Universidad Técnica Nacional

Sede Del Pacífico

Licenciatura en Ingeniería en Tecnologías de Información

Proyecto de Graduación

Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República

Estudiantes

Isaac Alejandro Arguedas Leitón
6 0414 0826

Luis Gerardo Barquero Aguilar
6 0440 0973

Marcos Daniel Herrera Madrigal
6 0437 0102

Puntarenas, 2020

ACTA DE APROBACIÓN

Sede del Pacífico
Carrera Ingeniería en Tecnologías de la Información

ACTA DE APROBACIÓN

En la ciudad de Puntarenas, a los 26 días del mes de febrero del año 2020 al ser las18:00 horas, estando presentes en el Campus Juan Rafael Mora Porras de la Sede del Pacífico de la Universidad Técnica Nacional, las siguientes personas:

Profesor Tutor: Floribeth Vindas Parra
Lector: Oberto Santín Cuesta
Lector: Jorge Félix Ruíz Fernández
Representante del Sector Productivo: Erick Saborío Berger
Presidente del Tribunal Examinador: Antonieta González Esquivel

En su condición de miembros del Tribunal Evaluador, para evaluar el proyecto de graduación y optar por el grado de Licenciatura en Ingeniería en Tecnologías de Información, de los estudiantes Isaac Alejandro Arguedas Leitón, cédula de identidad 604140826, Luis Gerardo Barquero Aguilar cédula de identidad 604400973, y Marcos Daniel Herrera Madrigal, cédula de identidad 604370102.

Reunido el Tribunal Evaluador los aspirantes procedieron a defender su proyecto de graduación denominado "**Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República".**

Concluida la defensa del proyecto de graduación, el Tribunal Evaluador consideró que, de conformidad con la normativa en la materia, los estudiantes obtuvieron una calificación de 100, cumpliendo con las exigencias requeridas para la aprobación de la tesis y le es conferido el grado de **Licenciatura en Ingeniería en Tecnologías de Información**

No ( ) Sí (✓) Mención honorífica

Ing. Floribeth Vindas Parra	Ing. Oberto Santín Cuesta	Ing. Jorge Félix Ruíz Fernández
Profesor Tutor	**Lector**	**Lector**
Ing. Erick Saborío Berger		Ing. Antonieta González Esquivel
Representante del Sector Productivo		**Presidente del Tribunal Examinador**

Estudiantes:
Isaac Alejandro Arguedas Leitón _____
Luis Gerardo Barquero Aguilar _____
Marcos Daniel Herrera Madrigal _____

Carrera Tecnologías de Información — Sello — Universidad Técnica Nacional

Central Telefónica: 2660-1700, Ext. 4034
e-mail:agonzaleze@utn.ac.cr, www.utn.ac.cr

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Nosotros, Isaac Alejandro Arguedas Leitón, Luis Gerardo Barquero Aguilar, y Marcos Daniel Herrera Madrigal, portadores de la cédula de identidad N° 604140826, 604400973, y 604370102, respectivamente; somos conocedores de las sanciones legales con que la Ley Penal de la República de Costa Rica castiga el falso testimonio y el Reglamento Disciplinario Estudiantil de la Universidad Técnica Nacional, UTN.

Declaramos bajo la fe de juramento lo siguiente: Que somos estudiantes de la Carrera de Tecnologías de la Información, en el nivel de Licenciatura de la Universidad Técnica Nacional, UTN y, como requisito de graduación, debemos realizar proyecto de graduación, el cual tiene como tema de investigación: Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República. Por lo tanto, manifestamos que la misma ha sido elaborada siguiendo las disposiciones exigidas por la Universidad Técnica Nacional, UTN.

Firmamos en la ciudad de Puntarenas a las 19 horas del 15 del mes de enero del 2020.

Isaac Alejando Arguedas Leitón	Luis Gerardo Barquero Aguilar	Marcos Daniel Herrera Madrigal
604140826	604400973	604370102

CARTA DE APROBACIÓN DE TUTORA

30 de enero del 2020

Señores
Comisión de Evaluación
Carrera, Tecnologías de información
UTN, Sede del Pacífico

Estimados señores:

Les informo que los estudiantes **Issac Alejandro Arguedas Leitón** portador de la cédula de identidad **6-0414-0826**, **Luis Gerardo Barquero Aguilar** con cédula de identidad **6-0440-0973** y de **Marcos Daniel Herrera Madrigal** portador de la cédula de identidad **6-0437-0102** han concluido con su trabajo final de graduación denominado **"Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República."**

Dicho trabajo fue revisado por dos lectores, una filóloga, así como por mi persona., por lo tanto, les solicito muy respetuosamente fijar una fecha para su presentación y defensa.

Muchas gracias por su atención.

Cordialmente,

M.Ed. Floribeth Vindas Parra
Profesora Tutora

CARTA DE LECTOR

Puntarenas, 21 de enero del 2020

Sra.
M.Sc. Antonieta González Esquivel
Directora de la Carrera de Tecnologías de la Información
Universidad Técnica Nacional

Estimada señora:

Sirva la presente para hacer de su conocimiento mi aprobación en calidad de lector, del trabajo final de graduación, titulado **"Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República."**, elaborado por los estudiantes **Issac Alejandro Arguedas Leitón** portador de la cédula de identidad **6-0414-0826**, **Luis Gerardo Barquero Aguilar** portador de la cédula de identidad **6-0440-0973** y de **Marcos Daniel Herrera Madrigal** portador de la cédula de identidad **6-0437-0102**, para optar por el grado académico de **Licenciatura en Ingeniería en Tecnologías de la Información**.

Hago constar que he revisado y corregido todos los aspectos referentes a este documento; por lo que indico que el mismo se encuentra listo para ser presentado a la Universidad Técnica Nacional, como trabajo final de graduación.

Atentamente:

M.Sc. Jorge Félix Ruiz Fernández
Cédula: 6-0231-0557.

Puntarenas, 21 de enero del 2020

Sra.
M.Sc. Antonieta González Esquivel
Directora de la Carrera de Tecnologías de la Información
Universidad Técnica Nacional

Estimada señora:

En mi calidad de lector, me permito informar la aprobación del trabajo final de graduación, titulado **"Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República.",** elaborado por los estudiantes **Issac Alejandro Arguedas Leitón** portador de la cédula de identidad **6-0414-0826**, **Luis Gerardo Barquero Aguilar** portador de la cédula de identidad **6-0440-0973** y de **Marcos Daniel Herrera Madrigal** portador de la cédula de identidad **6-0437-0102**, para optar por el grado académico de **Licenciatura en Ingeniería en Tecnologías de la Información**.

Doy fe de haber revisado y corregido este documento; y manifiesto que el mismo se encuentra listo para ser presentado a la Universidad Técnica Nacional, como trabajo final de graduación.

Atentamente:

M.Sc. Oberto Santín Cuesta
Cédula: 8-0091-0857.

CARTA DE FILÓLOGO

CONSTANCIA DE REVISIÓN FILOLÓGICA

Heredia, 27 de enero de 2020
Universidad Técnica Nacional
Sede del Pacífico

Estimados señores:

Se han revisado y corregido errores gramaticales, de puntuación, ortográficos y de estilo, que se manifiestan en el documento escrito de un proyecto de graduación.

Título del proyecto: *Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República*

Sustentantes:

Isaac Alejandro Arguedas Leitón

Luis Gerardo Barquero Aguilar

Marcos Daniel Herrera Madrigal

Título académico por el que se opta: Licenciatura en Tecnologías de información

Este Trabajo Final de Graduación cumple con los requisitos formales establecidos por la Real Academia Española, las Normas APA en su sexta edición (2018) y todo lo relacionado con la normativa lingüística. Puede ser presentado como requisito de graduación.

Atentamente,

Sandra M. Aguilar M.

Bachiller Sandra María Aguilar Molina
Cédula 401350928
Carné de Colegio de Licenciados y Profesores en Letras, Filosofía, Ciencias y Arte # 9605
Asociación Costarricense de Filólogos # 246
Correo: sandraaguilar2009@gmail.com
Teléfonos: 22380346/ 70674854

AGRADECIMIENTOS

El presente trabajo se lo agradecemos, principalmente, a DIOS por ser nuestra guía en la vida, y a nuestros padres, abuelos, por habernos apoyado incondicionalmente, pese a las dificultades e incovenientes que se nos presentaron en el ciclo de estudio.

Agradecemos a nuestra profesora de proyecto de graduación, Floribeth Vindas Parra, quien, con su experiencia y conocimiento, nos orientó en nuestro proceso de investigación.

También agradecemos a todos los docentes que, con su conocimiento, sabiduría y apoyo, nos motivaron a seguir siempre hacia delante en nuestro desarrollo como profesionales de la Universidad Técnica Nacional.

Finalmente, nuestro profundo agradecimiento a Jonathan Vindas Benavides y a todas las autoridades y personal del Benemérito Liceo José Martí, por confiar en nosotros y permitirnos realizar todo el proceso investigativo, que conlleva a nuestro Trabajo Final de Graduación, en su centro educativo.

DEDICATORIA

Este proyecto de graduación se lo dedicamos a Dios ya que, día con día, nos inspira a tratar de cumplir nuestras metas.

A nuestros padres y abuelos, que, con su trabajo, amor y sacrificio, nos han ayudado en todos estos años lectivos, gracias a ellos hemos logrado llegar donde estamos y por ellos hoy somos personas muy capaces.

A todos los profesores, que ,a lo largo de nuestra vida, han dejado una semilla y nos han inculcado valores y diversos conocimientos.

A todas aquellas personas, que nos motivaron a seguir y finalizar este trabajo.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Este proyecto de investigación denominado "**Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República**", desarrollado por los estudiantes Isaac Alejandro Arguedas Leiton, Luis Gerardo Barquero Aguilar y Marcos Daniel Herrera Madrigal de la Universidad Tecnica Nacional de Costa Rica para optar por el grado de Licenciatura en Ingeniería en Tecnologías de Información, tiene como objetivo analizar la red administrativa del Benemérito Liceo José Martí, de acuerdo con lo establecido por las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República, con la finalidad de gestionar la seguridad física de los dispositivos de dicha red.

En esta investigación, se utiliza el enfoque mixto, debido a esto se recolectan diversos datos a través de un cuestionario a los funcionarios administrativos, también se realiza una observación en las instalaciones, se aplica un cuestionario y entrevista al encargado de Tecnologías de la Información de la institución.

