinadas a la protección de la información.	
Riesgos a mitigar	
Riesgos vulnerables asociados a la confidencialidad, integridad y disponibilidad de la información.	

Dominio: Aspectos organizativos de la seguridad de la información

Objetivo de control: Organización interna

Control: Segregación de tareas

Informe: No se cumple.

No se han definido las tareas de la directora de informática, respecto a la seguridad de la información, tampoco no se ha definido un área de TI bajo el dominio de la alta gerencia. Existe el área de informática que brinda los servicios tecnológicos bajo el dominio de la administración.

Hallazgo	No están definidas las tareas respecto a la seguridad de la información.
Objetivo	
Definir y realizar las tareas necesarias para mantener la seguridad de la información	
Recomendación	
Elaborar un plan de tareas, que defina los pasos necesarios aplicables para mantener la seguridad de la información.	
Riesgos a mitigar	
Desfalco o fraude interno en la institución.	

Hallazgo	No se ha definido un área de TI con dominio de la alta gerencia.
Objetivo	
Definir un área de TI que permita la toma de decisiones con la alta gerencia.	
Recomendación	
Definir e implementar el área de TI con dominio de la gerencia.	
Riesgos a mitigar	
Toma de decisiones con incertidumbre. Malas estrategias de trabajo. Recesión económica.	

Dominio: Seguridad ligada a los recursos humanos.

Objetivo de control: Antes de la contratación.

Control: Investigación de antecedentes.

Informe: Se cumple parcialmente

No se investiga a fondo los antecedentes del personal, ya que solo se piden cartas de recomendación.

Hallazgo	No se investiga a fondo los antecedentes.
Objetivo	
Seguridad en los procesos de selección del personal.	
Recomendación	
Investigación de referencias personales y laborales. Investigación de antecedentes y verificación de referencias profesionales.	
Riesgos a mitigar	
Contratación negligente.	

Control: Términos y condiciones de contratación

Informe: No se cumple.

No se han definido los términos y condiciones del trabajo.

Hallazgo	No están definidos los términos y condiciones.
Objetivo	
Establecer las obligaciones contractuales del empleado y la institución.	
Recomendación	
Elaborar el documento de términos y condiciones que contenga las cláusulas que regule los contratos de adhesión.	
Riesgos a mitigar	
Legal y contractual.	

Control: Durante la contratación.

Informe: No se cumple.

No están definidas las responsabilidades de la dirección para garantizar la seguridad de la información.

Hallazgo	No están definidas las responsabilidades de la dirección.
Objetivo	
Garantizar la seguridad de la información en los puestos de trabajo.	
Recomendación	
Definir, documentar e implementar las responsabilidades que debe adquirir la dirección para velar por el cumplimiento de la seguridad de la información en los puestos de trabajo de la institución, principalmente en el área de informática.	
Riesgos a mitigar	
Manipulación no autorizada de la información. Fraudes internos.	

Control: Concienciación, educación y capacitación en seguridad de la información.

Informe: Se cumple parcialmente.

La directora de informática recibe capacitaciones, pero estas no se enfocan en la seguridad, mantenimiento y administración de las tecnologías de la información.

Hallazgo	No hay capacitación asociada a las tecnologías de la información.
Objetivo	
Mejorar la administración de la seguridad de las tecnologías de la información.	
Recomendación	
Promover las capacitaciones sobre la seguridad, mantenimiento y administración de las tecnologías de la información.	
Riesgos a mitigar	
Malas prácticas de administración de los recursos informáticos.	

Dominio: Gestión de activos

Objetivo de control: Responsabilidades sobre los activos

Control: Inventario de activos

Informe: Se cumple parcialmente.

Se realiza inventario de manera muy general.

Hallazgo	No se lleva a cabo un inventario detallado de los recursos informáticos.
Objetivo	
Mejorar la calidad de los inventarios.	
Recomendación	
Elaborar un formato adecuado de inventario, que detalle cada aspecto importante de los recursos informáticos.	
Riesgos a mitigar	
Robo y daño de los recursos informáticos. Inventario de pérdidas. Vida Útil.	

Control: Uso aceptable de los activos.

Informe: No se cumple.

No existen procedimientos que regulen el uso adecuado de los activos.

Hallazgo	No se han implementado procedimientos para regular el uso adecuado de los activos.
Objetivo	
Implementar procedimientos que regulen el uso correcto de los activos informáticos.	
Recomendación	
Definir, documentar e implementar procedimientos que regular el uso adecuado de los activos informáticos.	
Riesgos a mitigar	
Mala manipulación y uso inadecuado de los recursos informáticos.	

Control: Manejo de los soportes de almacenamiento.

Informe: No se cumple.

No existen controles y procedimientos aplicados a la protección de los medios de almacenamiento.

Hallazgo	No se protegen los medios de almacenamiento.
Objetivo	
Controlar y proteger los medios de almacenamiento.	
Recomendación	
Definir y establecer los procedimientos operativos adecuados para proteger los medios de almacenamiento de información.	
Riesgos a mitigar	
Divulgación, modificación, retirada y destrucción no autorizadas.	

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 se controla el acceso a la información.

Hallazgo	No hay políticas de control de acceso a la información y recursos informáticos.
Objetivo	
Implementar políticas de control de acceso a la información y recursos informáticos.	
Recomendación	
Definir, documentar y establecer políticas de control de acceso en base a las necesidades de seguridad de la institución.	
Riesgos a mitigar	
Acceso y manipulación no autorizada a la información y recursos informáticos.	

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

Informe: Se cumple parcialmente.

No se han implementado controles adecuados para el acceso a la red desde todas las áreas de la institución, ya que solo el área de contabilidad cuenta con controles específicos de acceso a la red.

Hallazgo	No se han definido controles adecuados de acceso a la red.
Objetivo	
Garantizar el control de acceso a la red.	
Recomendación	
Definir, documentar e implementar controles de acceso a la red en todas las áreas de la institución.	
Riesgos a mitigar	
Uso no autorizado de la red. Acceso no autorizado de los servicios de red. Acceso no autorizado a dispositivos finales, intermediarios y servidores.	

Objetivo de control: Gestión de acceso de usuarios

Control: Gestión altas/bajas en el registro de usuarios

Informe: No se cumple.

No se realizan procedimientos de alta/baja de usuarios.

Hallazgo	No existe procedimiento formal de alta/baja de usuarios.
Objetivo	
Definir los procedimientos de alta/baja de usuarios.	
Recomendación	
Definir y establecer los procedimientos adecuados para dar de alta/baja a un usuario de los sistemas en red.	
Riesgos a mitigar	
Riesgos operacionales, acceso y modificaciones no autorizadas.	

Control: Gestión de los derechos de acceso con privilegios especiales

Informe: Se cumple.

Se controlan los usuarios con privilegios especiales en la red.

Hallazgo	Se lleva el control de usuarios con privilegios especiales de manera informal.
Objetivo	
Elaborar la documentación que permita llevar un control formal.	
Recomendación	
Elaborar la documentación necesaria para llevar un control formar y detallado de los usuarios con privilegios especiales.	
Riesgos a mitigar	
Accesos de alto nivel, no autorizados a los sistemas en red.	

Objetivo de control: Control de acceso a sistemas y aplicaciones

Control: Restricción de acceso a la información

Informe: Se cumple parcialmente.

Se implementan cambios de contraseña cada dos meses en el servidor de red, se controla la entrada al área de informática, se hace uso de proxy para la comunicación del sistema en red.

Hallazgo	Los dispositivos de red que están fuera del área de informática están desprotegidos.
Objetivo	
Asegurar el acceso a la información.	
Recomendación	
Implementar normas y políticas de seguridad a los dispositivos fuera del área de informática.	
Riesgos a mitigar	
Acceso y modificación no autorizada a los sistemas de información en red.	

Objetivo de control: Gestión de contraseñas de usuarios.

Informe: No se cumple.

No se gestionan las contraseñas de usuario.

Hallazgo	No se aplican procedimientos de gestión de contraseña de usuarios.
Objetivo	
Gestionar y asegurar contraseñas de calidad.	
Recomendación	
Definir y establecer los procedimientos de gestión y asignación de contraseñas seguras.	
Riesgos a mitigar	
Acceso y manipulación no autorizada a la información.	

Dominio: Cifrado.

Objetivo de control: Controles criptográficos.

Control: Políticas de uso de controles criptográficos.

Informe: No se cumple.

No controles criptográficos ni regulaciones de control criptográfico.

Hallazgo	No existen controles criptográficos ni políticas de uso de controles criptográficos.
Objetivo	
Proteger la confidencialidad, autenticidad e integridad de la información.	
Recomendación	
Definir y establecer políticas de uso y procedimientos de control de encriptamiento de la información.	
Riesgos a mitigar	
Rotura de contraseñas. Robo y destrucción de información. Manipulación de la información.	

Control: Gestión de claves.

Informe: No se cumple.

No se gestionan claves de encriptamiento.

Hallazgo	No existe gestión de claves de encriptamiento.
Objetivo	
Protección de claves criptográficas.	
Recomendación	
Desarrollar e implementar políticas de uso, protección y ciclo de vida de las claves criptográficas.	
Riesgos a mitigar	
Perdida de claves. Perdida de información sensible.	

Dominio: Seguridad Física y ambiental.

Objetivo de control: Áreas seguras.

Control: Controles físicos de entrada.

Informe: Se cumple parcialmente.

Aproximadamente los 50% de los activos de informáticas no se encuentran en áreas seguras. El único control físico de entrada es la puerta oficina de informática y sala de video conferencias.

Hallazgo	No se han definido, documentado e implementado controles físicos entrada.
Objetivo	
Garantizar la seguridad de la información y activos informáticos.	
Recomendación	
Implementar controles físicos de entrada, como: uso de credenciales, registros de firmas de entrada y salida, cámaras de seguridad, alarmas antirrobo.	
Riesgos a mitigar	
Acceso físico no autorizado Daño e interferencia de la información y activos informáticos.	

Control: Seguridad de oficinas, despachos y recursos.

Informe: Se cumple parcialmente.

No se ha diseñado y aplicado sistemas de seguridad física a las oficinas, solo presentan como método de seguridad las puertas de entrada.

Hallazgo	No existen sistemas de seguridad física aplicados.
Objetivo	
Seguridad física a las oficinas, salas e instalaciones de la institución.	
Recomendación	
Implementar sistemas de seguridad física.	
Riesgos a mitigar	
Desastres naturales, incendios accidentales, tormentas e inundaciones. Acceso no autorizado. Sabotajes internos deliberados.	

Control: Protección contra amenazas externas y ambientales

Informe: Se cumple parcialmente.

Al menos el 50% de los activos informáticos están protegidos.

Hallazgo	No se aplica protección contra ataques maliciosos o accidentes al 50 % de los activos informáticos.
Objetivo	
Protección de activos informáticos.	
Recomendación	
Implementar mecanismos de protección a los activos informáticos.	
Riesgos a mitigar	
Desastres naturales, incendios accidentales, tormentas e inundaciones. Sabotajes internos deliberados, ataques maliciosos.	

Objetivo de control: Seguridad de los equipos.

Control: Seguridad del cableado.

Informe: No se cumple.

El cableado no se encuentra canaleteado y debidamente protegido.

Hallazgo	El cableado no está estructurado.
Objetivo	
Estructuración del cableado.	
Recomendación	
Aplicar estándares [4]ANSI/TIA/EIA-568-B.	
Riesgos a mitigar	
Intercepción de información. Interferencia en las comunicaciones. Daño del cableado.	

Control: Mantenimiento de los equipos.

Informe: Se cumple.

Se realiza mantenimiento preventivo y correctivo cada 3 a 5 meses.

Hallazgo	No se ha definido un plan de mantenimiento.
Objetivo	
Garantizar la disponibilidad y funcionalidad de los activos informáticos.	
Recomendación	
Definir y documentar un plan de mantenimiento detallado.	
Riesgos a mitigar	
Vida útil.	

[4] **ANSI/TIA/EIA-568-B:** son tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones. Para más información ver: http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf

Control: Seguridad de los equipos y activos fuera de las instalaciones.

Informe: No se cumple.

No se aplican mecanismos de seguridad a los activos y equipos informáticos fuera de la oficina de informática.

Hallazgo	No existe seguridad para los activos y equipos informáticos fuera de la oficina de informática.
Objetivo	
Garantizar la seguridad de los activos informáticos.	
Recomendación	
Implementar mecanismos de seguridad física.	
Riesgos a mitigar	
Acceso y manipulación no autorizada. Daños a los activos informáticos. Robo.	

Dominio: Seguridad operativa.

Objetivo de control: Responsabilidades y procedimientos de operación.

Control: Documentación de procedimientos de operación.

Informe: No se cumple.

No se realiza documentación de los procedimientos de operación de los dispositivos informáticos.

Hallazgo	No existe documentación de procedimientos de operación.
Objetivo	
Garantizar el manejo correcto de los dispositivos informáticos.	
Recomendación	
Definir y documentar un plan de mantenimiento detallado.	
Riesgos a mitigar	
Vida útil.	

Control: Gestión de cambios.

Informe: No se cumple.

No se realiza gestión de los cambios que ocurren en la infraestructura de red.

Hallazgo	No existe gestión de cambios.
Objetivo	
Garantizar la seguridad de la información de la institución.	
Recomendación	
Elaborar un plan de gestión de cambios.	
Riesgos a mitigar	
Perdida de información.	

Control: Gestión de capacidades

Informe: Se cumple.

Los recursos informáticos actuales ofrecen condiciones para operar de manera óptima a largo plazo.

Hallazgo	No se monitorea las proyecciones de los requisitos de capacidad futuros.
Objetivo	
Proyectar y garantizar que los recursos informáticos operen de manera óptima en el futuro.	
Recomendación	
Implementar normativas de gestión de capacidades [5]ITIL.	
Riesgos a mitigar	
Pérdida en la calidad de servicios. Colapso de la red. Perdida de información. Saturación de los medio de transmisión.	

[5] **ITIL:** La Gestión de la Capacidad es la encargada de que todos los servicios TI se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada. Ver más en información: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_capacidad/vision_general_gestion_de_la_capacidad/vision_general_gestion_de_la_capacidad.php

Objetivo de control: Protección contra código malicioso.

Control: Controles contra código malicioso.

Informe: Se cumple parcialmente.

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

Hallazgo	Existen maquinas sin licencias de antivirus.
Objetivo	
Garantizar la protección de la información contra código malicioso.	
Recomendación	
Adquirir licencias de [6]ESET NOD32 Antivirus.	
Riesgos a mitigar	
Código malicioso (gusanos, troyanos, malware)	

Objetivo de control: Copias de seguridad.

Control: Copias de seguridad de la información.

Informe: Se cumple parcialmente.

Solo se llevan a cabo copias de seguridad del sistema contable, no se tiene acceso al servidor de red para realizar copias de seguridad.

Hallazgo	No existen copias de seguridad del servidor de red.
Objetivo	
Garantizar la continuidad y protección de la información.	
Recomendación	
Implementar copias de seguridad del servidor de red.	
Riesgos a mitigar	
Perdida de la información.	

[6] **ESET NOD32 Antivirus:** te ofrece una protección rápida, efectiva y sencilla de utilizar sin entorpecer tus tareas cotidianas y sin afectar el rendimiento de tu equipo. La galardonada tecnología de detección proactiva de ESET detecta la mayoría de las amenazas conocidas y desconocidas que circulan por la red. Ver más información en: http://www.eset.com.ni/hogar/nod32-antivirus.html

Objetivo de control: Registros de actividad y supervisión.

Control: Registro y gestión de eventos de actividad.

Informe: No se cumple.

No se realiza monitoreo de los eventos de seguridad.

Hallazgo	No existe monitoreo y no se registran los eventos de la seguridad.
Objetivo	
Garantizar la seguridad de los sistemas y activos informáticos.	
Recomendación	
Aplicar soluciones [7]SIEM (Security Information Event Management).	
Riesgos a mitigar	
Perdida de la información.	

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 a los sistemas de información y red.
Objetivo	
Minimizar las interrupciones de los procesos informáticos.	
Recomendación	
Planificar y establecer controles de auditoria a los sistemas de información y red.	
Riesgos a mitigar	
Interrupciones de procesos informáticos claves.	

[7] **SIEM (Security Information Event Management):** recogen, analizan y priorizan los eventos de seguridad dentro de su red. Existen varios tipos de soluciones, desde los colectores de logs hasta las soluciones más completas, que ayudan a implantar SIEM de acuerdo con las "mejores prácticas" en cumplimiento de las normativas y estándares de seguridad más exigentes. Ver más información en: http://www.ireo.com/soluciones/seguridad-perimetral/gestion-de-eventos-siem/

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 monitoreo de red.

Hallazgo	No se implementan controles de red.
Objetivo	
Garantizar la seguridad y el correcto uso de la red.	
Recomendación	
Implementar la herramienta de monitoreo de red [8]Forefront TMG.	
Riesgos a mitigar	
Intrusión. Malware.	

Control: Mecanismos de seguridad asociados a servicios de red.

Informe: Se cumple parcialmente.

Se implementa el uso de proxy SQUID como mecanismo de seguridad asociados a los servicios de red.