A través de los datos obtenidos en esta investigación, se aportan criterios importantes en torno a la seguridad de la red física administrativa, el resultado más relevante es que no cumplen con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información, que dicta la Contraloría General de la República, motivo por el cual se propone que dicha institución se apropie de las mencionadas normas.

Con base en lo mencionado anteriormente, se realizan dos propuestas, una nombrada “Reglamento para la gestión de la red física administrativa del Benemérito Liceo José Martí” y la otra denominada “Plan de contingencia”, ambas enfocadas en las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República.

Para hacer referencia a la presente investigación se puede utilizar las siguientes palabras claves: **Red administrativa Liceo José Martí, Análisis de la gestión de la seguridad del hardware, Seguridad del Hardware, Análisis de la red administrativa del Liceo José Martí, Gestión de red Liceo José Martí.**

CAPÍTULO I

INTRODUCCIÓN

1.1. Introducción

A continuación, se presenta el proyecto “Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República”, en el cual se realiza una investigación previa de la red administrativa de la institución con el fin de recolectar información para el desarrollo de esta.

En este trabajo, se pueden encontrar términos relacionados con las redes informáticas y el uso de las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República. Asimismo, hay información del Benemérito Liceo José Martí, como su ubicación y misión, entre otros.

Además, se presenta el marco metodológico, en el cual se destaca la utilización del enfoque mixto, así como el sujeto, la muestra y los instrumentos utilizados para el desarrollo de esta investigación. Con base en estos últimos, se recolecta la información, se realiza el análisis y la interpretación de dichos resultados. A partir de eso, se realizan las conclusiones, recomendaciones y se hace una propuesta dirigida a la red física administrativa, una que tiene por nombre “Reglamento para la gestión de la red física administrativa del Benemérito Liceo José Martí” y un “Plan de contingencia”, tomando en cuenta los Capítulos I “Normas de aplicación” y IV “Prestación de servicios y mantenimiento” de las Normas

Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República.

1.2. Justificación

El análisis investigativo es una de las profesiones más antiguas, su existencia data de épocas lejanas, de la civilización griega. Sus antecedentes se pueden encontrar a finales de la antigua Grecia.

El análisis informático se basa en la recolección de la información relevante a los procesos informáticos por analizar, con la finalidad de estandarizar su funcionamiento y obtener una idea concreta de cómo funcionan todos los procesos ligados al área de tecnologías de la información. Sin embargo, el personal encargado de la auditoría informática también realiza pruebas en apoyo a otras áreas, donde exista flujo de información electrónica.

Un estudio de hardware en las redes informáticas consiste en una revisión del estado de todos los componentes físicos de la red de una organización, esta sirve para detectar, de manera proactiva, las vulnerabilidades presentes en los equipos, tanto internos como externos; además, la falla de administración e instalación de estos.

Es recomendable realizar un análisis informático en instituciones, las cuales dependen de la tecnología, para llevar a cabo su labor, con el fin de determinar los problemas, que puedan amenazar las redes, y, así, resguardar la integridad de los equipos y su funcionamiento óptimo.

Gracias al análisis, que se realiza, se obtiene un conocimiento completo de la red en cuanto al área física y, a su vez, se conoce el estado general de toda la infraestructura de red física informática del sector administrativo.

Debido a la importancia de la administración y gestión de redes, se lleva a cabo este análisis, ya que algunas instituciones no cuentan con personal que analice la seguridad y el funcionamiento de las redes; estas pueden encontrarse expuestas a los peligros que repercutan negativamente en su funcionamiento.

Esta averiguación busca analizar y determinar el hardware de la red administrativa del Benemérito Liceo José Martí, con el fin de entender plenamente su funcionamiento a partir del conocimiento adquirido como informáticos, dan, así, a conocer el estado actual de lo analizado en la institución.

1.3. Planteamiento y delimitación del problema de la investigación

1.3.1. Formulación del problema

El Benemérito Liceo José Martí, actualmente, es una de las instituciones educativas más importantes del área de Puntarenas, esta alberga gran cantidad de estudiantes, por ello, se requiere de suficiente personal administrativo, el cual realice todos los procesos en la institución para que los estudiantes reciban sus clases con normalidad.

Dicha institución realiza sus procesos administrativos a través de dispositivos tecnológicos, que trabajan mediante una conexión de red. Debido a esto, la red física administrativa de la institución es de suma importancia en todos los procesos, que realiza el sector administrativo, por lo que la seguridad en torno

a esta debe ser prioritaria para llevar a cabo todas las labores cotidianas de la institución.

En la actualidad, es de importancia enfocarse en los buenos hábitos del uso de la plataforma y en la seguridad para que el uso de esta no se vea interrumpida debido a problemas relacionados con el uso inadecuado de la red física. De no implementar las medidas adecuadas, se podría ver afectada la red administrativa y, por ende, se paralizarían los servicios administrativos, que ocasionan retrasos en sus funciones.

Debido a todo lo descrito anteriormente, la seguridad de la red física administrativa es fundamental para la institución, por ello surge esta investigación en busca de asegurar dicha red, según lo que establece las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República.

1.3.2. Sub preguntas

Con base en lo descrito en la formulación del problema, se generan las siguientes interrogantes.

1. ¿Cómo funciona, actualmente, la red física administrativa de la institución?
2. ¿Cuál es la normativa a la que se apega la institución para velar con la continuidad de los servicios de la plataforma?
3. ¿Qué tanto se acerca la normativa encontrada en la institución a la utilizada para realizar la investigación?

4. ¿Cuál es la planificación estratégica empleada en la red?
5. ¿Cómo es la distribución de los recursos de la red física administrativa?
6. ¿Qué características posee la red física administrativa de la institución?

1.4. Alcances y limitaciones

1.4.1. Alcances

Esta investigación pretende realizar un análisis profundo de la seguridad física de los dispositivos de la red administrativa del Benemérito Liceo José Martí; se toman como base investigativa las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República.

Para ello, se utilizan los Capítulos I “Normas de aplicación” y IV “Prestación de servicios y mantenimiento” de las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República.

1.4.2. Limitaciones

Las limitaciones de la investigación del análisis de la seguridad de los dispositivos físicos son las siguientes.

- El análisis es realizado únicamente en la red administrativa del Liceo Diurno José Martí.
- El periodo de recolección de información está comprendido en el tercer cuatrimestre del año 2019.
- Se limita a los datos que proporcione el personal del Liceo Diurno José Martí.

- Se enfoca, únicamente, en los siguientes capítulos de las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República.
    - Seguridad física y ambiental: Punto 1.4.3 del Capítulo I “Normas de aplicación general”.
    - Administración y operación de la plataforma tecnológica: Punto 4.2 del Capítulo IV “Prestación de servicios y mantenimiento”.

1.5. Objetivos

1.5.1. Objetivo general

Analizar la gestión de la seguridad física de los dispositivos de la red Administrativa del Benemérito Liceo José Martí, de acuerdo con las Normas Técnicas para la Gestión y Control de las Tecnologías de Información por la Contraloría General de la República, durante el tercer cuatrimestre del año 2019.

1.5.2. Objetivos específicos

- Investigar la manera en que se realiza el control de acceso de los dispositivos físicos de la red administrativa del Benemérito Liceo José Martí, a través de una encuesta aplicada al personal administrativo.
- Reconocer la forma en que se desarrolla la administración y control de plataformas de la red administrativa del Benemérito Liceo José Martí, mediante una encuesta aplicada al personal administrativo.

- Contrastar las políticas de control de acceso a los dispositivos físicos, así como la administración y control de las plataformas tecnológicas de la red administrativa del Benemérito Liceo José Martí, con lo establecido por las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República durante el tercer cuatrimestre del año 2019.

1.6. Situación actual

Los antecedentes relacionados con el enfoque de la investigación son los siguientes.

En el año 2012, Daniel Alberto Gámez Prieto, de la Universidad Libre de Colombia, desarrolla un estudio denominado Metodología para el análisis y diseño de redes fundamentados en ITIL 4, para empresas de servicio, en el cual plantea “una metodología para el desarrollo eficiente de un análisis y diseño de redes, tomando como referencia las prácticas definidas en los libros de estrategia […] y diseño de servicios de ITIL”. (Gámez, 2012, p.17)

Hace hincapié que ITIL debe estar implementado para disminuir “los inconvenientes en infraestructura, […] lo cual significaría una solución tangible a los problemas de administración de servicios, infraestructura, de información y de seguridad”. (Gámez, 2012, p.17).

La evolución en la definición de procesos planteados en las prácticas de ITIL ha permitido dar un enfoque diferente para el análisis y diseño

> de red, permitiendo así una mejor comunicación entre el área de TI y el usuario final.
>
> ITIL define lineamientos, que permiten asegurar la calidad, continuidad del servicio, disminución de costos sin depreciar el valor organizacional. (Gámez, 2012, p.75).

En el año 2014, Edison Oswaldo Rosero Álvarez, de la Universidad Central del Ecuador, realiza una indagación denominada “Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado”, en esta investigación el autor hace énfasis en la seguridad de la red LAN, por lo cual indica que

> la aplicación de la metodología MAGERIT de Análisis y Gestión de Riesgos de Sistemas de Información permitirá conocer los riesgos y amenazas a las que se encuentra expuesta la red LAN de la organización, y sobre todo se podrá saber el impacto que causaría a cada uno de los activos, en el caso de que las amenazas se llegaran a materializar. (Rosero, 2014, p.XIV)

Además, recalca que “las tecnologías de la información (TI) son muy fundamentales en las organizaciones, ya que su más valioso activo es la información, que estas manejan, y es, por ello, que se debe brindarles la seguridad correspondiente”. (Rosero, 2014, p.1)

A través de su estudio, Rosero determina que

> los activos: switch de Distribución, switch de acceso, switch de capa 2, Firewall, [...] son los activos con un mayor nivel de riesgo en la organización, debido a la falta de implementación de salvaguardas de seguridad como recomiendan los estándares y código de buenas prácticas para la Gestión de la Seguridad de la Información. (Rosero, 2014, p.119)

Menciona que la Contraloría General del Estado “cuenta con un plan de seguridad de la información, pero el personal responsable no lo ha actualizado, por lo que existiría una probabilidad media en que las amenazas se materialicen”. (Rosero, 2014, p.119)

La seguridad de los dispositivos físicos es de suma importancia para evitar que estos se dañen o tengan vulnerabilidades, que puedan afectar la funcionalidad de la red de las empresas.

CAPÍTULO II

MARCO TEÓRICO

REFERENCIAL

2.1. Marco teórico

> El marco teórico consiste en la recopilación de antecedentes, investigaciones previas y consideraciones teóricas donde se sustenta un proyecto de investigación, análisis, hipótesis o experimento, permitiendo, así, la interpretación de los resultados y la formulación de conclusiones.
>
> El marco teórico, también llamado marco de referencia, es el soporte conceptual de una teoría o de los conceptos teóricos, que se utilizan para el planteamiento del problema de un proyecto o una tesis de investigación. (Significados, 2018, párr. 2)

En el siguiente apartado, se definen los diferentes elementos concernientes al contexto del tema en desarrollo, con la finalidad de esclarecer las diversas terminologías por emplearse, coadyuvando a que el lector tenga plena conciencia de lo expresado en la lectura.

2.2. Telecomunicaciones

El arte de las telecomunicaciones se lleva a cabo en el momento de realizar comunicaciones con personas o servicios, que se encuentran a grandes distancias, actualmente, existen diversos tipos de comunicaciones, que permiten interconectar el mundo por medio del internet, teléfono, radio y telefonía, los cuales pueden trasmitirse en tiempo real, logrando que toda la información llegue a su destino predestinado dentro de la red mundial.

> Las telecomunicaciones realizan su aparición en el año 1837, gracias a Samuel Morse, quien es el creador del primer telégrafo. Este es el primer sistema digital de comunicaciones, permitía la transmisión de la información a distancia, a partir del invento de Morse, se desarrolla un amplio campo tecnológico denominado “telecomunicaciones”. (Joskowicz, 2015, p.3)

2.3. Red de computadoras

> Una red de computadoras es un elemento indispensable para asegurar la comunicación entre dos o más computadoras, lo cual permite el intercambio de datos entre estas. No solo las empresas pueden beneficiarse de las potencialidades de las redes de computadoras. A nivel doméstico, los usuarios también podrían aprovechar sus bondades para compartir música, películas y cualquier otra información que sea de interés. De este modo, las redes informáticas constituyen uno de los avances tecnológicos más relevantes en la actualidad. (Sancler, s.f., párr.1)

Se refiere a grandes volúmenes de ordenadores interconectados con la cualidad de funcionar entre sí, permiten compartir datos de forma ágil y segura, a nivel empresarial este avance ha generado que los servicios brindados en las empresas sean cada vez más rápidos y eficaces a la hora de emplearlos.

2.3.1. Tipos de redes

Las redes se clasifican en diversos tipos, los cuales son los siguientes.

2.3.1.1. Redes de difusión y redes punto a punto

> Se consideran redes de difusión aquellas en las que cualquier dispositivo, que comparta el medio y emita una señal, pueda ser recibida por todas las estaciones.
>
> Estos sistemas suelen permitir la difusión de una transmisión a todos los computadores, que conforman la red, cuando esta lleva, en su cabecera, un código específico en el campo de la dirección, a esta modalidad de difusión se le denomina *broadcasting*. (Rodríguez, 2014, p.31)

La problemática principal de las redes de difusión es que la captura de paquetes en el momento de transmitirse podría provocar un flujo de información crítico en cualquier ámbito.

Las redes de punto a punto son establecidas para tener una comunicación directa con un ordenador o red en específico, como resultado se obtiene mayor seguridad, ya que se restringe la cantidad de ordenadores con la posibilidad de detectar lo que se transmite por la red.

2.3.1.2. Redes LAN, MAN y WAN

i. Redes LAN

Las redes de área local “Son redes privadas de pocos kilómetros. Por ejemplo, una red en el hogar, una oficina o un centro educativo. Se utilizan para conectar PCs y algunos periféricos y suelen operar a velocidades de entre 10 y 100 Mbps”. (Bellido, 2014, p.19)

Este tipo de red está orientada a un área específica, ya que su extensión es limitada.

ii. Redes MAN

La red de área metropolitana en adelante MAN:

> es una red que suele comprender desde varios edificios a una ciudad entera. Interconecta varias LAN entre sí usando conexiones de alta capacidad. Para la implementación de este tipo de redes, es necesaria alguna compañía de comunicaciones que proporcione servicios de conexión. (Castaño y López, 2013, p.18)

La MAN está enfocada en poblaciones mucho mayores en comparación con las LAN, por lo cual los proveedores de servicios pueden optar por poseer redes MAN dentro de sus controles y, así, ofrecer el servicio a los usuarios.

iii. Redes WAN

> Las redes de área extensa, en adelante WAN “es una red que interconecta ciudades entre sí e incluso todo un país. Normalmente, son creadas por los proveedores de servicio de Internet (ISP) para proporcionar conectividad de acceso privado a sus clientes”. (Castaño y López, 2013, p.18)
>
> Las redes WAN son redes compuestas por una agrupación de subredes en varias regiones, estas logran la conexión de dispositivos ubicados en zonas lejanas.

2.3.1.3. Ámbito de datos en los tipos de redes

Existen dos tipos de clasificaciones en cuanto al ámbito de los datos, que transitan en una red, estos poseen las siguientes clasificaciones.

i. Redes públicas de datos

En las redes públicas de datos:

> los nodos acceden a la red, utilizando la dirección IP que le proporciona su proveedor de servicio (ISP). Cuando los equipos de una red pública se conectan a Internet, forman parte íntegra de ella, siendo perfectamente visibles por cualquier otro equipo del mundo que también esté conectado a Internet. (Castaño y López, 2013, p.18)

En estas redes, sus dispositivos navegan a través de internet por medio de una sola IP pública, la cual es visible en internet.

ii. Redes privadas de datos

Las redes privadas de datos

> son un tipo de redes locales, que usan unas direcciones IP especiales, que se definen como privadas. Los equipos que forman parte de esta red no pueden acceder realmente a Internet y necesitan de un *router* que les haga de traductor entre sus direcciones IP privadas y las direcciones IP públicas, que circulan por Internet. Estas redes existen para intentar evitar que el número de direcciones IP públicas se agote. (Castaño y López, 2013, p.19)

En este caso, los dispositivos de la red utilizan direcciones IP privadas, por lo tanto, necesitan de otro equipo para realizar la traducción de las direcciones IP privadas a públicas, con el fin de poder navegar en internet.

2.3.1.4. Redes de conmutación

> La conmutación en las redes es la forma en la que se comunican las redes en el momento de establecer un camino de dos puntos, este se compone por un emisor y un receptor a través de los equipos de transmisión. (EcuRed, s.f., p.1)

Los diferentes caminos, que deben tomar los paquetes de comunicación se denominan nodos, que permiten trazar el recorrido que debe realizar el paquete para llegar a su destino y, así, poder realizar la conmutación,

entre los servicios existentes que utilizan las técnicas para conmutar, se encuentran la telefonía y los datos.

Entre las técnicas para conmutar redes, se encuentran las siguientes.

i. Redes de conmutación de circuitos

> La conmutación de circuitos se basa en la creación de un circuito físico entre los dos interlocutores de la red. Este circuito físico se establece antes de transmitir cualquier tipo de información y está formado por diferentes enlaces entre los nodos.
>
> En el momento de iniciarse una comunicación, el emisor debe comprobar que el destinatario del mensaje se encuentre disponible y, en caso de ser así, localizar una ruta libre dentro de la red, que incluya los respectivos conmutadores y enlaces entre este y el destinatario.
>
> Una vez establecido el camino y transmitida la información, la red debe ser capaz de restablecer los recursos utilizados y dejarlos disponibles para las siguientes, comunicaciones. (Rodríguez, 2014, pp. 9-10)

La red de conmutación por circuitos comprueba que el receptor esté disponible y busca una ruta libre para realizar la comunicación, de esta manera transmite la información, por ejemplo: en el caso de una (red telefónica conmutada RTC), se

establece un canal dedicado de comunicación para, así, poder transmitir el flujo de voz por medio del recurso de transmisión establecido durante la conexión.

ii. Redes de conmutación de paquetes

Las redes de conmutación de paquetes surgieren lo siguiente:

> con el fin de mejorar el rendimiento en la conmutación de circuitos, se diseña la conmutación de paquetes, con los siguientes objetivos de optimizar el empleo de los canales de comunicación.
>
> - Interconectar terminales con diferentes velocidades.
> - Crear conexiones simultáneas sin reserva de recursos. (Rodríguez, 2014, p.12)

Este tipo de conmutación permite que la entrega de paquetes se efectúe con seguridad, esto debido a, que, dentro del encabezado de la trama, se envía la dirección específica a la cual se destina el paquete, cabe recatar que el emisor deja en espera del receptor un mensaje de recibido sobre el paquete que se envía. Lo fundamental de este tipo de red es que la información se divide en paquetes, que pueden tomar diferentes rutas hasta llegar a su destino, esto la hace diferente a la conmutación por circuito.

2.3.2. Topologías de red

La topología de la red “es la propiedad que indica la forma física de la red, es decir, el modo en que se disponen los equipos y el sistema de cableado que los interconecta para cumplir su función”. (Abad, 2013, p.13)

Es la forma o diseño de cómo está construida físicamente la red, esto incluye la distribución y localización de los cables, que permiten la interconexión de los dispositivos físicos.

Las topologías se dividen en distintos tipos, las cuales son las siguientes.

2.3.2.1. Topología en estrella

En las infraestructuras de red que poseen su topología en estrella,

> las estaciones se conectan entre sí a través de un nodo especialmente privilegiado, que ocupa la posición central de la red, y que forma con el resto de las estaciones una estrella. A este nodo, se le denomina estación concentradora de la estrella. (Abad, 2013, p.13)

La topología en estrella es aquella en la cual se utiliza un dispositivo físico como eje central, por ejemplo, un conmutador, a este se conectan los demás equipos de la red, formando la figura de una estrella.

2.3.2.2. Topología en anillo

La topología en anillo “conecta todos sus equipos en torno a un anillo físico. Tampoco presenta problemas de congestión de tráfico; sin embargo, una rotura del anillo produce el fallo general de la red”. (Abad, 2013, p.13).

Es aquella donde los dispositivos se conectan uno tras otro a través de un cable físico, forman un anillo, por lo que cada computador o equipo posee un receptor y transmisor para lograr el paso de información.