Hallazgo	No están definidos los mecanismos de seguridad asociados a servicios de red.
Objetivo	
Garantizar la seguridad de los servicios de red.	
Recomendación	
Planificar y establecer mecanismos de seguridad asociados a servicios de red.	
Riesgos a mitigar	
Perdida de información. Perdida en la calidad de los servicios.	

[8] **Forefront TMG:** es una solución completa de puerta de enlace web segura que ayuda a proteger empleados de las amenazas basadas en web. Forefront TMG también ofrece seguridad perimetral simple y unificada con firewall integrado, VPN, prevención de intrusiones, inspección de malware y filtrado de URL. Ver más información en: https://technet.microsoft.com/es-ni/library/ff355324.aspx

Control: Segregación de redes.

Informe: No se cumple.

No se implementa redes de área local virtuales (VLAN).

Hallazgo	No se han implementado dispositivos intermediarios (SWITCH) de capa 3 administrables.
Objetivo	
Garantizar la segmentación de la red virtualmente.	
Recomendación	
Adquirir e implementar dispositivos intermediarios administrables de capa 3, switches [9]Cisco Catalyst 3550 Series.	
Riesgos a mitigar	
Acceso no autorizado a información sensible. Intrusión.	

Hallazgo	No se han implementado VLANs.
Objetivo	
Garantizar la seguridad de la información.	
Recomendación	
Definir e implementar VLANs de acuerdo a las necesidades de la institución.	
Riesgos a mitigar	
Acceso no autorizado a información sensible. Intrusión.	

[9] **Cisco Catalyst 3550 Series:** traducido : "los switches Ethernet inteligentes es una línea de switches multicapa de gran alcance, de configuración fija que se extienden hasta el borde de inteligencia acceso al metro, lo que permite amplitud de servicios, disponibilidad, seguridad y facilidad de administración" Ver más información en:
http://www.cisco.com/en/US/products/hw/switches/ps646/products_data_sheet09186a00800913d0.html

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 entidades externas.

Hallazgo	No se definen políticas y procedimiento de intercambio.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se deberían definir políticas y procedimientos de intercambio, en caso de que sea necesario intercambiar información con entidades externas.	
Riesgos a mitigar	
Uso indebido de la información. Daño a la seguridad, integridad y confiabilidad de la información.	

Control: Acuerdos de intercambios.

Informe: No se cumple.

No existen acuerdos de intercambio.

Hallazgo	No se definen acuerdos de intercambio.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se deberían definir acuerdos de intercambio, en caso de que sea necesario intercambiar información con entidades externas.	
Riesgos a mitigar	
Uso indebido de la información. Daño a la seguridad, integridad y confiabilidad de la información.	

Control: Mensajería electrónica.

Informe: No se cumple.

No existe seguridad ligada a la mensajería electrónica.

Hallazgo	No se implementas mecanismo de seguridad al uso de correo electrónico.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información que se transmite mediante la mensajería electrónica.	
Recomendación	
Implementar mecanismos de [10]cifrado corporativo.	
Riesgos a mitigar	
Uso indebido de la información. Daño a la seguridad, integridad y confiabilidad de la información.	

Control: Acuerdos de confidencialidad y secreto.

Informe: No se cumple.

No existen acuerdos de confidencialidad y secreto.

Hallazgo	No se definen acuerdos de confidencialidad y secreto.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se deberían definir e implementar acuerdos de confidencialidad y secreto.	
Riesgos a mitigar	
Uso indebido de la información. Daño a la seguridad, integridad y confiabilidad de la información.	

[10] **Cifrado corporativo:** Cifrar o encriptar datos significa alterarlos, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original. Ver más información en: http://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

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 supervisan los servicios prestados por terceros.

Hallazgo	No existe supervisión y revisión de servicios prestados por terceros.
Objetivo	
Garantizar el cumplimiento de los servicios prestados por terceros.	
Recomendación	
Se deben supervisar y revisar de manera rigurosa y periódicamente el cumplimiento de los servicios prestados por terceros.	
Riesgos a mitigar	
Mala calidad en los servicios informáticos.	

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 se gestionan los incidentes de seguridad.

Hallazgo	No existen procedimientos de manejo y gestión de incidente de la información.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se deben definir e implementar procedimientos de gestión de los incidentes de la información para establecer mejoras en la seguridad.	
Riesgos a mitigar	
Uso indebido de la información. Daño a la seguridad, integridad y confiabilidad de la información.	

Control: Notificación de eventos de seguridad de la información.

Informe: Se cumple parcialmente.

Se notifica a la administración los eventos más relevantes relacionados a la seguridad de la información.

Hallazgo	No existen canales de administración adecuados.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se deben definir canales de administración adecuados para informar de manera pertinente los eventos de seguridad de la información.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información.	

Control: Notificación de puntos débiles de la seguridad.

Informe: No se cumple.

No se documentan e informan los puntos débiles de la seguridad.

Hallazgo	No se gestionan e informan los puntos débiles de seguridad.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se debe gestionar cualquier sospecha de debilidad en la seguridad de la información y ser informados a los superiores.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información.	

Control: Valoración de eventos de seguridad de la información y toma de decisiones.

Informe: No se cumple.

No se gestionan los eventos de seguridad.

Hallazgo	No se evalúan ni clasifican los eventos los incidentes de seguridad.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Gestionar los eventos de seguridad y clasificarlos según su magnitud, con el fin de poder tomar decisiones acertadas acerca de cómo mitigar los incidentes.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información.	

Control: Aprendizaje de los incidentes de la seguridad de la información.

Informe: No se cumple.

No se analizan y documentan los incidentes de la seguridad de la información.

Hallazgo	No existe aprendizaje porque no se gestionan los incidentes de seguridad.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se gestionar los clasificar y documentar los incidentes de seguridad de la información.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Materialización de reincidencias.	

Control: Recopilación de evidencias

Informe: No se cumple.

No se definen ni aplican procedimientos para recopilar evidencias.

Hallazgo	No se identifica y documentan evidencias.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se deben definir y aplicar procedimientos que permitan identificar y recopilar evidencias de los incidentes de seguridad.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información. Discontinuidad de la información en los procesos informáticos.	

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: Planificación de la continuidad de la seguridad de la información.

Informe: No se cumple.

No se ha definido un plan de continuidad y recuperación.

Hallazgo	No existe un plan de continuidad de seguridad.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Elaborar el plan de continuidad de seguridad de la información, en caso de que se presenten situaciones crisis o desastres.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información.	

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

Informe: No se cumple.

No se implementa plan de continuidad de seguridad.

Hallazgo	No existe definido e implementado un plan de continuidad de la seguridad.
Objetivo	
Garantizar la seguridad, integridad y confiabilidad de la información.	
Recomendación	
Se debe establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información.	

Objetivo de control: Redundancias.

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

Informe: No se cumple.

No se implementa una arquitectura redundante.

Hallazgo	No existen componentes redundantes.
Objetivo	
Garantizar la disponibilidad de la información.	
Recomendación	
Implementar componentes que permitan la redundancia, para asegurar la disponibilidad de la información.	
Riesgos a mitigar	
Pérdida de información.	

Dominio: Cumplimiento.

Objetivo de control: Cumplimiento de los requisitos legales y contractuales.

Control: Identificación de la legislación aplicable

Informe: No se cumple.

No se han definido los requisitos legales y contractuales.

Hallazgo	No se han definido los requisitos de operación, uso y gestión de los recursos informáticos.
Objetivo	
Garantizar el cumplimiento de requisitos legales y contractuales.	
Recomendación	
Se deben establecer e implementar los requisitos estatuarios, reguladores y de seguridad contractuales.	
Riesgos a mitigar	
Incumplimiento legal.	

Control: Derechos de propiedad intelectual (DPI).

Informe: No se cumple.

No se implementan procedimientos para garantizar el cumplimiento de los requisitos, normativos y contractuales de los derechos de propiedad intelectual.

Hallazgo	No existen procedimientos aplicados para asegurar el cumplimiento de los derechos de propiedad intelectual.
Objetivo	
Garantizar el cumplimiento de requisitos, normativos y contractuales.	
Recomendación	
Se deben implementar procedimientos que garanticen el cumplimiento de los derechos de propiedad intelectual y utilizar software original.	
Riesgos a mitigar	
Violación a derechos de propiedad intelectual. Incumplimiento legal.	

Control: Protección de los registros de la organización.

Informe: No se cumple.

No se implementan mecanismo de seguridad que protejan adecuadamente los registros de información de la institución, bajo requisitos legislativos, normativos y contractuales.

Hallazgo	No están definidos los requisitos legislativos, normativos y contractuales que protejan los registros de información.
Objetivo	
Garantizar el cumplimiento de requisitos, normativos y contractuales.	
Recomendación	
Se deben definir los requisitos legislativos, normativos y contractuales, que permitan proteger los registros de información.	
Riesgos a mitigar	
Incumplimiento legal. Pérdidas, destrucción y falsificación de la información. Publicación no autorizada de los registros de información.	

Control: Protección de los datos y privacidad de la información personal.

Informe: No se cumple.

No existen normativas legales de protección de datos y privacidad

Hallazgo	No se implementan normativas de protección de datos y privacidad.
Objetivo	
Garantizar la protección de los datos y protección de la información personal.	
Recomendación	
Se deben implementar y definir normativas que garanticen el cumplimiento la protección de los datos y privacidad de la información personal.	
Riesgos a mitigar	
Violación a la privacidad de la información personal. Acceso no autorizado a la información.	

Control: Regulación de los controles criptográficos.

Informe: No se cumple.

No se implementan controles criptográficos.

Hallazgo	No se cifra la información que viaja por la red.
Objetivo	
Garantizar la seguridad, integridad y confidencialidad de la información.	
Recomendación	
Se deben implementar mecanismos de encriptamiento a la información que viaja por la red.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información.	

Objetivo de control: Revisión de la seguridad de la información.

Control: Revisión independiente de la seguridad de la información.

Informe: No se cumple.

No se revisa el enfoque organizacional de la institución para la implementación de controles, políticas, procesos y procedimientos para la seguridad de la información

Hallazgo	No se gestiona la seguridad de la información en base el enfoque organizacional.
Objetivo	
Garantizar la seguridad, integridad y confidencialidad de la información.	
Recomendación	
Implementar objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información acorde al enfoque organizacional.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información.	

Control: Cumplimiento de las políticas y normas de seguridad.

Informe: No se cumple.

No se revisa el cumplimiento de los procedimientos de información respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente, porque estas no están definidas.

Hallazgo	No se revisan el cumplimiento de políticas y normas de seguridad de la información.
Objetivo	
Garantizar la seguridad, integridad y confidencialidad de la información.	
Recomendación	
Se deben definir y establecer parámetro de revisión regular del cumplimiento las políticas y normas de seguridad.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Pérdida de información.	

Control: Comprobación de cumplimiento.

Informe: No se cumple.

No se verifica el cumplimiento de políticas y normas de seguridad dispuestas por la institución.

Hallazgo	No se revisa regularmente los que los recursos informáticos cumplan con las políticas y normas de seguridad.
Objetivo	
Garantizar la seguridad, integridad y confidencialidad de la información y los recursos informáticos.	
Recomendación	
Verificar regularmente que los recursos informáticos cumplan las políticas y normas de seguridad dispuestas por la institución.	
Riesgos a mitigar	
Daño a la seguridad, integridad y confiabilidad de la información. Incumplimiento legal.	

OTROS HALLAZGOS

Hallazgo	No hay acceso a la configuración del servidor de red.
Objetivo	
Garantizar la administración adecuada de los recursos informáticos.	
Recomendación	
Implementar el sistema operativo servidor [11]Windows Server 2012 R2.	
Riesgos a mitigar	
Pérdida de la continuidad de los servicios de red.	

Hallazgo	No se administra y delimita el uso del ancho de banda.
Objetivo	
Garantizar la calidad de la conectividad a internet.	
Recomendación	
Implementar la herramienta delimitadora de ancho de banda de [12]Forefront TMG.	
Riesgos a mitigar	
Pérdida en la calidad de los servicios de red.	

[11] **Windows Server 2012 R2:** ocupa un lugar central en la estrategia de Microsoft Cloud Platform, aporta la experiencia de Microsoft al dotar su infraestructura de servicios en la nube de escala global, gracias a las nuevas características y mejoras en virtualización, administración, almacenamiento, redes, infraestructura de escritorio virtual, protección de la información y del acceso, plataforma de aplicaciones y web, etc. Ver más información en: https://www.microsoft.com/es-xl/server-cloud/products/windows-server-2012-r2/overview.aspx

[12] **Forefront TMG:** es una solución completa de puerta de enlace web segura que ayuda a proteger empleados de las amenazas basadas en web. Forefront TMG también ofrece seguridad perimetral simple y unificada con firewall integrado, VPN, prevención de intrusiones, inspección de malware y filtrado de URL.
Ver más información en: https://technet.microsoft.com/es-ni/library/ff355324.aspx

PROBLEMÁTICAS RELEVANTES ENCONTRADAS

Detalle de las problemáticas encontradas

Alcaldía Municipal de San Ramón, Matagalpa

Área de informática

Problemática	Causa	Recomendación	Problemática	Causa	Recomendación
1. No se han implementados políticas de seguridad.	No existe conocimiento acerca de la importancia de aplicar políticas de seguridad físicas y lógicas.	Definir las metodologías de seguridad, con sus respectivos procesos y políticas destinadas a la protección de la información.	2. No se aplican controles y procedimientos a la protección de los medios de almacenamiento.	No se ha definido controles que permitan asegurar la protección de los medios de almacenamiento.	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 existe conciencia acerca de la importancia del papel que juega el área de TI dentro de la institución.	Concientizar a la gerencia y definir e implementar el área de TI con dominio de la gerencia.	4. No existen políticas de control de acceso.	No se ha definido e implementado las políticas para el control de acceso a la información.	Definir e implementar políticas de control de acceso.
5. No hay capacitación asociada a las tecnologías de la información.	La directora de informática recibe capacitaciones, pero estas no se enfocan en la seguridad, mantenimiento y administración de las tecnologías de la información.	Promover las capacitaciones sobre la seguridad, mantenimiento y administración de las tecnologías de la información.	6. No existen controles de acceso a la red.	No se han definido e implementado controles de acceso a red, desde las diferentes áreas de la institución.	Definir, documentar e implementar controles de acceso a la red
7. Se realiza el inventario de los activos informáticos de manera muy superficial.	No existe definido un formato de inventario que permita detallar los activos informáticos.	Elaborar un formato de inventario detallado.	8. Los dispositivos de red que están fuera del área de informática están desprotegidos.	No están centralizados los dispositivos de red en el área de informática.	Centralizar la infraestructura de red. Implementar políticas de seguridad a los dispositivos fuera del área de informática.

9. No se han definido controles físicos de entrada.	No existen políticas de controles físicos de entrada.	Implementar controles físicos de entrada, como: uso de credenciales, registros de firmas de entrada y salida, cámaras de seguridad, alarmas antirrobo.	10. No existe la implementación de controles criptográficos.	No existe el conocimiento ni la conciencia de la importancia de la implementación de encriptamiento a la información.	Definir y establecer políticas de uso y procedimientos de control de encriptamiento de la información.
11. No se aplica protección contra ataques maliciosos o accidentes al 50 % de los activos informáticos.	Existen activos fuera del área del de informática y estos se encuentran desprotegidos y propensos a ataque malintencionados.	Implementar mecanismos de protección a los activos informáticos.	12. No existe seguridad ligada a la mensajería electrónica	No se implementas mecanismo de seguridad al uso de correo electrónico.	Implementar mecanismos de cifrado corporativo.
13. El cableado no se encuentra estructurado.	No se implementaron estándares de estructuración al cableado.	Aplicar estándares ANSI/TIA/EIA-568-B	14. No se supervisan los servicios prestados por terceros.	No existe supervisión y revisión de servicios prestados por terceros.	Se deben supervisar y revisar de manera rigurosa y periódicamente el cumplimiento de los servicios prestados por terceros.
15. No existe un plan de mantenimiento definido.	No se ha definido un plan de mantenimiento.	Definir y documentar un plan de mantenimiento detallado.	16. No se gestionan los incidentes de seguridad.	No existen procedimientos de manejo y gestión de incidente de la información.	Se deben definir e implementar procedimientos de gestión de los incidentes de la información para establecer mejoras en la seguridad.

17. No se realiza documentación de los procedimientos de operación de los dispositivos informáticos	No existen procedimientos de operación documentados de los dispositivos informáticos.	Definir y documentar los procedimientos de operación de los dispositivos informáticos.	18. No se documentan e informan los puntos débiles de la seguridad.	No se gestionan e informan los puntos débiles de seguridad.	Se debe gestionar cualquier sospecha de debilidad en la seguridad de la información y ser informados a los superiores.
19. Existen maquinas sin licencias de antivirus.	No sea adquirido licencias de antivirus para todas las computadoras.	Adquirir licencias de ESET NOD32 Antivirus.	20. No se gestionan los eventos de seguridad.	No se evalúan ni clasifican los eventos los 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.
21. No existe monitoreo y no se registran los eventos de la seguridad.	No se han implementado herramientas de monitoreo.	Aplicar soluciones SIEM (Security Information Event Management).	22. 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 crisis o desastres.
23. No se realizan auditorías a los sistemas de información y red.	No existen controles de auditoria.	Planificar y establecer controles de auditoria a los sistemas de información y red.	24. No existen procedimientos aplicados para asegurar el cumplimiento de los derechos de propiedad intelectual	No se implementan procedimientos para garantizar el cumplimiento de los requisitos, normativos y contractuales de los derechos de propiedad intelectual.	Se deben implementar procedimientos que garanticen el cumplimiento de los derechos de propiedad intelectual y utilizar software original.