2.3.2.3. Topología en bus

Los dispositivos de la topología

> en bus se conectan a una única línea de transmisión (bus), que recorre la ubicación física de todos los ordenadores. Esta red es muy simple en su funcionamiento, sin embargo, es muy sensible a problemas de tráfico o a las roturas de los cables.
>
> El medio de transmisión que forma la red es un único bus multiacceso compartido por todos los nodos, por lo que se debe establecer una contienda para determinar quién tiene derechos de acceso a los recursos de comunicación en cada instante. Este sistema de contienda determina el tipo de red. (Abad, 2013, p.13)

La topología en bus consta de un solo cable físico, al cual se conectan todos los dispositivos de red, por lo que una falla en dicho cable puede ocasionar pérdida de la conexión. Para la comunicación entre los

equipos, estos tienen que escuchar si nadie está transmitiendo para, así, pasar su información a través del enlace.

2.3.3. Arquitectura de red

La arquitectura de red engloba a los distintos protocolos de comunicación, los cuales se encargan de transmitir la información a través de la red, para ello, los datos viajan entre distintas capas, las cuales se encargan de que la información sea convertida, transportada y que llegue correctamente a su destino.

2.4. Modelo de referencia OSI/ISO

OSI es una “arquitectura de capas para redes de ordenadores y sistemas distribuidos, propuesta por la ISO como estándar de interconexión de sistemas abiertos”. (Abad, 2013, p.18)

El modelo de interconexión de sistemas abiertos es una arquitectura en capas, que se encarga de transportar los datos entre los distintos dispositivos que componen la red.

El modelo OSI se divide en siete capas, las cuales son las siguientes.

2.4.1. Capa física

La capa física se ocupa de definir las características mecánicas, eléctricas, funcionales y de procedimiento para poder establecer y liberar conexiones entre dos equipos de la red. Es la capa de más bajo nivel, por tanto, se ocupa de las transmisiones de los bits expresados como señales físicas. (Abad, 2013, p.19)

Es la encargada de transmitir la información en el medio de comunicación, transforma los datos en bits para que sean comprendidos por las computadoras y, de esta forma, transmitirlos de un lugar a otro.

2.4.2. Capa de enlace

Esta capa se encarga de la “Transmisión de tramas (bloques de datos) para proporcionar un servicio seguro de transferencia de datos a través del enlace físico”. (Universidad de Granada, s.f., p.14)

Dicha capa lleva a cabo la transferencia de la información entre el computador y la red, con seguridad y sin fallas o errores durante el envío.

2.4.3. Capa de red

La capa de red transmite “paquetes a través de la subred. Proporciona independencia a los niveles superiores respecto a las técnicas de conmutación y de transmisión utilizadas para conectar sistemas”. (Universidad de Granada, s.f., p.15)

Los protocolos contenidos en esta capa “especifican el direccionamiento y los procesos que permiten empaquetar y transportar los datos de la capa de transporte”. (Introducción, 2018, párr. 2)

El nivel de red de OSI es la encargada de transmitir y direccionar los distintos datos, que son enviados hacia destinos ubicados en redes distintas.

2.4.4. Capa de transporte

Es la capa que se encarga de la “transición entre los niveles orientados a la red (subred) y los niveles orientados a las aplicaciones”. (Abad, 2013, p.20)

> Los procesos que se describen en la capa de transporte del modelo OSI aceptan los datos de la capa de aplicación y los preparan para el direccionamiento en la capa de red. [...] La PC de origen se comunica con una PC receptora para decidir cómo dividir los datos en segmentos, cómo asegurarse de que ninguno de los segmentos se pierda y cómo verificar si llegan todos los segmentos. (Introducción, 2018, párr. 2)

La capa de transporte proporciona “Seguridad, transferencia de datos entre puntos finales, multiplexación de conexiones y control de flujo de origen-destino”. (Universidad de Granada, s.f., p.16)

El nivel de transporte de OSI se encuentra ubicada entre la capa de red y sesión y es la encargada de transportar los datos desde el origen al destino, los divide en segmentos, los cuales se verifican a la hora de su llegada y se vuelven a unir, asegurando que la información llegue completa.

2.4.5. Capa de sesión

La capa de sesión realiza el “Control de la comunicación entre aplicaciones (establecimiento gestión y cierre de sesiones [conexiones entre aplicaciones])”. (Universidad de Granada, s.f., p.16)

La capa de sesión del modelo OSI “permite el diálogo entre emisor y receptor, estableciendo una sesión, que es el nombre que reciben las conexiones en esta capa”. (Abad, 2013, p.21)

Es la que aprueba y finaliza la comunicación entre las computadoras o dispositivos, al mismo tiempo, administra el intercambio de los datos, que se realizan entre los hosts.

2.4.6. Capa de presentación

> La capa de presentación se ocupa de la sintaxis y de la semántica de la información, que se pretende transmitir, es decir, investiga en el contenido informativo de los datos. Esto es un indicativo de su alto nivel en la jerarquía de capas. (Abad, 2013, p.21)

Esta capa posee “Independencia respecto a las diferencias en la representación de los datos (codificación, compresión, criptografía…)”. (Universidad de Granada, s.f., p.16)

Su función es la representación de los datos, que se quieren enviar, asegurando que la información sea reconocible e interpretada correctamente por el host de destino.

2.4.7. Capa de aplicación

La capa de aplicación es donde “se definen los protocolos que utilizarán las aplicaciones y procesos de los usuarios. La comunicación se realiza utilizando protocolos de diálogo apropiados”. (Abad, 2013, p.22)

Proporciona servicios a los usuarios, por lo que se utiliza para el intercambio de la información entre las aplicaciones, que se ejecutan en los distintos dispositivos de la red.

2.5. Modelo de referencia TCP/IP

> TCP/IP consiste en una compleja arquitectura de red desarrollada en los años 70 por el Departamento de Defensa de Estados Unidos, que incluye varios protocolos agrupados en capas, son, sin lugar a dudas, la más utilizada en el mundo, ya que es la base de las comunicaciones de Internet.
>
> Su función principal es enlazar y comunicar distintos equipos informáticos en redes de área local (LAN) y área extensa (WAN). TCP determina el control del flujo y los acuses de recibo del intercambio de paquetes, mientras IP identifica el origen y destino según se envían los paquetes por la red. (Bellido, 2014, p.7)

Este modelo combina varias de las capas del modelo OSI, posee protocolos los cuales permiten la comunicación entre los dispositivos de la red.

El modelo TCP/IP se divide en cuatro capas, las cuales son las siguientes.

2.5.1. Capa de acceso a la red

La capa de acceso a la red

> Puntualiza a los hosts, que se tienen que conectar a la red mediante el mismo protocolo para que puedan recibir paquetes IP. Por otra parte, también se encarga de la asignación de direcciones IP a las direcciones físicas y del encapsulamiento de los paquetes IP en tramas. (Bellido, 2014, p.10)

Es la capa inferior de dicho modelo, se encarga de que los paquetes lleguen correctamente al medio físico, asegurando la transmisión de la información.

2.5.2. Capa de interred (internet)

La capa de internet

> Es la capa más importante de la arquitectura. Su objetivo es permitir que los hosts envíen paquetes (información) a la red y los hagan viajar de forma independiente a su destino. Es posible que estos lleguen desordenados, ya que durante el viaje pueden atravesar distintas redes, pero la función de ordenarlos corresponde a capas más altas. (Bellido, 2014, p.12)

Su función es permitir que los equipos puedan realizar el envío de sus paquetes desde cualquier red y que estos lleguen de forma correcta hacia el otro computador, independientemente de las rutas que hayan tomado para llegar a su destino.

2.5.3. Capa de transporte

> La capa de transporte se encarga de establecer una conversación entre el origen y el destino sin importar el contenido de los datos. Entre sus funciones, se encuentran la corrección de errores, el control de flujo y la confiabilidad de la conexión. (Bellido, 2014, p.13)

Esta capa se encarga de brindar la comunicación entre los dispositivos de la red, asegura un transporte confiable.

2.5.4. Capa de aplicación

En esta capa “se implementan las funcionalidades, que se pretenden alcanzar, manejando aspectos como la representación, codificación y control del diálogo”. (Bellido, 2014, p.13)

La capa de aplicación de TCP/IP engloba a la capa de sesión, presentación y aplicación de OSI, por lo que se encarga de la conexión y finalización entre las computadoras, representa los datos de forma reconocible y proporciona el intercambio de información entre los programas, que utilizan los usuarios.

2.6. Control de Acceso

El control de acceso se puede definir como

> un sistema electrónico, que restringe o permite el acceso de un usuario o grupo de usuarios a un área específica, valida la identificación por medio de diferentes tipos de lectura (clave por teclado, lector de tarjetas, biometría…) y, a su vez, controlando el recurso (puerta, armario, torniquete…) por medio de un dispositivo eléctrico como un electroimán, pestillo o motor. (Mora, 2016, p.10)

El control de acceso consiste en todos los pasos a seguir para poder comprobar la identidad de quién solicita acceso y autorizar a qué recursos tiene permiso, esto por medio de diversos controles físicos y lógicos, los cuales permiten que la entrada sea efectuada con su debido control.

- **Acceso físico**

  Esto significa poder ver, tocar y modificar una computadora y sus dispositivos. Las instalaciones de servidores, usualmente, toman este tipo de acceso muy en serio y se cierra bajo llave la habitación del servidor. El acceso a las computadoras de escritorio no siempre está tan controlado, incluso con las laptops, que pueden llevarse a cualquier lado. (Parson, s.f., párr. 2)

- **Acceso lógico**

  En general, el acceso lógico es un acceso en red a través de la intranet de la compañía o de internet. Los "puertos" son distintos tipos de accesos lógicos para entrar, acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información de identidad, con claves o direcciones de IP (Protocolo de internet) en una lista permitida. (Parson, s.f., párr. 3)

2.6.1. Tipos de control de acceso

Son todos aquellos mecanismos, que se utilizan para controlar el acceso a los dispositivos, entre los cuales se encuentran los siguientes.

- **Controles físicos**

Los controles de acceso físico son **“**aquellos que implementen medidas de seguridad física, por ejemplo, cerraduras electrónicas, sistemas de acceso biométrico…”. (Santín, 2018, p.42).

Son las medidas, que se encargan de asegurar la infraestructura física, por medio de diferentes sistemas de acceso, entre los controles más comunes están los siguientes.

- **Controles por contraseña:** Los sistemas de control de acceso por contraseña es un sistema que

  > Crean una seguridad contra los usuarios no autorizados, el sistema de seguridad solo puede confirmar que la contraseña es válida, y si no el usuario está autorizado a utilizar esa contraseña. Es la razón por la que normalmente deben mantenerse en secreto ante aquellos a quien no se le permite el acceso. (Control de acceso, s.f., párr. 6)

  Es un sistema que realiza la identificación de las personas autorizadas por medio de una contraseña, que, únicamente, conoce quién está autorizado.