25. No existe monitoreo de red.	No se implementan controles de red.	Implementar la herramienta de monitoreo de red Forefront TMG.	26. No se revisan el cumplimiento de políticas y normas de seguridad de la información.	No se revisa el cumplimiento de los procedimientos de información respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente, porque estas no están definidas.	Se deben definir y establecer parámetro de revisión regular del cumplimiento las políticas y normas de seguridad.
27. No se implementa redes de área local virtuales (VLAN).	No se han implementado dispositivos intermediarios (SWITCH) de capa 3 administrables.	Adquirir e implementar dispositivos intermediarios administrables de capa 3, switches Cisco Catalyst 3550 Series. Definir e implementar VLANs de acuerdo a las necesidades de la institución.	28. No hay acceso a la configuración del servidor de red.	No existe documentación de las credenciales de acceso al servidor de red.	Implementar el sistema operativo servidor Windows Server 2012 R2.
29. No se administra y delimita el uso del ancho de banda.	No se implementan herramientas de administración de ancho de banda.	Implementar la herramienta delimitadora de ancho de banda de Forefront TMG.			

Evaluadores

Br. Eli Josué Castillo M

Br. Norman Antonio Tercero M

Aprobado

Alcaldía Municipal de San Ramón, Matagalpa

CONCLUSIONES

ISO/IEC 27002:2013, es una guía de buenas prácticas para la seguridad de la información, proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

El diagnostico permitió conocer el porcentaje nivel de cumplimiento de la institución: políticas de seguridad 0%, aspectos organizativos de la seguridad de la información 0%, seguridad ligada al recurso humano 15%, gestión de activos 16.7%, control de acceso 23.3%, cifrado 0%, seguridad física y ambiental 31.7%, seguridad operativa 27.1%, seguridad en las telecomunicaciones 4.3%, relaciones con suministradores 0%, gestión de incidentes en la seguridad de la información 5%, aspectos de seguridad de la información en la gestión de la continuidad del negocio 0% y cumplimiento 0%, lo que demuestra la deficiencia de la infraestructura de red y de la seguridad de la información.

Se realizaron las tablas de hallazgo y recomendaciones de cada control de los dominios contemplados para la evaluación, donde se refleja cada problemática , el informe de cumplimiento y la sugerencia para garantizar buenas prácticas para la seguridad de la información e infraestructura de red.

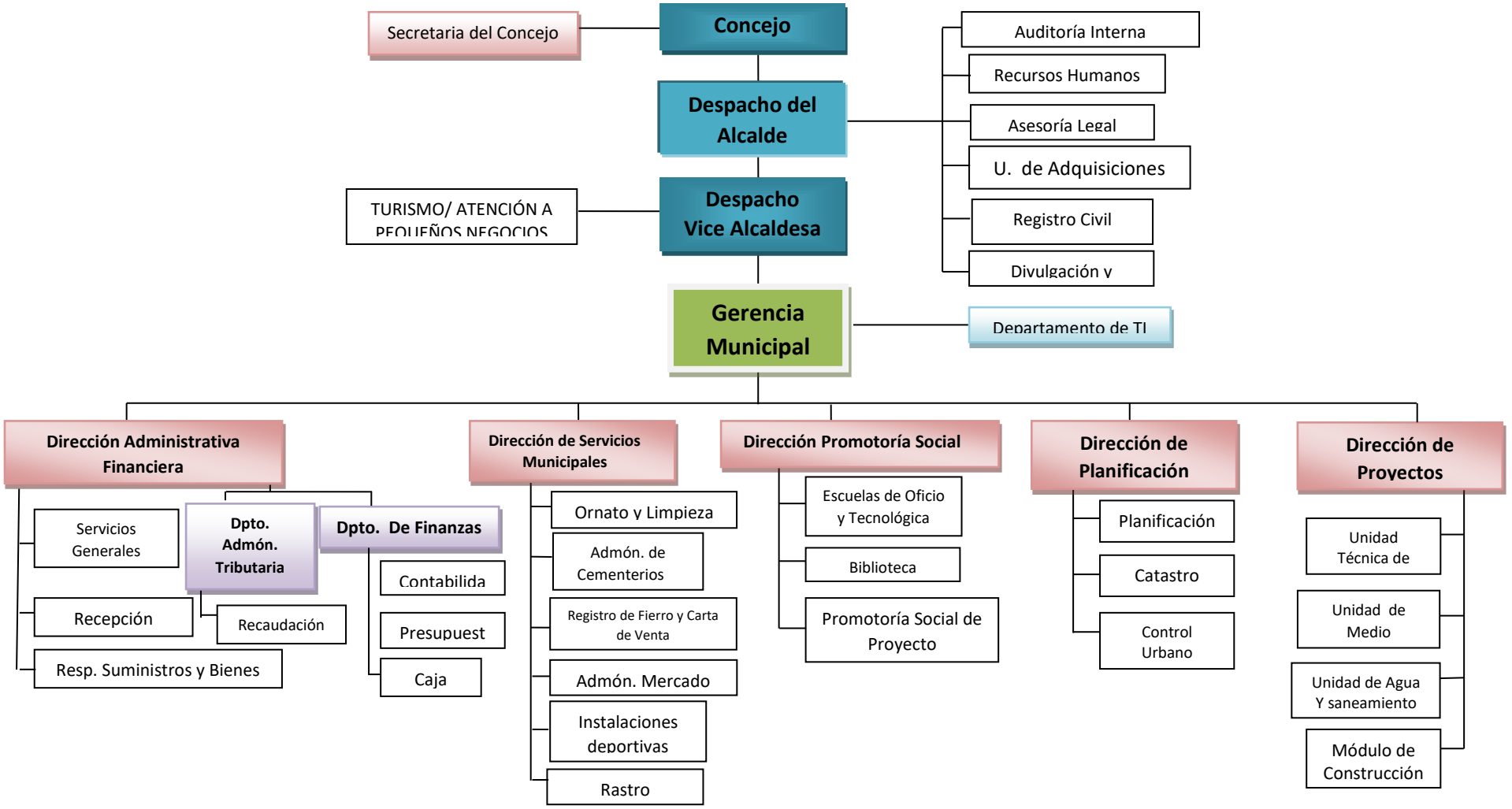
También se elaboró la tabla de problemáticas más relevantes encontradas, para dar a conocer cuáles son los puntos más importantes a tratar y priorizar las mejoras pertinentes, de esta manera garantizar la seguridad de la información en la institución. El beneficio de esta guía es ayuda a la institución a aplicar buenas prácticas en la seguridad de la información, para garantizar una infraestructura de red más robusta.

Se estimó el costo de la evaluación en base a la media de costo por horas (media $50) por la cantidad de horas empleadas (130 horas), lo cual refleja un costo total de evaluación de $6,500.00 (seis mil quinientos dólares netos).

ANEXOS DE GUÍA DE MEJORAS

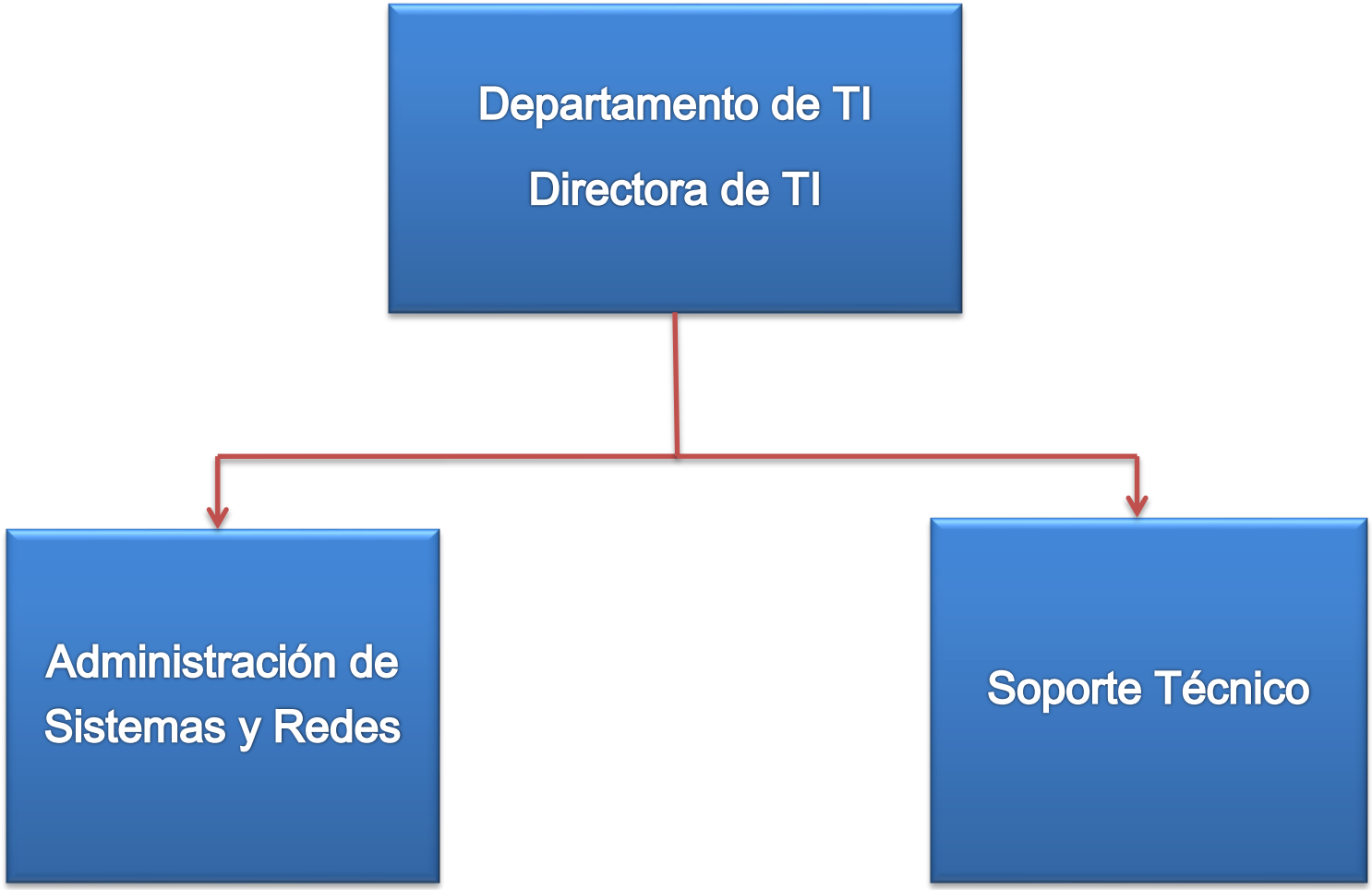
Anexo No 1.1

Organigrama propuesto



Anexo No 1.2

Estructura propuesta del departamento de TI



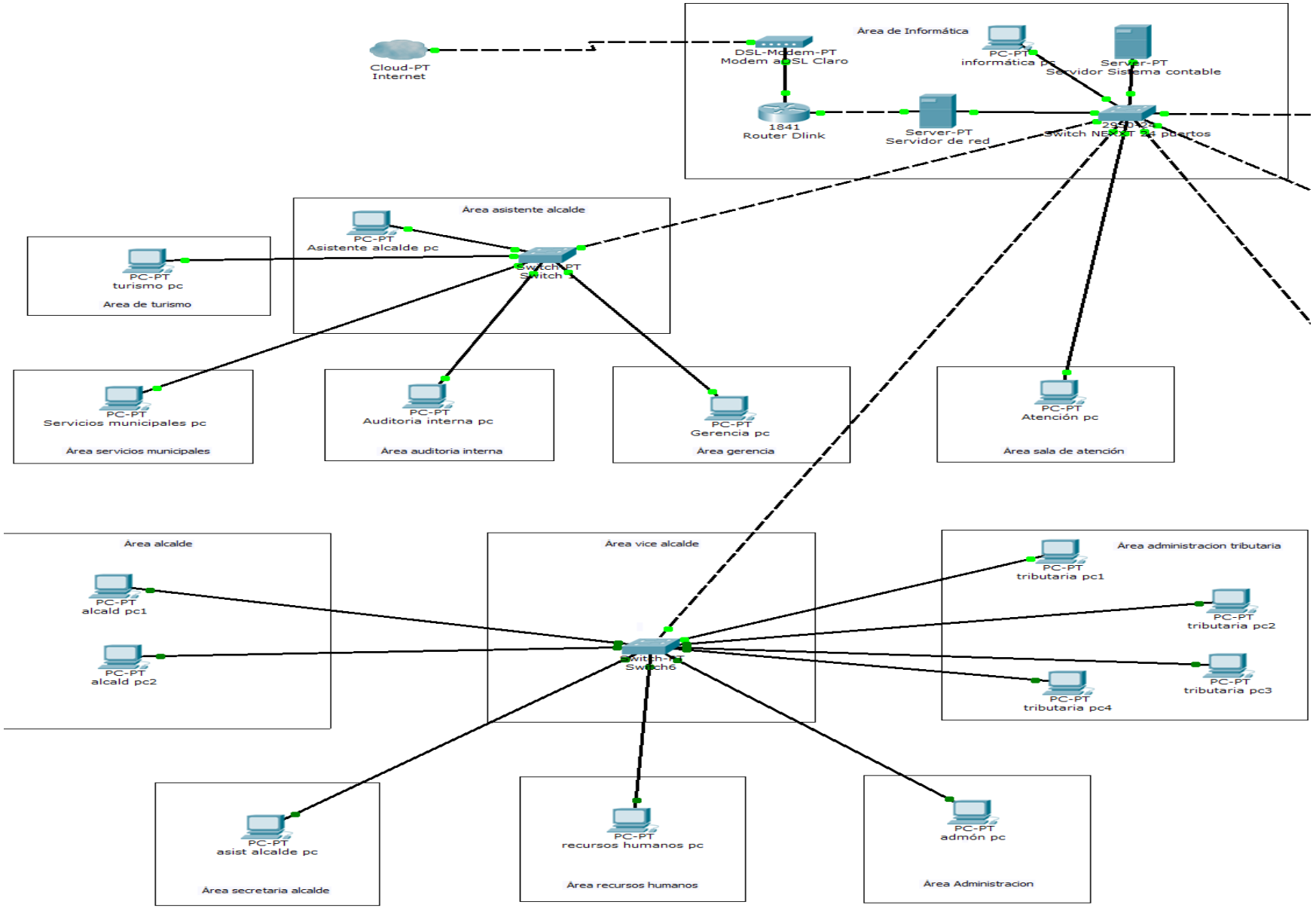
Anexo No 1.3

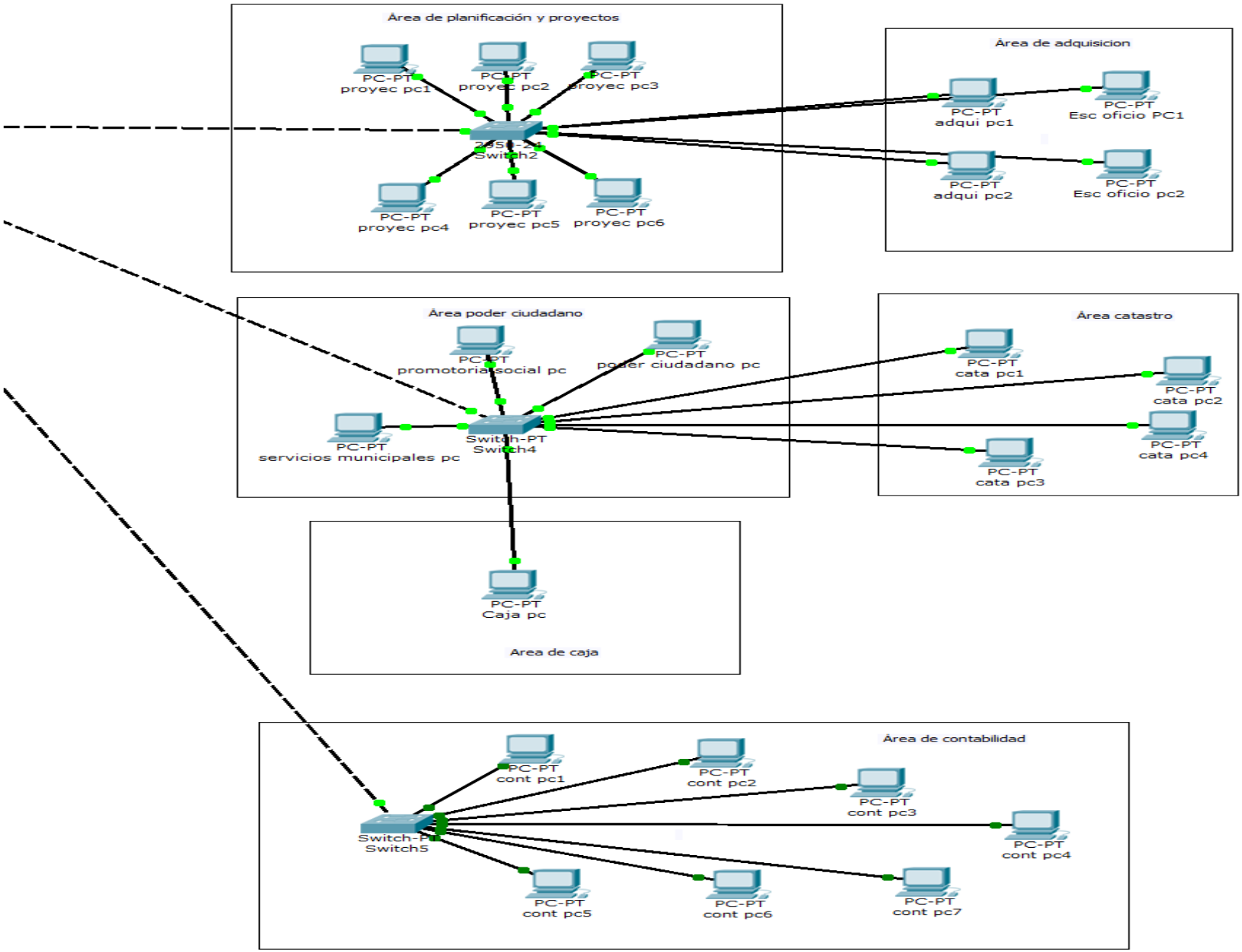
Funciones de la estructura propuesta del departamento de TI