- **Controles por token de seguridad:** Los controles de acceso por token de seguridad es un sistema, que utiliza un dispositivo que “puede ser en forma de una tarjeta inteligente o puede estar incorporando en un objeto utilizado comúnmente, como un llavero”. (Control de acceso, s.f., párr. 8)

  El token de seguridad es un dispositivo que identifica al propietario, por ejemplo, un llavero o teléfono celular. Existen varios tipos de token de seguridad, entre las comunes son las tarjetas RFID.

- **Controles por sistemas biométricos:** Los controles de acceso por sistemas biométricos utilizan características físicas de los usuarios para poder identificarlos, lo cual dificulta que, en este sistema, se pueda falsificar la identidad de alguien autorizado.

  Los sistemas biométricos se pueden clasificar en los siguientes.

  - Fisiológicos: huella dactilar, iris, retina, cara, geométrica de la mano, huella palmar, estructuras de las venas, estructura de la oreja, termografía facial.
  - Conductuales: voz, escritura, firma manuscrita, modo de teclear, modo de andar.

  (Control de acceso, párr. 11-12)

- **Controles técnicos y lógicos**

  Los controles de acceso técnico y lógico, usualmente, implementan “medidas de carácter tecnológico, como sistemas de detección de intrusos, seguridad de las aplicaciones y sistema operativo…”. (Santín, 2018, p.42)

  En este tipo de control, generalmente, son las medidas de seguridad, que se implementan en los sistemas tecnológicos, como puede ser software antivirus, cortafuegos, detectores de intrusos, usados para proteger los sistemas de amenazas interiores y exteriores.

- **Controles administrativos**

  Los controles de acceso administrativos son los que “suelen determinar, en función de la política de seguridad, las configuraciones que deben cumplir el resto de los controles”. (Santín, 2018, p.42)

  Los controles administrativos definen las medidas a seguir mediante una política de seguridad.

2.7. Tecnologías de información

Son una herramienta de proceso de información básica, estas se derivan de los primeros ordenadores existentes y de la informática, los cuales hacen su aparición el siglo pasado.

Las tecnologías de información son “un conjunto de tecnologías requeridas para el almacenamiento, recuperación, proceso y comunicación de la información”. (Martin, Olmedo y Andoney, 2017, p.1)

Todo el conjunto de tecnologías es resultante de años de investigación en el campo de la informática, en la actualidad, un sinfín de conceptos son derivados de las tecnologías informáticas, estos dan paso a la modernización del mundo tal y como se conoce.

Las Tecnologías de la Información y la Comunicación en adelante TIC

> se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones. Es el conjunto de tecnologías, que permiten el acceso, producción, tratamiento y

> comunicación de información presentada en diferentes códigos (texto, imagen, sonido, video). (Ayala & Gonzáles, 2015, p.27)

Con respecto al término TIC, este

> contempla toda forma de tecnología usada para: crear, almacenar, intercambiar y procesar información en sus varias formas, tales como: datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquellas aún no concebidas. Su objetivo principal es la mejora y el soporte a los procesos de operación y negocios para incrementar la competitividad y productividad de las personas y organizaciones en el tratamiento de cualquier tipo de información. (Ayala & Gonzáles, 2015, p.28)

2.8. Normas

Según la Real Academia Española (s.f.), una norma es una "Regla que se debe seguir o que se deben ajustar las conductas, tareas, actividades…" (párr. I)

En informática, se entiende como norma todos los lineamientos o procesos a seguir para que los sistemas informáticos puedan funcionar de manera óptima y segura, algunos ejemplos de normas informáticas son las siguientes.

- **Normas ISO**

  Las normas ISO son un conjunto de documentos que

  > Especifican requerimientos, que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo. Hasta el momento, ISO (International Organization for Standardization) ha publicado alrededor de 19.500 normas internacionales, que se pueden obtener desde la página oficial de ISO. (ISOTools, s.f., párr. 3)

  Las normas ISO son un conjunto de pautas estandarizadas internacionalmente, que se recomiendan para que, independientemente de la actividad realizada, esta tenga un funcionamiento eficiente y eficaz.

- **Normas COBIT**

  Según ISACA (s.f.) las normas COBIT son

  > Un marco para el gobierno y la gestión de la información y la tecnología de la empresa, dirigido a toda la empresa. COBIT define los componentes y los factores de diseño para construir y mantener un sistema de gobierno de mejor ajuste. (párr. 4)

  Las normas COBIT brindan una serie de recomendaciones de cómo debería estar formada una organización en todos sus departamentos, en informática brinda un modelo de cómo se debería realizar una auditoria informática.

- **Normas técnicas para la gestión y el control de las Tecnologías de Información**

  Estas normas solamente aplican para las instituciones públicas de la República de Costa Rica que

  > Establecen los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tienen como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado. (Contraloría General de la República, 2007, p.2)

2.9. Dispositivos físicos

Son todos los elementos tangibles, que se pueden encontrar en una red informática, donde cada uno ellos tienen una función específica, por ejemplo, interconectar redes, enrutar, distribuir, entre otros. Entre los dispositivos físicos podemos encontrar los siguientes.

2.9.1. Dispositivos finales

Los dispositivos con los que las personas se familiarizan de forma usual “se denominan ‘dispositivos finales’ o ‘hosts’. Estos dispositivos forman la interfaz entre los usuarios y la red de comunicación subyacente”. (Dispositivos finales, 2018, párr. I)

Los dispositivos finales son todos los elementos físicos, que conforman el punto final de una red y, también, donde los usuarios tienen contacto con la red.

Algunos ejemplos de dispositivos finales son los siguientes.

- **Computadoras**

  Estaciones de trabajo, computadoras portátiles, servidores.

- **Dispositivos móviles**

  Teléfonos inteligentes, tabletas.

- **Teléfonos VoIP**

  Son teléfonos capaces de utilizar el protocolo de internet para la transmisión de voz, el término VoIP es un acrónimo de Voz sobre Protocolo de Internet (Voice Over Internet Protocol en inglés).

- **Conmutadores**

  > Un conmutador o *switch* es un dispositivo digital lógico de interconexión de equipos, que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. (Conmutador, s.f., párr. 1)

  Un conmutador es un dispositivo de red, cuya función es interconectar varios segmentos de una red, crea un canal entre el origen y destino de un paquete, y utiliza como identificador las direcciones MAC de cada equipo.

- **Enrutadores**

> Los ruteadores funcionan en la capa de red del modelo OSI y son más inteligentes que los puentes para enviar los paquetes entrantes a su destino final. Debido a que los ruteadores trabajan en la capa de red, cualquier conexión a través del ruteador requiere solo que las capas superiores utilicen los mismos protocolos, los ruteadores pueden traducir cualquiera de los protocolos de la capa 1-3 a cualquier otro protocolo de las capas 1-3. […] Los ruteadores se pueden conectar tanto con redes similares como diferentes. A menudo, se utilizan en los enlaces de las redes de área amplia (WAN).
>
> Los ruteadores también pueden determinar la ruta más corta para alcanzar un destino y la usan. Pueden realizar otros trucos con la finalidad de maximizar el ancho de banda de la red, y de forma dinámica, se ajustan a los problemas cambiantes o patrones de trafico de una red. (Ruteadores, s.f., párr. 1)

Los enrutadores (también conocidos como ruteadores o *routers*) son dispositivos de red más avanzados, con la capacidad de interconectar varias, estos son los encargados de enviar todos los paquetes hacia las redes externas, debido a su capacidad pueden crear rutas optimizadas para el trasiego de datos, mejorando el ancho de banda de las conexiones.

- **Puntos de acceso inalámbricos**

Según la Linksys (s.f.)

> Un punto de acceso es un dispositivo que crea una red de área local inalámbrica (WLAN), normalmente en una oficina o un edificio de grandes dimensiones. Un punto de acceso se conecta a un router, switch o hub por un cable Ethernet y proyecta una señal Wi-Fi en un área designada. (párr. II)

Un punto de acceso inalámbrico es un dispositivo capaz de conectar inalámbricamente varios dispositivos a la red, permitiendo cubrir una gran área sin la necesidad de instalar cables.

- **Repetidores**

> Es un dispositivo electrónico, que conecta dos segmentos de una misma red, transfiere el tráfico de uno a otro extremo, bien por cable o inalámbrico.
>
> Los segmentos de red son limitados en su longitud, si es por cable, generalmente, no superan los 100 M., debido a la pérdida de señal y la generación de ruido en las líneas.
>
> Con un repetidor, se puede evitar el problema de la longitud, ya que reconstruye la señal, eliminando los ruidos y la transmite de un segmento al otro. (Repetidor, s.f., párr. 1)

El repetidor es un dispositivo, que se encarga de retrasmitir las señales enviadas por un conmutador, enrutador o punto de acceso, debido a que las distancias de transmisión son limitadas, estos dispositivos ayudan a eliminar esta limitante, ya que ellos reconstruyen la señal y eliminan los problemas, que presentan, y las trasmite hacia el punto de destino.

CAPÍTULO III

MARCO CONTEXTUAL

3.1. Marco contextual

> El marco contextual o situacional de un proyecto de investigación describe el contexto y/o la situación en la que la investigación se va a realizar. Cuando el trabajo de investigación consiste en la formulación de un proyecto o en el diseño de un programa, el marco contextual o situacional es fundamental. (Ex Libris, s.f., p.1)

A continuación, se describe la institución en donde se realiza esta investigación, con el objetivo de tener claro el lugar y cómo se encuentra organizado.

3.2. Aspectos situacionales de la institución o empresa

3.2.1. Descripción de la empresa

El Benemérito Colegio Nocturno José Martí. Pertenece al Circuito N° 5 de la Dirección Regional de Enseñanza de Puntarenas; es creado en el año de 1941 por un grupo de puntarenenses visionarios, que, sienten la necesidad de fundar una institución educativa secundaria que ayude a hombres y mujeres de la provincia, para que puedan prepararse académicamente, mejorar su calidad de vida y contribuir en el desarrollo de la economía. Actualmente, tiene un terreno con un área de 5874.26 m.^{2} y está inscrito en el Registro Público a nombre de la Junta Administrativa del Liceo José Martí, Distrito Primero, Cantón Central, Provincia Puntarenas.