Cargo	Perfil	Funciones
Directora de TI	**Licenciado en computación Ingeniero en sistemas o computación**	**1. Planear, dirigir y controlar las estrategias de TI.** **2. Coordinar la ejecución de los planes de desarrollos tecnológicos.** **3. Coordinar planes de capacitación orientadas al mejoramiento de las capacidades del personal de TI.** **4. Gestión y soporte de las TIC.** **5. Gestión de las políticas y normas de seguridad de la información.** **6. Elaboración del presupuesto anual de TI.** **7. Elaboración de inventarios de los recursos informáticos.** **8. Mantener informada a la gerencia sobre el estado de los procesos desarrollados con TI.**
Administración de sistemas y redes	**Licenciado en computación / Preferible CCNA Ingeniero en sistemas o computación / Preferible CCNA**	**1. Administración, soporte y mantenimiento a los sistemas informáticos.** **2. Administración, soporte y mantenimiento de la infraestructura de red.** **3. Administración de usuarios.** **4. Realizar copias de seguridad de los sistemas informáticos** **5. Monitoreo de red y sistemas.**
Soporte técnico	**Licenciado o ingeniero en sistemas o computación / Preferible Ingeniero o técnico electrónico**	**1. Soporte técnico de los servicios informáticos a usuarios.** **2. Desarrollo de planes de mantenimiento.** **3. Mantenimiento correctivo y preventivo de equipos informáticos.** **4. Instalación y mantenimiento de software.** **5. Control de inventario de hardware y software.**

Anexo No 1.4

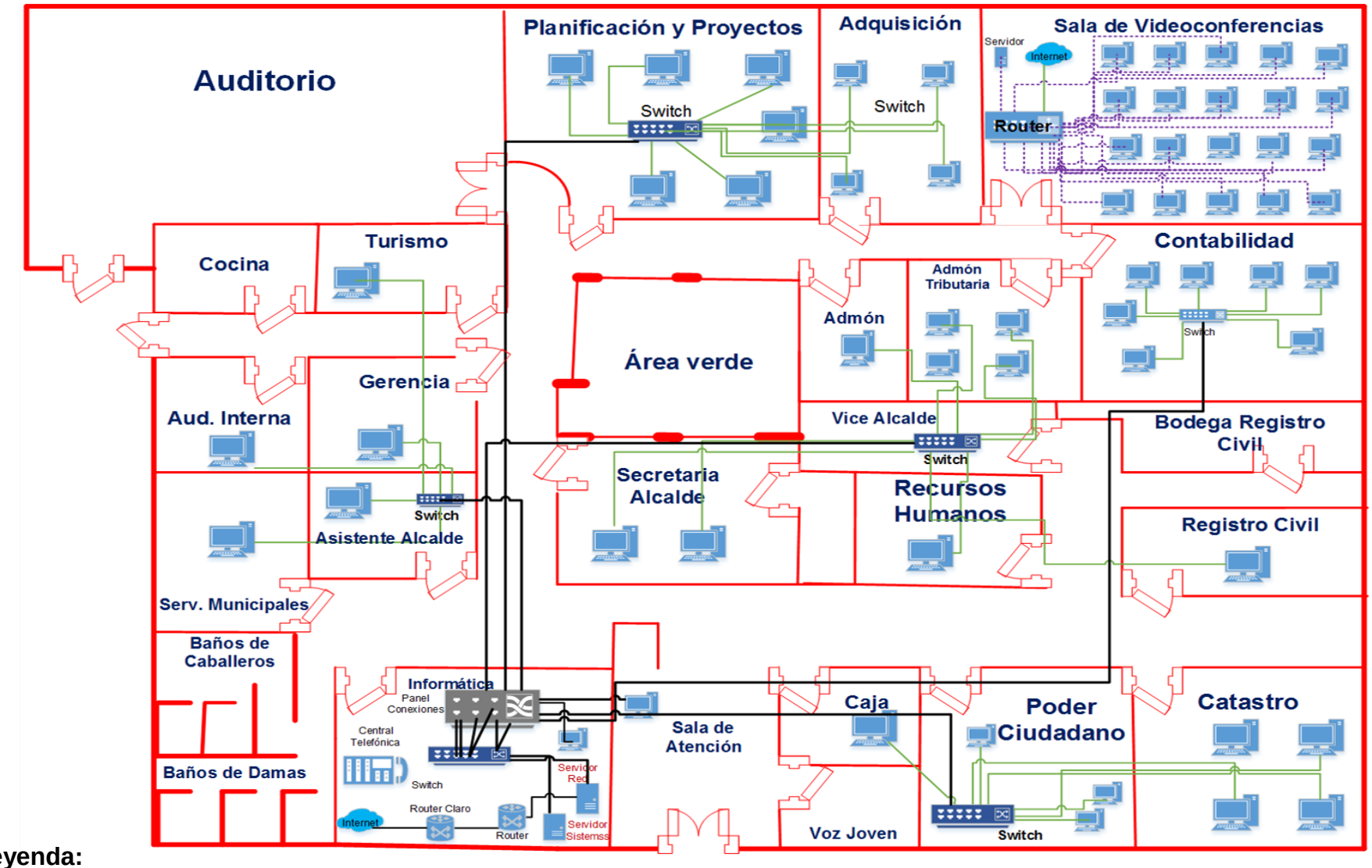
Topología lógica propuesta red principal




Área de planificación y proyectos
PC-PT proyec pc1
PC-PT proyec pc2
PC-PT proyec pc3
2950-24 Switch2
PC-PT proyec pc4
PC-PT proyec pc5
PC-PT proyec pc6
Área de adquisicion
PC-PT adqui pc1
PC-PT Esc oficio PC1
PC-PT adqui pc2
PC-PT Esc oficio pc2
Área poder ciudadano
PC-PT promotoria social pc
PC-PT poder ciudadano pc
PC-PT servicios municipales pc
Switch-PT Switch4
Área catastro
PC-PT cata pc1
PC-PT cata pc2
PC-PT cata pc3
PC-PT cata pc4
PC-PT Caja pc
Area de caja
Área de contabilidad
PC-PT cont pc1
PC-PT cont pc2
PC-PT cont pc3
PC-PT cont pc4
Switch-PT Switch5
PC-PT cont pc5
PC-PT cont pc6
PC-PT cont pc7

Anexo No 1.5

Topología física propuesta de la red principal



Leyenda:

- ✓ Conexión inalámbrica
- ✓ Conexión cableada

Anexo 2

Operacionalización de Variables

Variables	Concepto	Sub variable	Indicadores	Preguntas	Informante	Técnicas
Infraestructura de red LAN	Una evaluación de la infraestructura de red es el proceso por el cual se explora la red para identificar riesgos, asumirlos y minimizarlos mediante técnicas y protocolos de seguridad.	Redes	• Definición	¿Usted conoce el término red de computadores? Sí_ No_ ¿Usted comprende cuales son los objetivos de la implementación de redes de computadores? Sí_ No_	Directora Informática	Entrevista
			• Arquitectura de red	¿La tecnología de red empleada es capaz de soportar de manera rápida y eficiente los servicios que se brindan a través de esta? Sí_ No_ ¿La conexión a internet está disponible 24/7? Sí_ No_ ¿Existe un proveedor secundario de servicio de internet, en caso que el principal falle? Sí_ No_ ¿La tecnología implementada en capaz de admitir a nuevos dispositivos y usuarios en la red? Sí_ No_ ¿Se priorizan servicios en la red, tales como streaming, voIp, etc? Sí_ No_ ¿Se han implementado protocolos de seguridad en la red? Sí_ No_	Directora Informática	Entrevista

			• Tipos de redes	¿Qué tipo de red existe en la institución? a) LAN b) MAN c) WAN	Directora Informática	Entrevista Observación
			• Topología de red	¿Qué topología de red está implementada en la institución? a) Bus b) Estrella c) Anillo d) Malla e) Árbol f) Ninguna ¿Según su criterio, la topología de red actualmente implementada es la indicada para esta institución? Sí_ No_	Directora Informática	Entrevista Observación
			• Elementos de una red	¿Qué medio de trasmisión de datos se usa en la institución?	Directora Informática	Entrevista Observación
		Calidad de las comunicaciones	• Factores Externos	Según su criterio ¿la red posee todos los dispositivos necesarios para ofrecer un servicio de calidad?	Directora Informática	Entrevista
			• Factores Internos	¿Qué tipo de datos se transportan a través de la red? (Conexión a base de datos, sitios web, videos, voiP,etc)? ¿El tráfico de red es monitoreado? Sí_ No_ ¿Qué herramientas de software utiliza para monitorear la red?	Directora Informática	Entrevista Observación
		Infraestructura Física	• Dispositivos	¿Con que tipos y cantidad de dispositivos de red cuenta la institución?	Directora Informática	Entrevista Observación

			de Red	¿Los dispositivos de red que están implementados son de última generación? Sí_ No_ Para usted ¿Qué grado de dificultad presenta la administración de los dispositivos de red		
			• Cableados o Guiados	¿Qué tipo de cable y categoría utilizan las conexiones de red?	Directora Informática	Entrevista Observación
			• Medios de transmisión inalámbricos	¿Se hace uso de redes inalámbricas en la institución? Sí_ No_	Directora Informática	Entrevista Observación
			• Estación de trabajo	¿Todas las computadoras de la institución tienen acceso a la red? Sí_ No_ ¿Se realizan mantenimientos de manera continua a los ordenadores? Sí_ No_ ¿Se encuentran en buenas condiciones los ordenadores? Sí_ No_	Directora Informática	Entrevista
			• Políticas de seguridad Físicas	¿Existen políticas de seguridad 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	Directora Informática	Entrevista Observación

				información? Sí_ No_ ¿El personal de informática está en constante capacitación sobre las reglas y procedimientos establecidos sobre la seguridad física de la red? Sí_ No_		
			• Amenazas Físicas	Los equipos de red fuera del cuarto de informática, ¿se encuentran protegidos? Sí_ No_ Si la respuesta es sí, ¿De qué manera? ¿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 y amenazas hacia la seguridad física de la infraestructura red? Sí_ No_ Si la respuesta es sí, ¿Cuáles son?	Directora Informática	Entrevista Observación

		Infraestructura Lógica	• Servidores	¿Qué sistemas operativo servidor utiliza?	Directora 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 ¿Posee direcciones IP públicas exclusivas para la red de la institución? Sí_ No_	Directora Informática	Entrevista Observación
			• Servicios de Red	¿Cuáles servicios de red se ofrecen?	Directora Informática	Entrevista
			• Segmentación de Red	¿Actualmente se implementan segmentación de red? Sí_ No_	Directora Informática	Entrevista
			• Ancho de Banda	¿Con cuanto ancho de banda cuenta la institución? Según su criterio ¿El ancho de banda contratado es suficiente para proporcionar una conexión óptima a los usuarios? ¿Por qué?	Directora Informática	Entrevista Observación
			• Firewall	¿La infraestructura de red lógica cuenta con firewall? Sí_ No_ ¿Se monitorean los eventos registrados por el firewall? Sí_ No_	Directora Informática	Entrevista
			• VPN	¿Actualmente se cuenta con redes virtuales privadas? Sí_ No_	Directora Informática	Entrevista

			• Centrales Telefónicas	¿Existe una central telefónica? Sí _ No_ ¿Se cuenta con la suficiente cantidad de terminales telefónicas para proveer el servicio a los usuarios? Sí_ No_	Directora Informática	Entrevista Observación
			• Políticas de seguridad Lógica	¿Están establecidas políticas de seguridad lógica en la red? Si la respuesta es sí, ¿Cuáles son?	Directora Informática	Entrevista
			• Amenazas Lógicas	¿La institución cuenta con los mecanismos necesarios para prevenir los riesgos lógicos? (Acl, Firewalls, antivirus) Sí_ No_ Si la respuesta es sí, ¿Cuáles son estos mecanismos?	Directora Informática	Entrevista Observación
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?	Directora Informática	Entrevista
		Políticas de seguridad	• Conjunto de políticas	¿Están definidas las políticas de seguridad de la información en la red de la institución? Si su respuesta es sí, responda: ¿Existe la documentación de dichas políticas? ¿Estas políticas has sido	Directora Informática	Entrevista

				comunicada a los empleados de la institución?		
		Aspectos organizativos de la seguridad de la información	• Segregación de tareas	¿Está definida el área de TI? ¿Se han definido cuáles son sus tareas respecto a la seguridad de las redes, para minimizar el riesgo de un mal uso de los activos de la institución?	Directora Informática	Entrevista
		Seguridad ligada al recurso humano	• Antes de la contratación	Antes de su contratación como responsable del área informática, ¿se le dieron a conocer cuáles son los términos y condiciones del empleo?	Directora Informática	Entrevista
			• Investigación de antecedentes	¿La institución le solicito un documento legal en el que se reflejen sus antecedentes en otros empleos? ¿Qué tipo de documento se le solicito?	Directora Informática	Entrevista
			• Términos y Condiciones de contratación	En su contrato de empleo, ¿Cuáles son los términos, condiciones y obligaciones que este conlleva?	Directora Informática	Entrevista
			• Durante la contratación	¿La dirección se ha encargado de velar por el cumplimiento de la seguridad de las redes en el área de informática?	Directora Informática	Entrevista
			• Concienciación, educación y capacitación en seguridad de la información	¿La dirección le da a conocer cuáles son los cambios de las políticas y los procedimientos organizacionales que son relevantes a su área?	Directora Informática	Entrevista

		Gestión de activos	• Responsabilidades sobre los activos	¿Cuáles son sus responsabilidades en el mantenimiento de los controles adecuados sobre los activos, para conservar la seguridad de las redes?	Directora Informática	Entrevista
			• Inventario de activos	¿Lleva a cabo el inventario de activos del área de informática? ¿Cada cuánto tiempo realiza dicho inventario?	Directora Informática	Entrevista
			• Uso aceptable de los activos	¿Cuáles son los procedimientos para regular el uso adecuado de los activos del área de redes?	Directora Informática	Entrevista
			• Manejo de los soportes e almacenamiento	¿Cuáles son los controles y procedimientos que se aplican para proteger los medios de almacenamiento?	Directora Informática	Entrevista
		Control de acceso	• Requisitos de negocio para el control de acceso	¿Se controla el acceso a la información? ¿De qué manera?	Directora Informática	Entrevista
			• Política de control de accesos	¿Se encuentran establecidas las políticas de control de acceso en el área de redes? ¿Estas políticas están documentadas?	Directora Informática	Entrevista
			• Control de acceso a las redes y servicios asociados	¿Existe control de acceso de los usuarios, para verificar que estos utilizan los servicios de red que se le han autorizado? ¿De qué manera?	Directora Informática	Entrevista
			• Gestión de acceso de usuarios	¿Existen procedimientos formales que le permitan determinar, que parámetros tomar en cuenta al momento de asignar los permisos de acceso a la red, a los	Directora Informática	Entrevista

				usuarios? ¿Cuáles son?		
			• Gestión de altas/bajas registro de usuarios	¿Qué procedimientos formales se realizan, al momento de dar de alta o baja a un usuario de la red?	Directora Informática	Entrevista
			• Gestión de los derechos de acceso con privilegios especiales	¿Existen usuarios con privilegios especiales de acceso a la red? ¿Cuáles son estos privilegios?	Directora Informática	Entrevista
			• Control de acceso a sistemas y aplicaciones	¿Qué procedimientos de seguridad están implementados para evitar que los usuarios manipulen los sistemas, datos y dispositivos restringidos?	Directora Informática	Entrevista
			• Restricciones de acceso a la información	¿Qué mecanismos de seguridad están implementados para restringir el acceso a la información por parte de los usuarios no autorizados?	Directora Informática	Entrevista
			• Gestión de contraseñas de usuarios	¿De qué manera se gestionan las contraseñas de los usuarios? ¿Existen parámetros definidos para la asignación de contraseñas? ¿Cuáles son?	Directora Informática	Entrevista
		Cifrado	• Controles criptográficos	¿Implementa técnicas de encriptamiento a la información?	Directora Informática	Entrevista
			• Políticas de uso de controles criptográficos	¿Existen políticas de seguridad que regulen el uso de cifrado?	Directora Informática	Entrevista