Pertenece al Ministerio de Educación Pública, goza de personería y cédula jurídica, compartidas con el Liceo Diurno José

> Martí y el Colegio Nocturno José Martí. Este centro educativo funciona de conformidad con principios constitucionales, leyes fundamentales, decretos, reglamentos y circulares, que se expiden y adoptan en el nivel nacional, regional o zonal y que rigen la vida institucional en sus aspectos administrativos, pedagógicos y en sus relaciones con la comunidad. (Dirección Regional Educación Puntarenas, s.f., párr. 1)

3.2.2. Ubicación geográfica

El Benemérito Liceo José Martí se encuentra ubicado en la provincia de Puntarenas, cantón Puntarenas, costado oeste de la Catedral de Nuestra Señora del Carmen.

3.2.3. Misión

La misión del Benemérito Liceo José Martí es

> Promover y propiciar un servicio educativo, eficiente y eficaz, que garantice el desarrollo integral del educando, mediante la motivación, profesionalización, capacitación y asesoría al personal docente y administrativo, sin dejar de lado el sentido de pertenencia (identidad) de padres de familia y toda la comunidad al proceso educativo. (Dirección Regional Educación Puntarenas, s.f., párr. 1)

3.2.4. Visión

La visión del Benemérito Liceo José Martí busca

> Dar una respuesta eficiente y eficaz al cliente interno y externo, mediante la oferta y los servicios, que se brindan, administrando técnica, pedagógica y jurídicamente el proceso de la enseñanza, para la búsqueda del desarrollo socioafectivo y vocacional de los sujetos. (Dirección Regional Educación Puntarenas, s.f., párr. 1)

3.2.5. Valores

El Benemérito Liceo José Martí “se regirá por los valores del profesionalismo, tolerancia, disciplina, responsabilidad, respeto, honestidad, lealtad y solidaridad”. (Dirección Regional Educación Puntarenas, s.f., párr. 1)

3.2.6. Organigrama

La siguiente imagen muestra la estructura organizacional del Benemérito Liceo José Martí. (Ver anexo #1)

CAPÍTULO IV

MARCO METODOLÓGICO

4.1. Marco metodológico

El marco metodológico es la explicación de los mecanismos por utilizar, por lo tanto, en este apartado, se describen las técnicas o métodos, que se aplican en la indagación.

> El marco metodológico […] se encarga de revisar los procesos a realizar para la investigación, no solo analiza qué pasos se deben seguir para la óptima resolución del problema, sino que también determina si las herramientas de estudio que se van a emplear ayudarán de manera factible a solucionar el problema. (Leguia, s.f., p.1).

Por lo tanto, determina los procedimientos utilizados en el análisis de la problemática de la investigación.

El marco metodológico posee distintos enfoques, que se utilizan con la finalidad de señalar el rumbo de la metodología de la investigación.

4.2. Enfoque cuantitativo

Este tipo de enfoque se basa en el análisis y comprobación de datos exactos, la información que se busca analizar proviene, generalmente, de números, por lo tanto, las preguntas, que se realizan en este enfoque, son de cantidades.

> El método cuantitativo se basa principalmente en los números y es una metodología que pretende tomar decisiones, entre varias opciones, usando las variables de información y datos. Es decir, la investigación

cuantitativa es un procedimiento de decisión, que trata de analizar y delimitar la asociación, la generalización y el objeto de los resultados que se obtienen al estudiar una población.

Generalmente, el método cuantitativo requiere de la utilización de recursos en el campo de la estadística para tratar los elementos numéricos. Esta metodología necesita que haya una relación numérica entre las variables del problema de investigación para poder delimitarlo con facilidad, así como para saber dónde empieza, qué dirección tiene y el tipo de elementos que lo conforman.

La investigación cuantitativa, también es conocida como racionalista, positiva o empírico-analítica, y tiene como finalidad obtener respuestas de la población a preguntas específicas. La información y los datos, que se analizan con el método cuantitativo por medio de encuestas, siempre son cuantificables con muestras numéricas (porcentajes, tasas, magnitudes…). (Sanz, 2017, párr. 2)

En el momento de analizar el enfoque cuantitativo, se señala que

El método cuantitativo utiliza preferentemente información cuantificable. Siguen un sistema metodológico con reglas y técnicas de investigación, con las cuales recopila información válida y confiable, necesaria para generar los datos que analiza a través de la mediación y del análisis estadístico. (Seas, 2017, p.346)

En este enfoque, se recolecta cierta cantidad de datos para realizar un estudio o análisis de una determinada investigación, trata de probar una hipótesis o teoría.

4.3. Enfoque cualitativo

El enfoque cualitativo se encarga de estudiar la realidad de las cosas, interpreta situaciones o fenómenos según la investigación, se basa en la calidad de las evidencias y, a la vez, se enfoca meramente en las prácticas.

> La investigación cualitativa es aquella donde se estudia la calidad de las actividades, relaciones, asuntos, medios, materiales o instrumentos en una determinada situación o problema. La misma procura lograr una descripción holística, esto es, que intenta analizar exhaustivamente, con sumo detalle, un asunto o actividad en particular. (Vera, s.f., p.1)

> Esta investigación proporciona alternativas para describir, interpretar y explicar los fenómenos ocurridos. Para ello, se toma en cuenta el contexto social y cultural en que se presenta. (Seas, 2017, p.347)

En la investigación cualitativa, se recolectan datos cualitativos sobre situaciones, manifestaciones, eventos, entre otros, con el fin de analizar las evidencias y obtener las conclusiones.

4.4. Enfoque mixto

En el siguiente párrafo, se describe el significado del enfoque mixto.

> Es un proceso que recolecta; analiza y vincula datos cuantitativos y cualitativos en un mismo estudio, o una serie de investigaciones para responder a un planteamiento del problema. Asimismo, el enfoque mixto puede utilizar los dos enfoques para responder distintas preguntas de investigación de un planteamiento de un problema. (Rivas, s.f., p.2).
>
> La característica principal de los métodos mixtos (MM) es la combinación de la perspectiva cuantitativa (cuanti) y cualitativa (cuali) en un mismo estudio. Cuando las preguntas de investigación son complejas, la combinación de los métodos permite darle profundidad al análisis y comprender mejor los procesos de enseñanza y aprendizaje. (Hamui-Sutton, 2013, p.212)

Surge como la combinación del enfoque cuantitativo y cualitativo en un mismo estudio, con el fin de tener un conocimiento más profundo sobre el tema, por lo tanto, permite una vía para realizar mejor la indagación y explotación de los datos.

4.5. Enfoque de la investigación

El enfoque de la investigación brinda la dirección, que se desea adoptar en el momento de desarrollar lo investigado.

La investigación tiene un enfoque mixto, debido a que permite realizar preguntas más complejas en el momento de efectuar los cuestionarios, que captan la información de los encuestados, con el fin de comprender y analizar a fondo los dispositivos físicos de la red administrativa, al ser mixta permite cuantificar y describir los datos con gran detalle, lo que es de gran importancia para la indagación.

Se utiliza el enfoque mixto para obtener la información, se realizan encuestas y cuestionarios al personal administrativo y de informática del Benemérito Liceo José Martí, ya que es uno de los instrumentos más utilizados, por lo tanto, las preguntas son estandarizadas según las normas técnicas para la gestión y el control de las Tecnologías de la Información de la Contraloría General de la República, brindan respuestas sobre la red administrativa, sin emitir juicios, sino más bien obtener información acerca de esta red, que sea muy específica para la comprobación de los datos y, así, obtener un resultado.

Este tipo de investigación combina las fortalezas de los enfoques cualitativo y cuantitativo, con el fin de observar el problema específico y, a su vez, formular la recolección y análisis de datos por realizarse en la investigación, además de la determinación de los objetivos planteados.

Según Hernández, Fernández y Baptista, citados por Guelmes y Nieto (2015)

> el enfoque mixto va más allá de la simple recolección de datos de diferentes modos sobre el mismo fenómeno, ya que implica desde el planteamiento del problema, mezclar la lógica inductiva y la deductiva, por lo que un estudio mixto debe serlo en el planteamiento del problema, la recolección y análisis de los datos, y en el reporte del estudio. (p.1)

4.6. Tipos de investigación

Los tipos de investigación son vistos como el marco general del proceso metodológico, el cual se sigue con el fin de responder el problema de investigación y lograr los objetivos planteados. (Jensy, 2015, p.86)

Algunos de los tipos de investigación se exponen a continuación.

4.6.1. Etnográfico

> La etnografía es uno de los métodos más relevantes, utilizados en el enfoque de investigación cualitativo. En este, se aborda el objeto de estudio con el fin de comprender e interpretar la realidad a la que pertenece, busca obtener planteamientos y conocimientos teóricos. En este tipo de investigación, se recopila una visión general del lugar estudiado desde distintos puntos de vista. (Psyma, 2015, párr. 2)

4.6.2. Biográficos

> Permite ampliar el conocimiento, que se tiene de lo que ocurre en el ambiente investigativo, a través del punto de vista del sujeto implicado, personas anónimas, que aportan una mirada personal de su proceso como educativo o formativo. Su utilidad radica en que, mediante este tipo se pueden plantear hipótesis y proporciona un control mayor sobre la información obtenida. (Tapia, 2016, párr. 1)

4.6.3. Descriptivos

Los tipos de investigación descriptivos

> buscan especificar las propiedades, características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno, que se someta a un análisis. En un estudio descriptivo, se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para, así, describir lo que se investiga. (Tipos de investigación, 2018, párr. 2)

4.6.4. Experimentales

> En este enfoque, el investigador manipula las variables de estudio, con el fin de controlar el aumento o disminución de dichas variables y su efecto en las conductas determinadas. Esto es realizado en condiciones controladas, con la finalidad de describir cómo, qué o por qué se produce una situación en particular. (Alonso et al., s.f., p.5)

4.6.5. Correlacionales

En este tipo de investigación, el investigador debe medir dos variables. Busca que dichas variables interactúen entre sí, de manera que cuando una cambie, al hacer la investigación, se tendrá claro que la otra variable también cambia. (Escárcega, s.f., párr. 2)

4.6.6. Basados en encuesta

La encuesta es una de las técnicas de investigación social de más extendido uso en el campo de la Sociología, que ha trascendido el ámbito estricto de la investigación científica, para convertirse en una actividad cotidiana de la que todos participamos tarde o temprano. (López y Fachelli, 2015, p.5)

La encuesta es una técnica de recogida de datos mediante la aplicación de un cuestionario a una muestra de individuos. A través de las encuestas, se pueden conocer las opiniones, las actitudes y los comportamientos de los ciudadanos.

En una encuesta, se realizan una serie de preguntas sobre uno o varios temas a una muestra de personas seleccionadas, se siguen una serie de reglas científicas, que hacen que esa muestra sea, en su conjunto, representativa de la población general de la que procede. (Centro de Investigaciones Sociológicas, s.f., párr. 1)

4.6.7. Tipo de investigación aplicada

El tipo de investigación, que se va a realizar, utiliza la combinación de la investigación descriptiva e investigativa, particularmente esta se basa en los hechos recolectados por medio de las encuestas y cuestionarios realizados a los diversos usuarios con acceso a la red y, en general, a los dispositivos de red, que se encuentren en la institución, de la misma forma busca realizar observaciones y analizar a profundidad los dispositivos de red encontrados en la institución, esto con la finalidad de describir la información a generar en los procesos de la investigación.

4.7. Sujetos y fuentes de información

Hace referencia a expedientes, archivos, revistas, tesis, libros, artículos de internet, entre otros. Se deben clasificar en primarias y secundarias; el sujeto de investigación también se considera una fuente de información. (Jensy, 2015, pp.89-90)

4.7.1. Sujetos

Contempla todos aquellas personas o lugares, que participan en la investigación, en este caso específico, el personal administrativo y de informática del Benemérito Liceo José Martí. En el caso de los encargados de informática, son quienes propician la mayoría de información concerniente al área física de las redes, el personal administrativo que va a brindar información sobre el uso de la red administrativa.

4.7.2. Fuentes

Estas fuentes son primordiales para desarrollar una investigación, ya que, si no se pudiese acceder a ellas, la información no sería amplia para lograr una investigación favorable.

4.7.2.1. Fuentes primarias

Este tipo de fuente “son aquellas en las que los datos provienen directamente de la población o muestra de la población”. (Torres y Paz, 2014, p.3)

Se denominan fuentes primarias a toda esa información de primera mano de una fuente totalmente confiable, por ejemplo, los libros, entrevistas, manuales del área.

En esta investigación, se utilizarán libros, las Normas Técnicas de la Contraloría General de la República y manuales de la estructura de la red.

4.7.2.2. Fuentes secundarias

Es la fuente de información que “parten de datos preelaborados, como pueden ser datos obtenidos de anuarios estadísticos, de Internet, de medios de comunicación”. (Torres y Paz, 2014, p.3)

Las fuentes secundarias contienen información analizada y reorganizada que proviene de los documentos originales por ejemplo los blogs y revistas. En la investigación se utilizarán páginas y archivos en PDF provenientes de internet.

4.8. Población y muestra

Se toma en cuenta que por población se refiere un conjunto de individuos, que poseen las mismas características para realizar un estudio. En cuanto a la muestra, se denota como una selección específica de una población, esto de forma aleatoria con la finalidad de poder analizarla y, así, no tener que analizar, en general, a toda la población, esto incurre en el ahorro de tiempo ya que no sería tan extenso el proceso de indagación.

4.8.1. Población

> Algunos autores usan el término población cuando el campo de trabajo de la investigación comprende solo personas; sin embargo, otro gran número de investigadores usan población para referirse tanto a personas, como animales, plantas, seres inanimados o entes abstractos como números o cantidades. (Ulloa, 2012, p.1)

Según Ulloa (2012), se puede definir a la población como “el conjunto de todos los elementos materia de la investigación”. (p.1)

La población, para esta investigación, son los encargados del área de informática y el personal administrativo del Benemérito Liceo José Martí.

4.8.1.1. Población meta

Compuesta por el sector de la población, en quienes se enfoca el trabajo de investigación. En caso de que la población sea numerosa y sea reducida a una muestra, es necesario señalar el tipo de muestreo

empleado para obtener una clara idea de los procedimientos de elección en la población. (Jensy, 2015, p.50)

4.8.2. Muestra

> Una muestra es un subconjunto de la población, que se obtiene para averiguar las propiedades o características de esta última, por lo que interesa que sea un reflejo de la población, que sea representativa de ella. (Ludewig, s.f., p.2)

La muestra se utiliza cuando “no es posible hacer la investigación en toda la población o investigación censal por razones de costos, de tiempo o económicas en general”. (Ulloa, 2012, p.1)

Por ende, la muestra es seleccionada entre la población existente de encargados de TI y administrativos del Benemérito Liceo José Martí para obtener un resultado a base del análisis empleado a la muestra.

Para efectos de esta investigación, la muestra va a ser un 100% de los encargados de informática y el personal administrativo.

4.9. Técnicas para obtener información

Las técnicas de recolección de datos en un estudio dictan, según el enfoque, la forma en la cual se debe recopilar la información, fundamentalmente, son utilizadas para recolectar información en torno a lo investigado.

Existen varias técnicas de recolección de datos, por ejemplo, las siguientes.

- **Entrevista**

  Se utiliza como método de recolección de datos en una investigación, ya que la entrevista posee la cualidad de interiorizar en cuanto a temas puntuales de interés para el entrevistador, esta se emplea en la muestra de la población escogida.

- **Observación**

  El presente método se basa en recabar información meramente de evidencia observada o captada por medios de sondeo, lo cual hace que este método sea, normalmente, uno de los más utilizados en el momento de analizar un ambiente determinado.

- **Cuestionarios**

  El presente método se basa en el desarrollo de formularios con una cantidad variable de preguntas aplicadas al personal, que utiliza la red administrativa, se desea profundizar en los diversos aspectos de la red física administrativa de la institución, ya que, según las preguntas empleadas, se puede obtener un panorama completo acerca de lo indagado.

4.9.1. Técnica aplicada

La técnica aplicada en esta investigación se enfoca en la recopilación de datos a partir de encuestas, cuestionarios y observaciones, los cuales permiten adquirir, de forma vasta, la información.

El cuestionario se enfoca de forma amigable con el encuestado para abstraer la información requerida y, así, poseer el conocimiento, que tienen estos en relación con tema de estudio.

Por otro lado, la encuesta brinda una mayor descripción de los puntos requeridos en la investigación, por lo cual es de suma importancia su utilización, con el propósito de poseer un punto más detallado del lugar.

La observación permite, al investigador, dar un paradigma técnico propio y crítico, por lo cual se da un enfoque holístico en pro a la mejora de la institución, da a relucir cuáles son los puntos, en los cuales se debe enfocar la institución para su crecimiento futuro, aportando seguridad y confiabilidad.

CAPÍTULO V

ANÁLISIS E INTERPRETACIÓN

DE RESULTADOS

5. Análisis de resultados

El siguiente análisis se focaliza en la interpretación de los resultados obtenidos a raíz de la colecta de datos realizada en el Benemérito Liceo José Martí, en el tercer cuatrimestre del año 2019, específicamente a los funcionarios que hacen uso de la red administrativa, según lo dictado por la Contraloría General de la República en las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información, N-2-2007-CO-DFOE, hace hincapié en los capítulos I y IV, en los cuales se destaca la seguridad física y ambiental, tanto como la administración y operación de la plataforma tecnológica. La idea central es explicar y comparar los datos encontrados en la investigación con lo estipulado por la Contraloría General de la República para señalar si, efectivamente, se cumple con lo especificado en esta normativa en los capítulos previamente señalados, todo con el fin de mejorar lo relacionado con la infraestructura física de red en el área administrativa del Benemérito Liceo José Martí.

Para recolectar la información, se hace uso de un cuestionario a 10 funcionarios administrativos del Benemérito Liceo José Martí, también se realiza una observación en las instalaciones del Liceo y se aplica un cuestionario y entrevista al encargado de Tecnologías de la Información de la institución.

5.1. Seguridad física y ambiental

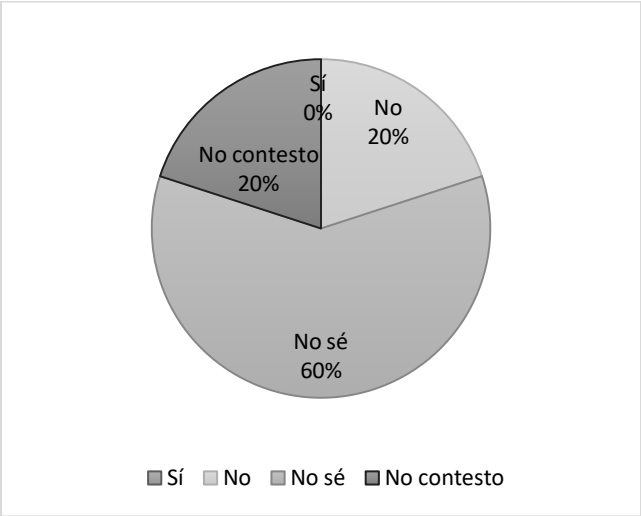
Según la Contraloría General de la República, en el apartado 1.4.3, “La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos”. (Contraloría General de la República, 2007, p.3)

Es importante el resguardo de todos los equipos informáticos ante altercados de índole ambiental o físico, los cuales podrían atentar contra la integridad de los dispositivos utilizados en las diversas áreas del sector informático, ya que la pérdida de estos podría generar una detención de los servicios brindados.

Por lo anterior, se procede a consultar sobre las políticas existentes en seguridad física y ambiental al personal administrativo del Benemérito Liceo José Martí, los resultados obtenidos se expresan en el gráfico #1.

Gráfico #1

Conocimiento del personal administrativo sobre las políticas de seguridad física y ambiental en el Benemérito Liceo José Martí



Fuente: Creación propia, 2019.

Tabla #1

Conocimiento del personal administrativo sobre las políticas de seguridad física y ambiental en el Benemérito Liceo José Martí

Respuesta	**Frecuencia**	**Porcentaje**
Sí	0	0%
No	2	20%
No sé	6	60%
No contesta	2	20%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El personal administrativo en general (60%) indica desconocimiento sobre la existencia de políticas de seguridad física y ambiental, 20% asegura que no existen dichas políticas en la institución y el 20% restante no responde ninguna de las opciones.

Por lo tanto, se corrobora con el cuestionario aplicado al encargado de Tecnologías de la Información que no cuentan con las políticas necesarias de seguridad física y ambiental, que dictan las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República.

Tabla #2 Aspectos encontrados y Recomendaciones

Aspectos encontrados	**Recomendaciones**
• No existen políticas de seguridad física y ambiental para la institución.	• Proponer una política de seguridad física y ambiental, según lo que dictan las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información.