			• Gestión de Claves	¿De qué manera administra las claves que permiten el cifrado y descifrado de la información?	Directora Informática	Entrevista
		Seguridad física y ambiental	• Áreas seguras	¿Los dispositivos de la red se encuentran en un área debidamente protegida ante el acceso no autorizado?	Directora Informática	Entrevista Observación
			• Controles físicos de entrada	¿Existen medidas de controles físicos aplicadas a las áreas donde se encuentran los dispositivos de red? ¿Cuáles son estos controles?	Directora Informática	Entrevista Observación
			• Seguridad de oficinas y recursos	¿Qué medidas de seguridad de acceso físico implementa en la oficina de informática y sala de video conferencia?	Directora Informática	Entrevista Observación
			• Protección contra amenazas externas y ambientales	¿Los dispositivos de red y servidores se encuentran en un lugar capaz de soportar desastres naturales y evitar incidentes malintencionados a la información?	Directora Informática	Entrevista Observación
			• Seguridad de los equipos	¿Los dispositivos de red y servidores están debidamente climatizados? ¿Están conectados a fuente de energía de respaldo? ¿Los dispositivos de red intermediarios como Switchs se encuentran ubicados en un rack, el cual evite la manipulación no autorizada de estos?	Directora Informática	Entrevista Observación
			• Seguridad del cableado	¿Los cables de red están canaleteados? ¿Se encuentran debidamente colocados para evitar la manipulación no autorizada de estos?	Directora Informática	Entrevista Observación

			• Mantenimiento de los equipos	¿Qué tipo de mantenimiento se les suministra a los dispositivos de red y servidores? (Preventivos y correctivos) ¿Cada cuánto tiempo se llevan a cabo dichos mantenimientos?	Directora Informática	Entrevista
			• Seguridad de activos y equipos fuera de las instalaciones	¿Existen dispositivos de red fuera de las instalaciones de la institución y que estos se encuentren a cargo de esta?	Directora Informática	Entrevista
		Seguridad operativa	• Documentación de procedimientos de operación	¿Existe documentación de los procedimientos de operación de los recursos de red?	Directora Informática	Entrevista
			• Gestión de cambios	¿Se controlan los cambios afectan en la infraestructura de red que afectan la seguridad de la información?	Directora Informática	Entrevista
			• Gestión de capacidades	¿Los recursos actualmente implementados, ofrecen las condiciones necesarias para operar de manera óptima en un futuro?	Directora de informática	Entrevista
			• Protección contra código malicioso	¿Actualiza de manera continua el antivirus y antimalware en todos los ordenadores?	Directora de informática	Entrevista
			• Controles contra código malicioso	¿Existen controles de seguridad que permitan la detección y mitigación de malware?	Directora de informática	Entrevista
			• Copias de seguridad de la información	¿Realiza copias de seguridad de los servidores de información y red? ¿Las copias de seguridad	Directora de informática	Entrevista

				son guardadas en un lugar seguro? ¿Cada cuánto tiempo realiza copias de seguridad? ¿Realiza copias de seguridad de los dispositivos de red intermediarios?		
			• Registro de actividad y supervisión	¿Monitorea de manera continua los sistemas de red? ¿De qué manera realiza el monitoreo?	Directora de informática	Entrevista
			• Registro y gestión de eventos de calidad	¿Monitorea y controla el uso de información en cada uno de los usuarios que manipulan los datos?	Directora de informática	Entrevista
			• Consideraciones de las auditorías de los sistemas de información	¿Se realizan auditorías de sistemas de información y redes?	Directora de informática	Entrevista
			• Controles de auditoria de los sistemas de información	¿Se planifican las actividades que conlleva la auditoría? ¿Mientras se realiza el proceso de auditoría se dan a conocer las debilidades que se poseen a la vez estas son corregidas?	Directora de informática	Entrevista
		Seguridad de las telecomunicaciones	• Gestión de la seguridad en las redes	¿Hace uso de herramientas como: CISCO SECURE SCANNER o ETRUST INTRUSION DETECTION, esto con el fin de gestionar la seguridad en la red?	Directora de informática	Entrevista
			• Mecanismos de seguridad asociados a servicios de	¿Qué mecanismos de seguridad emplea para proteger los servicios que ofrece la red?	Directora de informática	Entrevista

			red			
			• Segregación de redes	¿Existen redes virtuales locales en la institución?	Directora de informática	Entrevista
			• Intercambio de información con partes externas	¿Mediante la red intercambia información con entidades externas?	Directora de informática	Entrevista
			• Políticas y procedimientos de intercambio de información	¿Bajo qué políticas y procedimientos se basan para realizar intercambio de información?	Directora de informática	Entrevista
			• Acuerdos de intercambio	¿Qué acuerdos se establecen durante el intercambio de información?	Directora de informática	Entrevista
			• Mensajería electrónica	¿Qué mecanismos de seguridad utiliza para el uso de correo electrónico?	Directora de informática	Entrevista
			• Acuerdos de confidencialidad	¿Se documentan y actualizan los acuerdos de confidencialidad, esto con el fin de evitar fugas de información?	Directora de informática	Entrevista
		Relaciones con Suministradores	• Gestión de la prestación del servicio por suministradores	¿Se verifica el cumplimiento de los acuerdos de los servicios que ofrecen terceros?	Directora de informática	Entrevista
			• Supervisión y revisión de los servicios prestados por terceros	¿La institución monitorea el cumplimiento prestado por los proveedores de servicio de internet (ISP)?	Directora de informática	Entrevista

		Gestión de incidentes en la seguridad de la información	• Gestión de incidentes de seguridad de la información.	¿Existen procedimientos de manejo de los incidentes relacionados a la seguridad de la información en el área de redes?	Directora de informática	Entrevista
			• Responsabilidades y procedimientos	¿Están establecidos los procedimientos para dar respuesta a los incidentes de seguridad de la información en el área de redes?	Directora de informática	Entrevista
			• Notificación de eventos de seguridad de la información	¿Se notifica a la administración los eventos asociados a la seguridad de la información del área de redes?	Directora de informática	Entrevista
			• Notificación de puntos débiles de la seguridad	¿Cuándo se sospecha que existen puntos débiles en la seguridad de la información en la infraestructura de red, estos son documentados e informados?	Directora de informática	Entrevista
			• Valoración de eventos de seguridad de la información y toma de decisiones	¿Se evalúan y clasifican los incidentes de seguridad de la infraestructura de red?	Directora de informática	Entrevista
			• Aprendizaje de los incidente de la seguridad de la información	¿El análisis de los incidentes de seguridad de la información ha aportado conocimientos para reducir la probabilidad de futuros incidentes?	Directora de informática	Entrevista

			• Recopilación de evidencias	¿Se recopilan evidencias de incidente relacionados a la seguridad de la información en la infraestructura de red?	Directora de 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?	Directora de informática	Entrevista
			• Planificación de la continuidad de la seguridad de la información	¿Se determinan cuáles son los requisitos de la seguridad de la información para su gestión durante situaciones críticas?	Directora de informática	Entrevista
			• Implantación de la continuidad de la seguridad de la información	¿Se han implementado procesos, procedimientos y controles para garantizar el nivel necesario de seguridad de la información ante situación adversas?	Directora de informática	Entrevista
			• Redundancias	¿Existen dispositivos de red que permitan la redundancia en la infraestructura de red?	Directora de informática	Entrevista
			• Disponibilidad de las instalaciones para el procesamiento de la información	¿Los dispositivos redundantes ofrecen disponibilidad de la red en todo momento?	Directora de informática	Entrevista

		Cumplimiento	• Cumplimiento de los requisitos legales y contractuales	¿Están definidos los requisitos para la operación, uso y gestión de los recursos de red?	Directora de informática	Entrevista
			• Identificación de la legislación aplicable	¿Existe una documentación de normativas legislativas que regulen los requisitos para el uso de los recursos de red?	Directora de informática	Entrevista
			• Derechos de propiedad intelectual (DPI)	¿Existen procedimientos aplicados para asegurar el uso de recursos originales, tal como el uso de software licenciado?	Directora de informática	Entrevista
			• Protección de los registros de la organización	¿Están los registros de información de la institución debidamente protegidos contra destrucción, falsificación, acceso y publicación?	Directora de informática	Entrevista
			• Protección de datos y privacidad de la información personal	¿La infraestructura de red garantiza la protección y privacidad de la información personal?	Directora de informática	Entrevista
			• Regulación de controles criptográficos	¿Existen controles de cifrado de la información que viaja mediante la red?	Directora de informática	Entrevista
			• Revisión de la seguridad de la información	¿Se revisa con regularidad la seguridad de los recursos de la infraestructura de red?	Directora de informática	Entrevista

			• Revisión independiente de la seguridad de la información	¿Se revisa el enfoque organizacional de la institución para la implementación de controles, políticas, procesos y procedimientos para la seguridad de la información en la infraestructura de red?	Directora de informática	Entrevista
			• Cumplimiento de las políticas y normas de seguridad	¿Se revisa de manera regular el cumplimiento de las políticas y normas de seguridad de la información en la red?	Directora de informática	Entrevista
			• Comprobación del cumplimiento	¿Se revisan de manera regular los recursos de red, para verificar su óptimo cumplimiento con las políticas y normas de seguridad?	Directora de informática	Entrevista

Anexo No 3

Entrevista 1

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida a la directora de informática de la alcaldía municipal de San Ramón, Matagalpa.

El objetivo de esta entrevista es con el fin de recaudar información para determinar la condición actual de la infraestructura de red lógica y física de la Alcaldía Municipal de San Ramón, Matagalpa.

Redes

- **Definición**
  1. ¿Usted conoce el término red de computadores?
     Sí ◯ No ◯
  2. ¿Comprende cuáles son los objetivos de la implementación de redes de computadoras?
     Sí ◯ No ◯

- **Arquitectura de Red**
  1. ¿La tecnología de red empleada es capaz de soportar de manera rápida y eficiente los servicios que se brindan a través de esta?
     Sí ◯ No ◯
  2. ¿La conexión a internet está siempre disponible?
     Sí ◯ No ◯
  3. ¿Existe un proveedor secundario de servicio de internet, en caso que el principal falle?
     Sí ◯ No ◯

4. ¿La infraestructura de red implementada en capaz de admitir a nuevos dispositivos y usuarios en la red?
   Sí ◯ No ◯

5. ¿Se priorizan servicios en la red, tales como Streaming, VoIP, etc?
   Sí ◯ No ◯

6. ¿Existen herramientas y procedimientos aplicados para mitigar las fallas de seguridad?
   Sí ◯ No ◯

- **Tipos de Redes**
  1. ¿Qué tipo de red existe en la institución?
     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) Malla
     e) Árbol
     f) Ninguna

  2. Según su criterio, ¿La topología de red actualmente implementada es la indicada para esta institución?
     Sí ◯ No ◯

- **Elementos de una Red**
  1. ¿Qué medio de trasmisión de datos se usa en 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)?

  2. ¿El tráfico de red es monitoreado?

Infraestructura Física

- **Dispositivos de Red**
  1. ¿Con qué tipos y cantidad de dispositivos de red cuenta la institución?

  2. ¿Los dispositivos de red que están implementados son de última generación?

     Sí ◯ No ◯

  3. Para usted ¿Qué grado de dificultad presenta la administración de los dispositivos de red?

- **Cableados o Guiados**
  1. ¿Qué tipo de cable y categoría utilizan las conexiones de red?

- **Medios de transmisión inalámbricos**
  1. ¿Se hace uso de redes inalámbricas en la institución?

     Sí ◯ No ◯

- **Estación de trabajo**
  1. ¿Con cuántas computadoras por área 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 los ordenadores?
     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 de la red que permitan prevenir la manipulación y acceso no autorizado de la información?
     Sí ◯ No ◯

  2. ¿El personal de informática está en constante capacitación sobre las reglas y procedimientos establecidos sobre la seguridad física de la red?
     Sí ◯ No ◯

3. ¿Se encuentran protegidos los equipos de red que están fuera del cuarto de informática?
   Sí ◯ No ◯

4. ¿Los dispositivos de red se encuentran climatizados?
   Sí ◯ No ◯

5. ¿Los dispositivos de red se encuentran debidamente conectados a la fuente eléctrica?
   Sí ◯ No ◯

6. ¿Existen antecedentes de riesgos y amenazas hacia la seguridad física de la infraestructura red?
   Sí ◯ No ◯

Infraestructura Lógica

- **Servidores**
  1. ¿Qué sistemas operativos servidor utiliza?

- **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

  2. ¿Posee direcciones IP públicas exclusivas para la red de la institución?
     Sí ◯ No ◯

- **Servicios de Red**
  1. ¿Cuáles servicios de red se ofrecen?
- **Segmentación de Red**
  1. ¿Se implementan segmentación de red?
     Sí ◯ No ◯

- **Ancho de Banda**
  1. ¿Con cuanto ancho de banda cuenta la institución?

  2. Según su criterio ¿El ancho de banda contratado es suficiente para proporcionar una conexión óptima a los usuarios? ¿Por qué?

- **Firewall**
  1. ¿La infraestructura de red lógica cuenta con firewall?
     Sí ◯ No ◯

  2. ¿Se monitorean los eventos registrados por el firewall?
     Sí ◯ No ◯
- **VPN**
  1. ¿Actualmente se cuenta con redes virtuales privadas?
     Sí ◯ No ◯

- **Centrales Telefónicas**
  1. ¿Existe una central telefónica?
     Sí ◯ No ◯

  2. ¿Se cuenta con la suficiente cantidad de terminales telefónicas para proveer el servicio a los usuarios?
     Sí ◯ No ◯

- **Políticas de seguridad Lógica**
  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? (Acl, Firewalls, antivirus)
     Sí ◯ No ◯

Anexo No 4

Entrevista 2

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida a la directora de informática de la alcaldía municipal de San Ramón, 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 la alcaldía municipal de San Ramón, Matagalpa.

ISO/IEC 27002:2013

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

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

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

Políticas de Seguridad

- **Directrices de la dirección en seguridad de la información.**
  - ✓ **Conjunto de Políticas**
  1. ¿Están definidas las políticas de seguridad en la red de la institución?

Aspectos Organizativos de la Seguridad de la Información

- **Organización Interna**
  - ✓ **Segregación de Tareas**
  1. ¿Está definida el área de TI?

  2. ¿Se han definido cuáles son sus tareas respecto a la seguridad de las redes, para minimizar el riesgo de un mal uso de los activos de la institución?

Seguridad Ligada al Recurso Humano

- **Antes de la Contratación**
  1. Antes de su contratación como responsable del área informática, ¿Se le dieron a conocer cuáles son los términos y condiciones del empleo?

  - ✓ **Investigación de Antecedentes**
  1. ¿La institución le solicitó un documento legal en el que se reflejen sus antecedentes en otros empleos? ¿Qué tipo de documento se le solicitó

  - ✓ **Términos y Condiciones de Contratación**
  1. En su contrato de empleo, ¿Cuáles son los términos, condiciones y obligaciones que este conlleva?

- **Durante la Contratación**
  1. ¿La dirección se ha encargado de velar por el cumplimiento de la seguridad de las redes en el área de informática?

  - ✓ **Concienciación, Educación y Capacitación en Seguridad de la Información**
  1. ¿La dirección le brinda capacitaciones y le da conocer cuáles son los cambios de las políticas y los procedimientos organizacionales que son relevantes a su área?

Gestión de Activos

- **Responsabilidades sobre los Activos**
  1. ¿Cuáles son sus responsabilidades en el mantenimiento de los controles adecuados sobre los activos asignados a informática?

     ✓ **Inventario de Activos**
     1. ¿Lleva a cabo el inventario de activos del área de informática?
     2. ¿Cada cuánto tiempo realiza dicho inventario?

     ✓ **Uso aceptable de los Activos**
     1. ¿Cuáles son los procedimientos para regular el uso adecuado de los activos del área de redes?

- **Manejo de los Soportes de Almacenamiento**
  1. ¿Cuáles son los controles y procedimientos que se aplican para proteger los medios de almacenamiento?

Control de Acceso

- **Requisitos de Negocio para el Control de Acceso**
  1. ¿Se controla el acceso a la información? ¿De qué manera?

     ✓ **Política de Control de Accesos**
     1. ¿Se encuentran establecidas las políticas de control de acceso? ¿Están documentadas?

     ✓ **Control de Acceso a las Redes y Servicios Asociados**
     1. ¿Existe control de acceso de los usuarios, para verificar que estos utilizan los servicios de red que se le han autorizado? ¿De qué manera?

- **Gestión de Acceso de Usuarios**
    1. ¿Existen procedimientos formales que le permitan determinar, que parámetros tomar en cuenta al momento de asignar los permisos de acceso de red a los usuarios? ¿Cuáles son?

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

    1. ¿Qué procedimientos formales se realizan al momento de dar de alta o baja a un usuario de la red?

    ✓ **Gestión de los Derechos de Acceso con Privilegios Especiales**

    1. ¿Controla los usuarios que tienen privilegios especiales de acceso a la red? ¿Cuáles son estos privilegios?

- **Control de Acceso a Sistemas y Aplicaciones**
    1. ¿Qué procedimientos de seguridad están implementados para evitar que los usuarios manipulen los sistemas, datos y dispositivos restringidos?

    ✓ **Restricciones de Acceso a la Información**

    1. ¿Qué mecanismos de seguridad están implementados para restringir el acceso a la información por parte de los usuarios no autorizados?

    ✓ **Gestión de Contraseñas de Usuarios**

    1. ¿De qué manera se gestionan las contraseñas de los usuarios?

    2. ¿Existen parámetros definidos para la asignación de contraseñas? ¿Cuáles son?

Cifrado

- **Controles Criptográficos**
    1. ¿Implementa técnicas de encriptamiento a la información?

✓ **Políticas de Uso de Controles Criptográficos**

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

✓ **Gestión de Claves**

1. ¿De qué manera administra las claves que permiten el cifrado y descifrado de la información?

Seguridad física y ambiental

- **Áreas Seguras**
  1. ¿Los dispositivos de las redes se encuentran en un área debidamente protegida ante la manipulación y acceso no autorizado?

✓ **Controles Físicos de Entrada**

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

✓ **Seguridad de Oficinas y Recursos**

1. ¿Qué medidas de seguridad de acceso físico implementa en la oficina de informática y sala de video conferencia?

✓ **Protección contra Amenazas Externas y Ambientales**

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

- **Seguridad de los Equipos**
  1. ¿Los dispositivos de red y servidores están debidamente climatizados?

2. ¿Están conectados a fuente de energía de respaldo?

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

- ✓ **Seguridad del Cableado**

1. ¿Los cables de red están canaleteados?

2. ¿Los cables de red están se encuentran debidamente protegidos para evitar la manipulación no autorizada de estos?

- ✓ **Mantenimiento de los Equipos**

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

2. ¿Cada cuánto tiempo se llevan a cabo dichos mantenimientos?

- ✓ **Seguridad de Activos y Equipos fuera de las Instalaciones**

¿Existen dispositivos de red fuera de las instalaciones de la institución y que estos se encuentren a cargo de esta?

Anexo No 5

Entrevista 3

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida a la directora de informática de la alcaldía municipal de San Ramón, 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 la alcaldía municipal de San Ramón, Matagalpa.

Seguridad Operativa

- **Responsabilidades y procedimientos de operación**
  - ✓ **Documentación de procedimientos de operación.**
  1. ¿Existe documentación de los procedimientos de operación para los recursos de red?

  - ✓ **Gestión de cambios**
  1. ¿Se controlan los cambios que afectan en la infraestructura de red?

  - ✓ **Gestión de capacidades**
  1. ¿Los recursos actualmente implementados, ofrecen las condiciones necesarias para operar de manera óptima en un futuro?

- **Protección contra código malicioso**
  1. ¿Actualiza de manera continua el antivirus en todos los ordenadores?

- ✓ **Controles contra código malicioso**

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

- **Copias de seguridad**
  - ✓ **Copias de seguridad de la información**

1. ¿Realiza copias de seguridad de los servidores de sistemas y red?

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

3. ¿Cada cuánto tiempo realiza copias de seguridad?

- **Registro de actividad y supervisión**

1. ¿Monitorea de manera continua los sistemas? ¿De qué manera realiza el monitoreo?

- ✓ **Registro y gestión de eventos de actividad**

1. ¿Monitorea y controla el uso de información en cada uno de los usuarios que manipulan los datos?

- **Consideraciones de las auditorías de los sistemas de información**

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

- **Consideraciones de las auditorias de los sistemas de información**
  - ✓ **Controles de auditoria de los sistemas de información**

1. ¿Se planifican las actividades que conlleva la auditoría?

2. ¿Mientras se realiza el proceso de auditoría se dan a conocer las debilidades que se poseen a la vez estas son corregidas?

Seguridad de las telecomunicaciones

- **Gestión de la seguridad en las redes**
  1. ¿Hace uso de herramientas de monitoreo de red como: CISCO SECURE SCANNER o ETRUST INTRUSION DETECTION, esto con el fin de gestionar la seguridad en la red?

  ✓ **Mecanismos de seguridad asociados a servicios de red**
  1. ¿Qué mecanismos de seguridad emplea para proteger los servicios que ofrece la red?

  ✓ **Segregación de Redes**
  1. ¿Existen redes virtuales locales en la institución?

- **Intercambio de información con partes externas**
  1. ¿Mediante la red intercambia información con entidades externas?

  ✓ **Políticas y procedimientos de intercambio de información**
  1. ¿Bajo qué políticas y procedimientos se basan para realizar intercambio de información?

  ✓ **Acuerdos de intercambio**
  1. ¿Qué acuerdos se establecen durante el intercambio de información?

  ✓ **Mensajería electrónica**
  1. ¿Qué mecanismos de seguridad utiliza para el uso de correo electrónico?

  ✓ **Acuerdos de confidencialidad y secreto**
  1. ¿Se documentan y actualizan los acuerdos de confidencialidad, esto con el fin de evitar fugas de información?

Relaciones con Suministradores

- **Gestión de la prestación del servicio por suministradores**

1. ¿Se verifica el cumplimiento de los acuerdos de los proveedores de servicio de internet?

- ✓ **Supervisión y revisión de los servicios prestados por terceros**

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

Anexo No 6

Entrevista 4

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de entrevista dirigida a la directora de informática de la alcaldía municipal de San Ramón, 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 la alcaldía municipal de San Ramón, Matagalpa.

Gestión de incidentes en la seguridad de la información

- **Gestión de incidentes de seguridad de la información y mejoras.**
    1. ¿Existen procedimientos de manejo de los incidentes relacionados a la seguridad de la información en el área de informática?

    ✓ **Responsabilidades y procedimientos**

    1. ¿Están establecidos los procedimientos para dar respuesta a los incidentes de seguridad de la información en el área de informática?

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

    1. ¿Se notifica a la administración los eventos asociados a la seguridad de la información en el área de informática?

    ✓ **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 tanto en la red como sistemas internos?

- ✓ **Valoración de eventos de seguridad de la información y toma de decisiones**

1. ¿Se evalúan y clasifican los incidentes de seguridad de la infraestructura de red?

- ✓ **Aprendizaje de los incidentes de la seguridad de la información**

1. ¿El análisis de los incidentes de seguridad de la información han aportado conocimientos para reducir la probabilidad de futuros incidentes?

- ✓ **Recopilación de evidencias**

1. ¿Se recopilan evidencias de incidentes relacionados a la seguridad de la información en la red?

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

- **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?

- ✓ **Planificación de la continuidad de la seguridad de la información**

1. ¿Se determinan cuáles son los requisitos de la seguridad de la información para su gestión durante situaciones críticas?

- ✓ **Implantación de la continuidad de la seguridad de la información**

1. ¿Se han implementado procesos, procedimientos y controles para garantizar el nivel necesario de seguridad de la información ante situación adversas?

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

     ✓ **Disponibilidad de las instalaciones para el procesamiento de la información**

     1. ¿Los dispositivos redundantes ofrecen disponibilidad de la red en todo momento?

Cumplimento

- **Cumplimiento de los requisitos legales y contractuales**
  1. ¿Están definidos los requisitos para la operación, uso y gestión de los recursos de red?

     ✓ **Identificación de la legislación aplicable**

     1. ¿Existe una documentación de normativas legislativas que regulen los requisitos para el uso de los recursos de red?

     ✓ **Derechos de propiedad intelectual (DPI)**

     1. ¿Existen procedimientos aplicados para asegurar el uso de recursos originales, tal como el uso de software con licencia?

     ✓ **Protección de los registros de la organización**

     1. ¿Los registros de información de la institución que se mueven en la red están protegidos contra destrucción, falsificación, acceso y publicación?

     ✓ **Protección de datos y privacidad de la información personal**

     1. ¿Existen normativas legales aplicadas a la privacidad y protección de la información personal?

- ✓ **Regulación de controles criptográficos**

1. ¿Existen controles de cifrado de la información que viaja mediante la red?

- **Revisión de la seguridad de la información**

1. ¿Se revisa con regularidad la seguridad de los sistemas de información y de red?

- ✓ **Revisión independiente de la seguridad de la información**

1. ¿Se revisa el enfoque organizacional de la institución para la implementación de controles, políticas, procesos y procedimientos para la seguridad de la información en la red?

- ✓ **Cumplimiento de las políticas y normas de seguridad**

1. ¿Se revisa de manera regular el cumplimiento de las políticas y normas de seguridad de la información en la red?

- ✓ **Comprobación del cumplimiento**

¿Se revisan de manera regular los recursos de red, para verificar su óptimo funcionamiento para el cumplimiento de las políticas y normas de seguridad?

Anexo No 7

Guía de Observación

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria Matagalpa

Guía de observación aplicada a la alcaldía municipal de San Ramón, Matagalpa.

Indicador	Observación	Detalles
Tipos de redes	Tipos de redes existes en la institución	Las dos redes implementadas en la institución son de área local (LAN), no existen otros tipos de redes porque no hay nodos externos en la institución
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 árbol.
Elementos de una red	Medio de trasmisión de datos usados en la institución	El medio de trasmisión usado en la red principal es a través de cables, mientras que en la sala de video conferencias se utiliza medios de transmisión inalámbricos.

Factores Internos	Monitoreo en el tráfico de red	No se realiza monitoreo de red en la institución
Dispositivos de Red	Dispositivos de red de última generación	Se determinó que los dispositivos de red utilizados están desfasados
Cableados o Guiados	Cable y categoría utilizados en las conexiones de red	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 pudo observar que los dispositivos de red intermediarios fuera del área de informática no poseen ninguna protección contra acceso y manipulación no autorizada
	Climatización de equipos	Únicamente los equipos que están en la oficina de informática y sala de video conferencias están climatizados.
	Dispositivos de red conectados a fuentes de respaldo de energía eléctrica	Los dispositivos de red se encuentran conectados a fuentes de respaldo de energía eléctrica.

Ancho de Banda	Ancho de banda en las redes	Se realizaron pruebas de velocidad en las dos redes, sumando un total de 15 mbits/seg, divididos en 10 mbits/seg para la primera red y 5 mbits/seg para la sala de video conferencias.
Centrales Telefónicas	Central telefónica	Se cuenta con una central telefónica análoga ubicada en el área de administración tributaria.
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 con dominio a la gerencia, solamente existe un área de informática bajo el dominio de la administración.
Áreas seguras	Área de dispositivos protegida ante el acceso no autorizado	Los dispositivos que están en el área de informática y video conferencia están protegidos bajo llave, por lo tanto para tener acceso a estos se necesita autorización previa de la directora de informática. Mientras que los dispositivos que están dispersos en las demás áreas no cuentan con ninguna protección.
Seguridad de oficinas y recursos	Medidas de seguridad de acceso físico implementada en la oficina de informática y sala de video conferencia	El único control físico usado es la puerta para entrar a la oficina de informática y sala de video conferencias.

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.
Seguridad de los equipos	Dispositivos intermediarios ubicados en rack	En la infraestructura de red no existe un rack que permita centralizar las conexiones de red.
Seguridad del cableado	Cables canaleteados	El cableado no está estructurado, ni protegido con canaletas que eviten la manipulación del cable.

Anexo No 8

Matriz de resultado de las entrevistas realizadas a la directora de informática
(Entrevista Redes)

Indicadores	Directora de Informática
¿Usted conoce el término red de computadores?	Si
¿Comprende cuáles son los objetivos de la implementación de redes de computadoras?	Si
¿La tecnología de red empleada es capaz de soportar de manera rápida y eficiente los servicios que se brindan a través de esta?	Si, el proxy permite que los usuarios no utilicen la red para hacer otras cosas que no están permitidas, por ejemplo los videos están bloqueados
¿La conexión a internet está siempre disponible?	Si
¿Existe un proveedor secundario de servicio de internet, en caso que el principal falle?	No, solo tenemos el servicio que nos da claro
¿La infraestructura de red implementada en capaz de admitir a nuevos dispositivos y usuarios en la red?	Si, la red tiene la capacidad para poder conectar más dispositivos
¿Se priorizan servicios en la red, tales como Streaming, VoIP, etc?	No tengo conocimiento, porque no puedo acceder el servidor de red, no tengo la contraseña y el muchacho que lo instaló se llevó todo y no dejo nada documentado
¿Existen herramientas y procedimientos aplicados para mitigar las fallas de seguridad?	Si, utilizamos antivirus
¿Qué tipo de red existe en la institución?	Una red LAN, solo nos conectamos internamente, no compartimos información hacia fuera

¿Qué topología de red está implementada en la institución?	Desconozco, cuando yo entré a trabajar ya estaba todo implementado y no existe ninguna documentación
Según su criterio, ¿La topología de red actualmente implementada es la indicada para esta institución?	No lo sé, desconozco el tipo de topología
¿Qué medio de trasmisión de datos se usa en la institución?	Se utiliza cableado para la principal y red inalámbrica para la sala de videoconferencia
Según su criterio, ¿La red posee todos los dispositivos necesarios para ofrecer un servicio de calidad?	Si
¿Qué tipo de datos se transportan a través de la red? (Conexión a base de datos, sitios web, videos, voiP,etc)?	Conexión a base de datos, videos, páginas web, los datos del sistema SIAFM
¿El tráfico de red es monitoreado?	No
¿Con qué tipos y cantidad de dispositivos de red cuenta la institución?	1 servidor de red, 1 servidor de sistema,3 router, 6 switch, 1 panel de conexiones
¿Los dispositivos de red que están implementados son de última generación?	No
Para usted ¿Qué grado de dificultad presenta la administración de los dispositivos de red?	Para el servidor no tengo la contraseña para acceder y administrarlo, los otros dispositivos no son difíciles de configurar
¿Qué tipo de cable y categoría utilizan las conexiones de red?	Cable UTP categoría 5e
¿Se hace uso de redes inalámbricas en la institución?	Si, solo en la sala de videoconferencias

¿Con cuántas computadoras por área cuenta la institución?	7 en contabilidad, 1 informática, 1 administración, 2 adquisición, 6 proyectos, 1 turismo, 1 auditor interno, 1 gerencia , 1 asistente del alcalde, 4 tributaria, 1 servicios municipales, 1 recursos humanos, 1 registro, 2 escuela de oficio, 3 divulgación, 3 catastro, 1 UMAS, 1 medio ambiente, 1 promotoría social, 1 secretaria de consejo, 1 recepción, 20 sala de video conferencia.
¿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 que están fuera del cuarto de informática?	No

¿Los dispositivos de red se encuentran climatizados?	Algunos, solo los que están dentro de la oficina de informática están con aire acondicionado los que están fuera no
¿Los dispositivos de red se encuentran debidamente conectados a la fuente eléctrica?	Si
¿Existen antecedentes de riesgos y amenazas hacia la seguridad física de la infraestructura red?	No
¿Qué sistemas operativos servidor utiliza?	Linux para el servidor proxy y Windows server 2007 para el servidor del sistema SIAFM
¿Qué rango de direccionamiento IP privado esta implementado en la infraestructura de red?	10.0.0.0 /8
¿Posee direcciones IP públicas asignadas para su en la red?	No
¿Cuáles servicios de red se ofrecen?	Proxy, chat interno, bases de datos, impresiones en red
¿Se implementan segmentación de red?	No
¿Con cuanto ancho de banda cuenta la institución?	10 Mb con claro y 5 Mb con ENATREL
Según su criterio ¿El ancho de banda contratado es suficiente para proporcionar una conexión óptima a los usuarios? ¿Por qué?	Sí, es suficiente ya que el tráfico que más se genera es el acceso a páginas en internet y las páginas que usan mucho internet están bloqueadas. El sistema no genera mucho tráfico
¿La infraestructura de red lógica cuenta con firewall?	No, solo se utilizan los que traen el sistema operativo en las computadoras
¿Se monitorean los eventos registrados por el firewall?	No

¿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? (Acl, Firewalls, antivirus)	Solo se hace uso de antivirus

Anexo No 9

Matriz de resultado de las entrevistas realizadas a la directora de informática
(Entrevistas ISO/IEC 27002:2013)

Indicadores	Directora de informática
¿Usted conoce acerca de normativas internacionales que ayudan a regir la seguridad de la información?	No conozco
¿Considera importante implementar normativas internacionales que regulan la seguridad de la información?	Sí, porque de esta manera se evitaría perdida de información y accesos de modificaciones de personas no autorizadas
¿Conoce acerca de la Norma ISO/IEC 27002:2013?	No conozco
¿Están definidas las políticas de seguridad en la red de la institución?	No están definidas
¿Está definida el área de TI?	No, no se ha definido un área de TI
¿Se han definido cuáles son sus tareas respecto a la seguridad de las redes, para minimizar el riesgo de un mal uso de los activos de la institución?	No me definieron cuales eran
Antes de su contratación como responsable del área informática, ¿Se le dieron a conocer cuáles son los términos y condiciones del empleo?	Si me dieron a conocer
¿La institución le solicitó un documento legal en el que se reflejen sus antecedentes en otros empleos? ¿Qué tipo de documento se le solicitó?	Si me pidieron y estos documentos solamente fueron cartas de recomendación.

En su contrato de empleo, ¿Cuáles son los términos, condiciones y obligaciones que este conlleva?	No están definidas
¿La dirección se ha encargado de velar por el cumplimiento de la seguridad de las redes en el área de informática?	Cuando ocurre un fallo únicamente me preguntan qué ha pasado con la red y por qué sucedió esto.
¿La dirección le brinda capacitaciones y le da a conocer cuáles son los cambios de las políticas y los procedimientos organizacionales que son relevantes a su área?	Solamente capacitaciones por parte de INIFOM y también me brinda los cambios de políticas y procedimientos en el área.
¿Cuáles son sus responsabilidades en el mantenimiento de los controles adecuados sobre los activos asignados a informática?	Cumplir con los controles y lo que la dirección me indique
¿Lleva a cabo el inventario de activos del área de informática?	Si realizo el inventario
¿Cada cuánto tiempo realiza dicho inventario?	El inventario lo realizo anualmente
¿Cuáles son los procedimientos para regular el uso adecuado de los activos del área de redes?	No existen procedimientos
¿Cuáles son los controles y procedimientos que se aplican para proteger los medios de almacenamiento?	No existen controles y procedimientos
¿Se controla el acceso a la información? ¿De qué manera?	No se controla
¿Se encuentran establecidas las políticas de control de acceso? ¿Están documentadas?	No existen políticas ni tampoco documentación de estas.
¿Existe control de acceso de los usuarios, para verificar que estos utilizan los servicios de red que se le han autorizado? ¿De qué manera?	Si, como es el caso de contabilidad, esto a través del servidor de red y el servidor de sistemas

¿Existen procedimientos formales que le permitan determinar, que parámetros tomar en cuenta al momento de asignar los permisos de acceso a la red a los usuarios? ¿Cuáles son?	Yo no tengo definidos los parámetros dado que estos ya están definidos por INIFOM
¿Qué procedimientos formales se realizan al momento de dar de alta o baja a un usuario de la red?	No realizo procedimientos
¿Controla los usuarios que tienen privilegios especiales de acceso a la red? ¿Cuáles son estos privilegios?	Si controla y el privilegio es tener acceso total a la red sin ninguna restricción.
¿Qué procedimientos de seguridad están implementados para evitar que los usuarios manipulen los sistemas, datos y dispositivos restringidos?	La contraseña del servidor se cambia cada dos meses, control de entrada a la oficina, uso de proxy en las computadoras y los dispositivos que están fuera de la oficina no se le aplican procedimientos de seguridad.
¿Qué mecanismos de seguridad están implementados para restringir el acceso a la información por parte de los usuarios no autorizados?	No todos los sistemas están en red. Los sistemas están restringidos con contraseñas que solamente yo conozco.
¿De qué manera se gestionan las contraseñas de los usuarios?	No gestiono las contraseñas de usuarios
¿Existen parámetros definidos para la asignación de contraseñas? ¿Cuáles son?	No existen parámetros
¿Implementa técnicas de encriptamiento a la información?	No se implementan
¿Existen políticas de seguridad que regulen el uso de cifrado?	No existen

¿De qué manera administra las claves que permiten el cifrado y descifrado de la información?	No existen claves
¿Los dispositivos de las redes se encuentran en un área debidamente protegida ante la manipulación y acceso no autorizado?	Solamente algunos dispositivos 50% en área protegida y 50% en área desprotegida
¿Existen medidas de controles físicos aplicadas a las áreas donde se encuentran los dispositivos de red? ¿Cuáles son estos controles?	Solamente en la oficina de informática y sala de video conferencia y el control es enllavar la puerta.
¿Qué medidas de seguridad de acceso físico implementa en la oficina de informática y sala de video conferencia?	Puerta con llave y solamente yo poseo la llave
¿Los dispositivos de red y servidores se encuentran en un lugar capaz de soportar desastres naturales y evitar incidentes malintencionados a la información?	Desastres naturales no es seguro y contra ataques malintencionados solamente están protegidos un 50% de los equipos
¿Los dispositivos de red y servidores están debidamente climatizados?	Solamente los servidores están climatizados , mientras que los otros equipos no
¿Están conectados a fuente de energía de respaldo?	Si, el 100% de los equipos
¿Los dispositivos de red intermediarios como conmutadores se encuentran ubicados en un rack, el cual evite la manipulación no autorizada de estos?	No
¿Los cables de red están canaleteados?	No
¿Los cables de red están se encuentran debidamente protegidos para evitar la manipulación no autorizada de estos?	No, estos pueden ser manipulados con facilidad

¿Qué tipo de mantenimiento se les suministra a los dispositivos de red y servidores? (Preventivos y correctivos)	Preventivos y correctivos
¿Cada cuánto tiempo se llevan a cabo dichos mantenimientos?	De 3 a 5 meses
¿Existen dispositivos de red fuera de las instalaciones de la institución que estén a cargo de esta y sí se aplican mecanismos de seguridad?	Si existen, pero no se aplican mecanismos de seguridad ✓ En la biblioteca hay: 10 computadoras personales, un módem y un enrutador inalámbrico ✓ En la escuela de oficio hay: 20 computadoras personales, un enrutador y un conmutador.
¿Existe documentación de los procedimientos de operación para los recursos de red?	No
¿Se controlan los cambios que afectan en la infraestructura de red?	No
¿Los recursos actualmente implementados, ofrecen las condiciones necesarias para operar de manera óptima en un futuro?	Si
¿Actualiza de manera continua el antivirus en todos los ordenadores?	Las máquinas que están con Kaspersky se actualizan diario, mientras que las otras que tiene Avast cada 20 días
¿Existen controles de seguridad que permitan la detección y mitigación de malware?	Solo antivirus
¿Realiza copias de seguridad de los servidores de sistemas y red?	Si, diario realizo copia de seguridad en el servidor del sistema SIAFM, en el servidor del proxy no tengo acceso
¿Las copias de seguridad son guardadas en un lugar seguro?	Si

¿Cada cuánto tiempo realiza copias de seguridad?	En el caso del sistema de SIAFM diario
¿Monitorea de manera continua los sistemas? ¿De qué manera realiza el monitoreo?	No, solo los monitoreo cuando presentan alguna falla
¿Monitorea y controla el uso de información en cada uno de los usuarios que manipulan los datos?	No
¿Se realizan auditorías de sistemas de información y redes?	No
¿Se planifican las actividades que conlleva la auditoría?	No
¿Mientras se realiza el proceso de auditoría se dan a conocer las debilidades que se poseen a la vez estas son corregidas?	No
¿Hace uso de herramientas de monitoreo de red como: CISCO SECURE SCANNER o ETRUST INTRUSION DETECTION, esto con el fin de gestionar la seguridad en la red?	No
¿Qué mecanismos de seguridad emplea para proteger los servicios que ofrece la red?	Solo el proxy
¿Existen redes virtuales locales en la institución?	No
¿Mediante la red Intercambia información con entidades externas?	No
¿Bajo qué políticas y procedimientos se basan para realizar intercambio de información?	Ninguna
¿Qué acuerdos se establecen durante el intercambio de información?	Ninguno

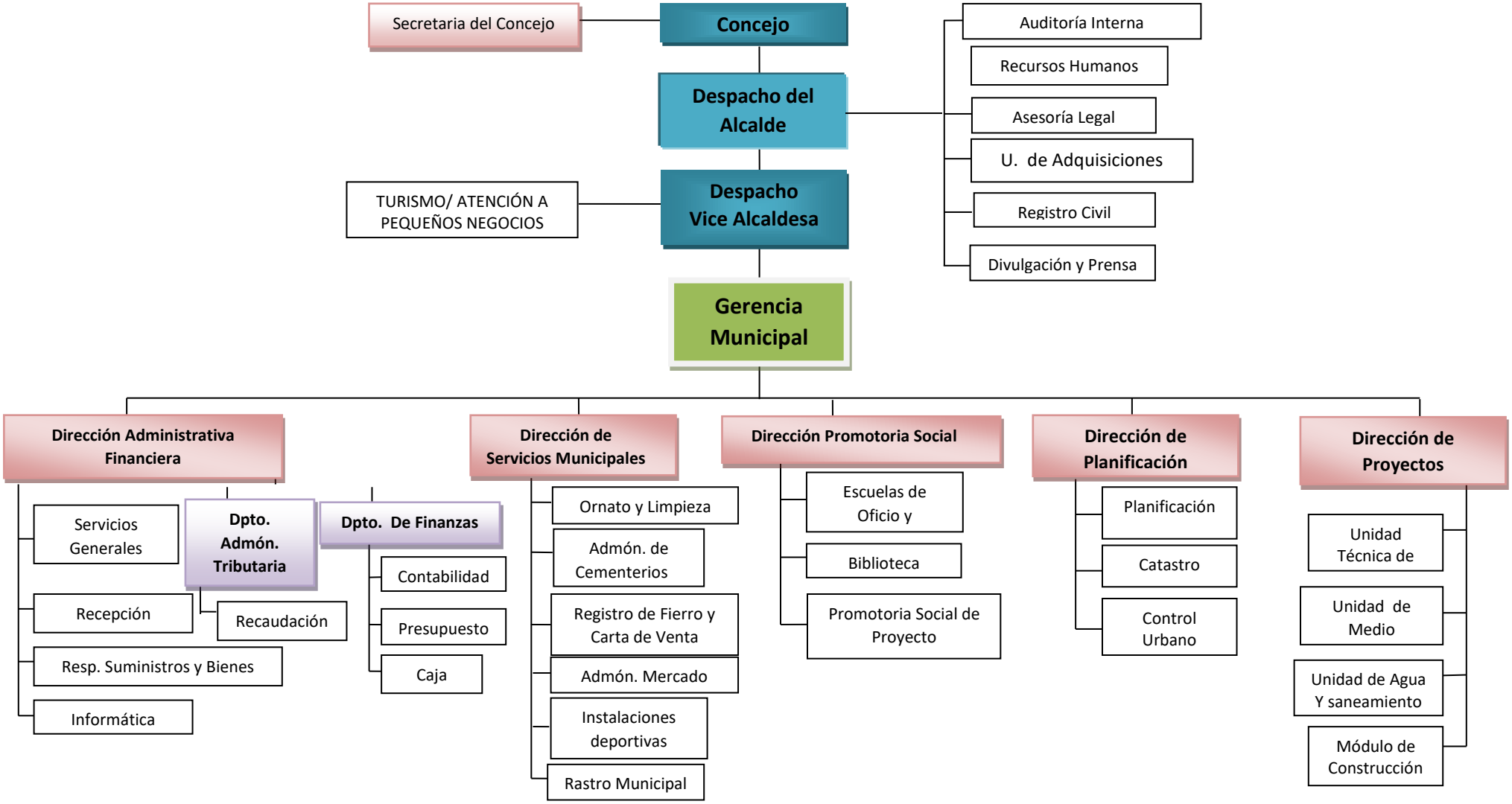
¿Qué mecanismos de seguridad utiliza para el uso de correo electrónico?	Ninguno
¿Se documentan y actualizan los acuerdos de confidencialidad, esto con el fin de evitar fugas de información?	No existen acuerdos de confidencialidad
¿Se verifica el cumplimiento de los acuerdos por parte de los proveedores de servicio de internet?	Si, lo que hago es hacer una prueba de velocidad para ver que si se está dando el ancho de banda que debería ser
¿La institución monitorea el cumplimiento de los servicios prestados por los proveedores de internet (ISP)?	No
¿Existen procedimientos de manejo de los incidentes relacionados a la seguridad de la información en el área de informática?	No
¿Están establecidos los procedimientos para dar respuesta a los incidentes de seguridad de la información en el área de informática?	No
¿Se notifica a la administración los eventos asociados a la seguridad de la información del área de informática?	A veces, solo cuando se trata de los sistemas internos
¿Se documenta y notifica a la administración la sospecha de puntos débiles en la seguridad de la información tanto en la red como sistemas internos?	No
¿Se evalúan y clasifican los incidentes de seguridad de la infraestructura de red?	No

¿El análisis de los incidentes de seguridad de la información ha aportado conocimientos para reducir la probabilidad de futuros incidentes?	A veces, porque no se efectúa un análisis detallado de los incidentes y tampoco son documentados
¿Se recopilan evidencias de incidente relacionados a la seguridad de la información en la infraestructura en la red?	No
¿Existe un plan de continuidad y recuperación de los procesos de seguridad de la información ante desastres?	No
¿Se determinan cuáles son los requisitos de la seguridad de la información para su gestión durante situaciones críticas?	No
¿Se han implementado procesos, procedimientos y controles para garantizar el nivel necesario de seguridad de la información ante situación adversas?	No
¿Existen dispositivos de red que permitan la redundancia en la infraestructura de red?	No
¿Los dispositivos redundantes ofrecen disponibilidad de la red en todo momento?	No existen dispositivos que permitan la redundancia en la red
¿Están definidos los requisitos para la operación, uso y gestión de los recursos de red?	No
¿Existe una documentación de normativas legislativas que regulen los requisitos para el uso de los recursos de red?	No
¿Existen procedimientos aplicados para asegurar el uso de recursos originales, tal como el uso de software con licencia?	No

¿Los registros de información de la institución que se mueven en la red están protegidos contra destrucción, falsificación, acceso y publicación?	Si, solo yo tengo acceso a la información respaldada.
¿Existen normativas legales aplicadas a la privacidad y protección de la información personal?	No
¿Existen controles de cifrado de la información que viaja mediante la red?	No
¿Se revisa con regularidad la seguridad de los sistemas de información y de red?	Solo cuando este presenta algunas fallas
¿Se revisa el enfoque organizacional de la institución para la implementación de controles, políticas, procesos y procedimientos para la seguridad de la información en la infraestructura de red?	No
¿Se revisa de manera regular el cumplimiento de las políticas y normas de seguridad de la información en la red?	No
¿Se revisan de manera regular los recursos de red, para verificar su óptimo funcionamiento para el cumplimiento de las políticas y normas de seguridad?	No

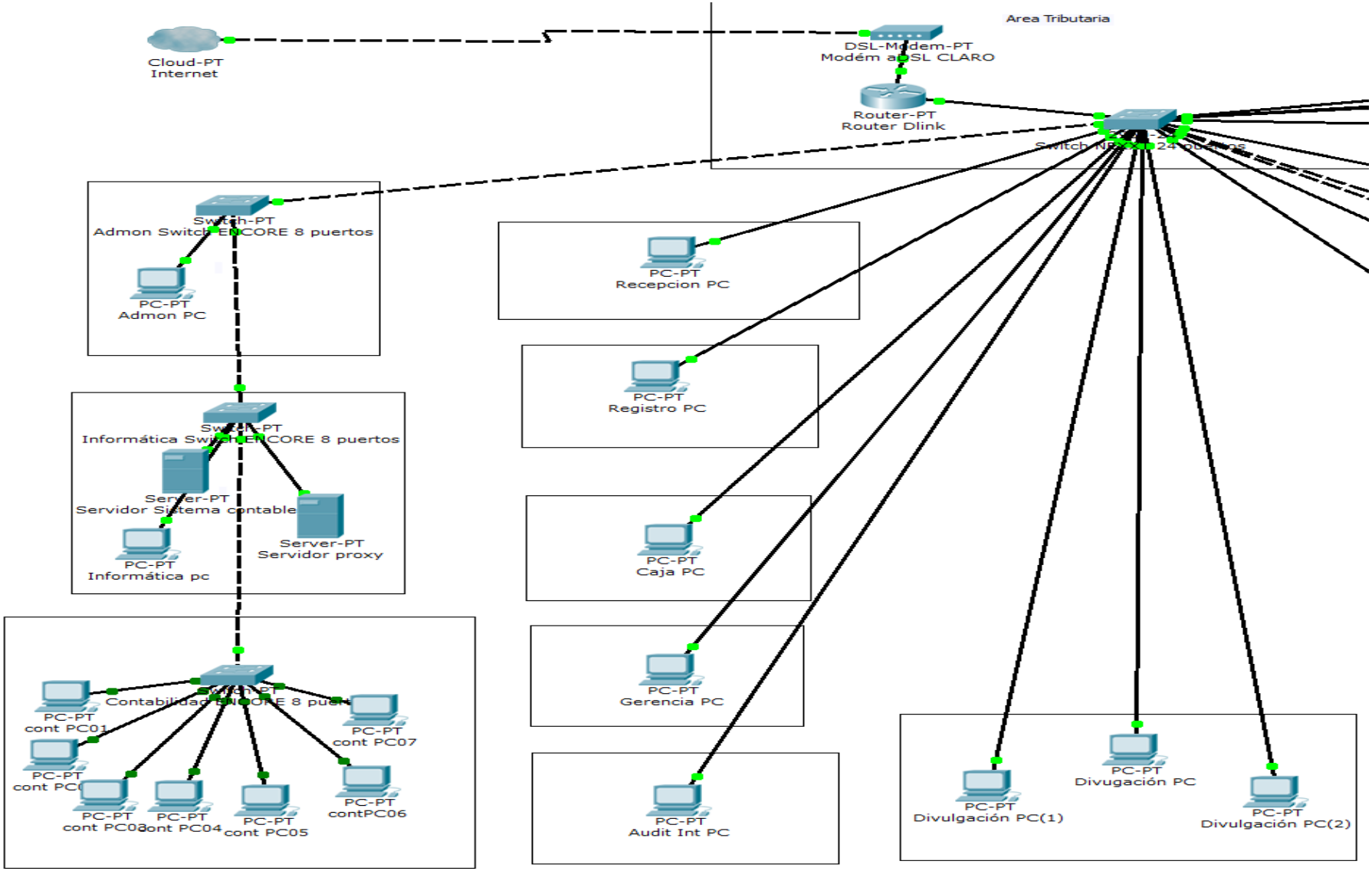
Anexo No 10

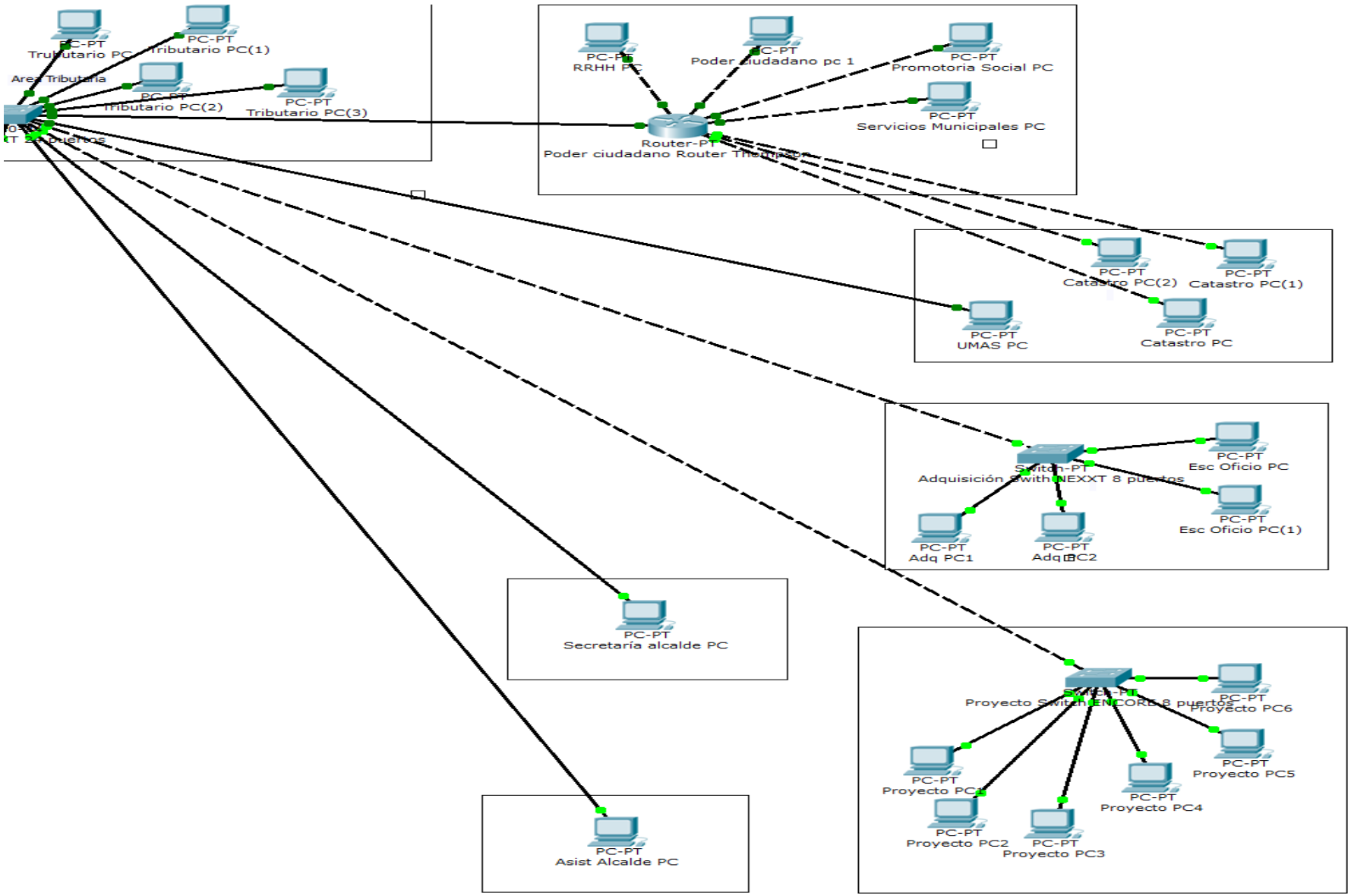
Organigrama actual Alcaldía Municipal de San Ramón



Anexo No 11

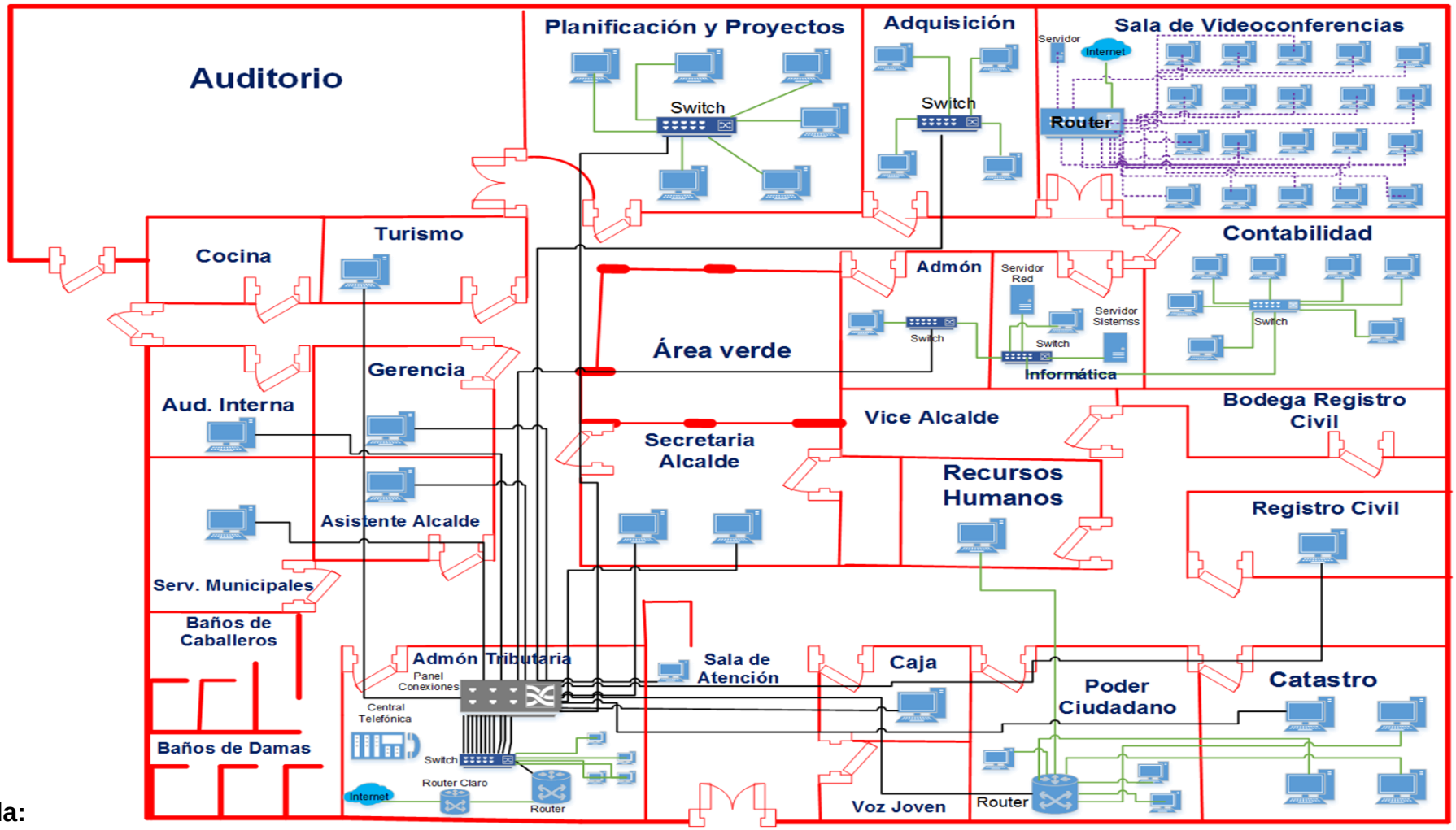
Topología de red lógica actual Alcaldía Municipal de San Ramón (Red principal)




PC-PT
Tributario PC
PC-PT
Tributario PC(1)
Area Tributaria
PC-PT
Tributario PC(2)
PC-PT
Tributario PC(3)
PC-PT
RRHH PC
PC-PT
Poder ciudadano pc 1
PC-PT
Promotoria Social PC
PC-PT
Servicios Municipales PC
Router-PT
Poder ciudadano Router Thompson
PC-PT
Catastro PC(2)
PC-PT
Catastro PC(1)
PC-PT
UMAS PC
PC-PT
Catastro PC
PC-PT
Esc Oficio PC
PC-PT
Esc Oficio PC(1)
PC-PT
Adq PC1
PC-PT
Secretaría alcalde PC
PC-PT
Proyecto PC6
PC-PT
Proyecto PC5
PC-PT
Proyecto PC4
PC-PT
Proyecto PC2
PC-PT
Proyecto PC3
PC-PT
Asist Alcalde PC

Anexo No 12

Topología de red física actual Alcaldía Municipal de San Ramón (Red principal)

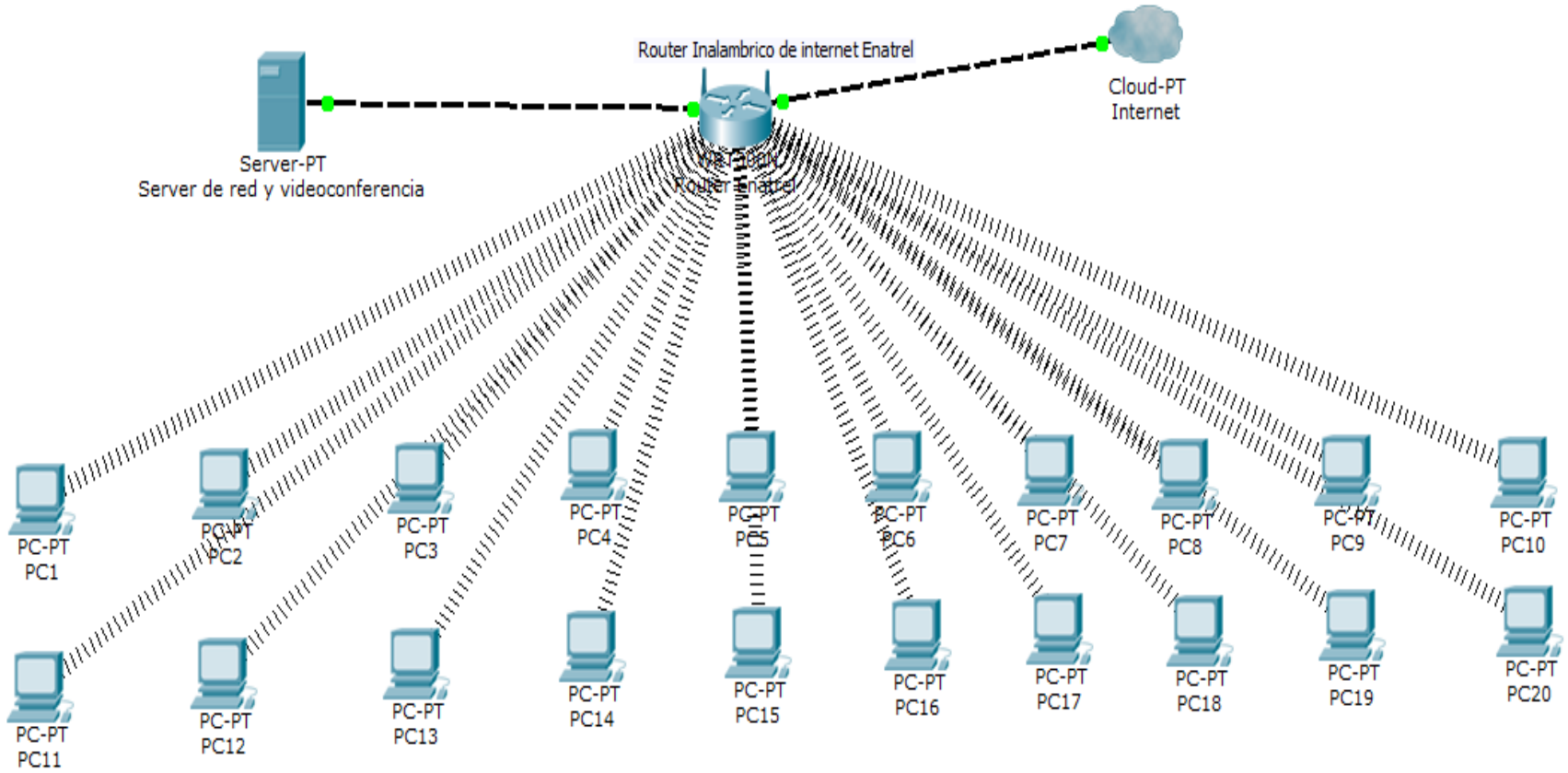


Leyenda:

- ✓ Conexión inalámbrica
- ✓ Conexión cableada

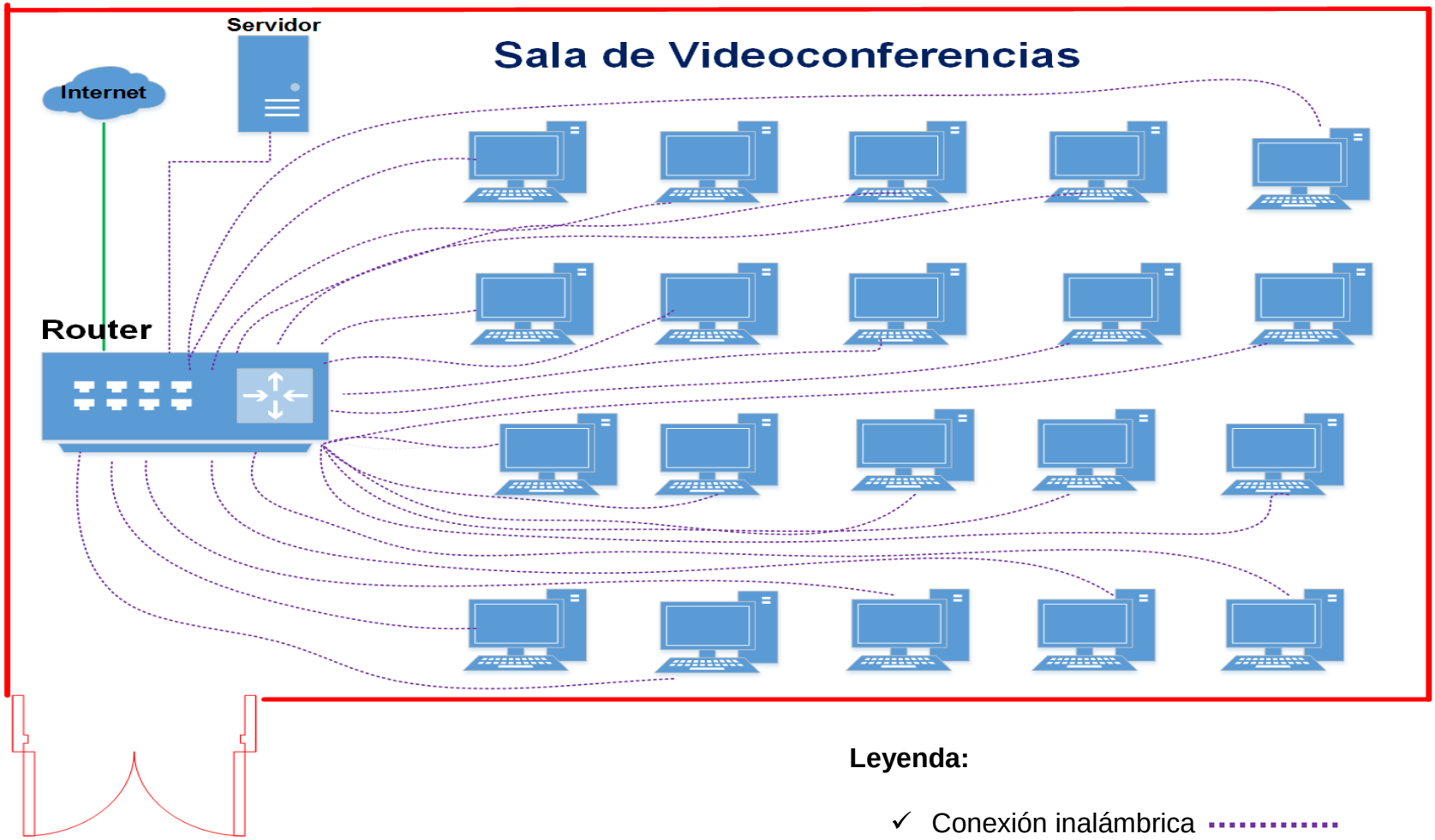
Anexo No 13

Topología de red lógica actual Alcaldía Municipal de San Ramón (Red videoconferencia)



Anexo No 14

Topología de red física actual Alcaldía Municipal de San Ramón (Red videoconferencia)



Leyenda:

- ✓ Conexión inalámbrica
- ✓ Conexión cableada