5.2. Controles de acceso a la institución

El acceso es levemente restringido en la entrada de la institución, ya que existe un guarda de seguridad encargado de regular el ingreso de personas, y, en caso de ser alguien no autorizado, se posee una bitácora, la cual colecta datos, tales como nombre y número de cédula del sujeto que desea entrar al Liceo, para el acceso al departamento de TI únicamente se posee una llave en la institución y la porta el encargado de Tecnologías de Información.

En el área de la dirección administrativa, existen inconsistencias en cuanto al control de acceso en las oficinas, debido a que el cubículo, en el que se encuentra la mayoría de los miembros de equipo, no posee separación física adecuada, es decir, la entrada a los cubículos es libre y cualquier persona ajena a la institución puede acceder fácilmente al equipo informático. En la oficina de auxiliares administrativos y en la biblioteca, la situación es similar, ya que no existe mayor protección en la entrada y se puede entrar sin ninguna dificultad; la oficina de asistencia directiva es la única que no colinda con otro departamento y posee un espacio adecuado para el desarrollo de sus actividades, pero es de fácil acceso, ya que la puerta principal lleva directamente a la oficina.

En cuanto a los controles de acceso a los dispositivos informáticos, tales como puntos de red, se encuentran en una posición sumamente accesible, ya que están a poca altura del suelo, por lo que pueden acceder a la red, sin embargo, en la dirección general, se localiza un IDF (Servicios de Distribución

Intermedia), el cual se encuentra a una altura considerable y debidamente cerrado bajo llave, lo cual hace que no sea de fácil acceso.

Tabla #3 Aspectos encontrados y Recomendaciones

Aspectos encontrados	**Recomendaciones**
• La institución cuenta con un guarda para regular el acceso de personal no autorizado, sin embargo, después de acceder al Liceo, las oficinas de los administrativos carecen de controles de acceso para sus respectivos cubículos. • Las oficinas del personal administrativo no poseen su separación adecuada, ya que son compartidas por múltiples miembros del equipo. • Los puntos de red son de fácil acceso porque se encuentran a una altura muy baja y cualquiera se puede conectar.	• Establecer controles de acceso de manera que solo personal autorizado pueda ingresar a las oficinas administrativas, y mecanismos de manera tal que otras personas puedan ser atendidas sin la necesidad de acceder físicamente. • Proponer que las oficinas del personal administrativo sean separadas adecuadamente, por ejemplo, que las mismas posean su propia puerta para que solo el personal autorizado tenga acceso. • Recomendar bloqueo de puertos de puntos de red que no estén en uso.

5.3. Ubicación física de los recursos de Tecnologías de la Información

La ubicación física de los dispositivos de red es de suma importancia para que nadie pueda tener acceso al hardware y que no les puedan hacer algún tipo de daño, se asegura la integridad de los equipos dentro de la institución.

En el Benemérito Liceo José Martí, la localización de los dispositivos de la red administrativa es adecuada, ya que cada equipo posee su escritorio y están lejos de las ventanas, lo que garantiza que nadie pueda hacerles daño, pese a esto los dispositivos informáticos se encuentran vulnerables a fenómenos naturales, como temblores, ya que los escritorios, donde se encuentran, no son cerrados y podrían caerse en caso de que ocurra un sismo de mucha magnitud.

Tabla #4 Aspectos encontrados y Recomendaciones

Aspectos encontrados	Recomendaciones
• Cada equipo de la red administrativa posee su propia mesa y se encuentran alejados de las ventanas, evitando daños o robos. • Los equipos informáticos pueden ser dañados por fenómenos naturales, como los temblores porque el escritorio de cada dispositivo es abierto, pueden caerse y dañarse sus componentes internos.	• Proponer la compra de escritorios cerrados y que estos posean rodines o sean estáticos para que no se vuelquen en caso de sismo.

5.4. Ingreso y salida de equipos de la institución

Es importante tener un control sobre el ingreso y la salida de los dispositivos tecnológicos de la red administrativa, porque esto brinda un registro adecuado y claro del equipo informático, lo que garantiza que el control de activos sea correcto.

Debido a la gestión del ingreso y salida de activos, se procede a consultar sobre la existencia de políticas de entrada y salida de equipos de la institución

al personal administrativo del Benemérito Liceo José Martí, los resultados obtenidos se expresan en la tabla #5.

Tabla #5

Conocimiento del personal administrativo sobre las políticas de ingreso y salida de equipos en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Sí	3	30%
No	1	10%
No sé	4	40%
No contestó	2	20%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El personal administrativo en general (40%) carece de conocimiento sobre la existencia de políticas de ingreso y salida de equipos de la institución, 10% asegura que no existen dichas políticas dentro de la institución, un 30 % indica que el Liceo sí cuenta con las políticas de entrada y salida de equipos y el 20% restante no responde ninguna de las opciones.

Por otra parte, se corrobora, con el cuestionario aplicado al encargado de Tecnologías de la Información, que sí cuentan con un control para el ingreso y salida de equipos de la institución, es preocupante que, contando con dichas políticas, muchos funcionarios administrativos no conozcan su existencia.

El acceso del personal administrativo a la política de ingreso y extracción de equipos de la institución (ver tabla #6) es de vital importancia para conocer los puntos que establece, de esta manera, el funcionario sabe cómo proceder cuando se necesite extraer un equipo de la institución.

Tabla #6

Acceso del personal administrativo a las políticas de ingreso y salida de equipos en el Benemérito Liceo José Martí

Respuesta	**Frecuencia**	**Porcentaje**
Sí	2	80%
No	1	20%
No contestó	0	0%
Total	**5**	**100%**

Fuente: Creación propia, 2019.

Las tres personas, que afirman que sí existe un control para el ingreso y salida de equipo informático (ver tabla #5), constituyen el 100% de la tabla #6, por lo que un total del 80% indica que sí puede acceder a las políticas para el ingreso y extracción de equipos de la institución y 20% asegura que no posee acceso.

Tabla #7 Aspectos encontrados y Recomendaciones

Aspectos encontrados	Recomendaciones
• Se corrobora la existencia de las políticas para el ingreso y salida de equipos de la institución, pero algunos empleados administrativos no conocen o aseguran que no existe dicha política. • Algunos empleados administrativos aseguran que no tienen acceso a las políticas. • Falta de comunicación ya que los funcionarios no conocen la política, solamente se les indica cómo realizar el proceso cuando lo requiere.	• Proponer capacitaciones para el personal administrativo para que obtengan el conocimiento de las políticas para el ingreso y salida de equipos de la institución. • Enviar un lineamiento o la boleta, que se utiliza, por correo electrónico a cada uno del personal para que se informen.

5.5. Control de los servicios de mantenimiento

Los dispositivos informáticos requieren de un mantenimiento prudente, por ello, se debe tener un control efectivo de los servicios de mantenimiento, esto ayuda a que funcionen de manera óptima y se prolongue su tiempo de vida útil.

De acuerdo con lo anterior, se procede a consultar, al personal de administración, la frecuencia con que se realiza el mantenimiento a los equipos, los resultados obtenidos se presentan en la tabla #8.

Tabla #8

Frecuencia con la que se brinda mantenimiento al equipo según el personal administrativo

Respuesta	**Frecuencia**	**Porcentaje**
Cada tres meses	3	30%
Cada seis meses	0	0%
Cada año	4	40%
No contestó	3	30%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El 40% del personal administrativo afirma que los servicios de mantenimiento son realizados cada año, 30% indica que dichas labores se ejecutan cada tres meses, el 30% restante no responde ninguna de las opciones.

Por lo tanto, hay un lapso abismal entre las respuestas aportadas por los funcionarios administrativos del Benemérito Liceo José Martí, en comparación con el cuestionario aplicado al encargado de Tecnologías de la Información, se corrobora que los servicios de control de mantenimiento son realizados cada tres meses, lo cual es un tiempo prudencial para mantener los equipos, trabajando óptimamente.

5.6. Controles para el desecho y reutilización de recursos de Tecnologías de la Información

Las instituciones deben contar con sus debidos controles para desechar y reutilizar equipo informático, ya que es necesario gestionar, de forma correcta, las distintas partes, que componen los computadores, reutilizando el hardware, que puede ser funcional en otro computador, y, posteriormente, tomar las medidas necesarias para el desecho de los demás componentes físicos.

Por lo tanto, se confirma, con el cuestionario aplicado al encargado de TI, que no cuentan con los controles para el desecho y reutilización de recursos de Tecnologías de la Información, lo cual es preocupante, ya que la institución cuenta con bastante equipo informático, pero no tiene un plan de control para los equipos que deben desechar o reutilizar.

Tabla #9 Aspectos encontrados y Recomendaciones

Aspectos encontrados	Recomendaciones
• No existe un control definido para el desecho y reutilización de recursos de Tecnologías de la Información. • El encargado de Tecnologías de la Información realiza actas de desecho y coordina con la municipalidad del área para la recolección del equipo.	• Proponer un control para realizar el desecho y reutilización de los recursos de Tecnologías de la Información.

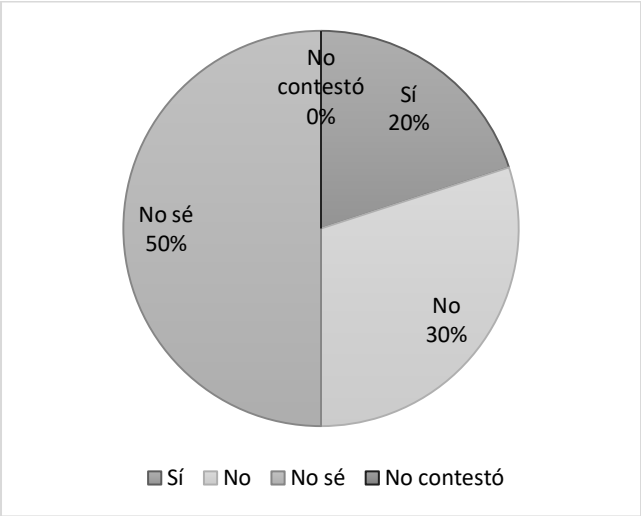
5.7. Continuidad, seguridad y control del suministro de energía eléctrica, cableado de datos y comunicaciones inalámbricas

La seguridad de los equipos tecnológicos es muy importante debido a que, a través de estos, se procesa información delicada, por lo tanto, se da continuidad a los análisis de seguridad, así como al cableado de datos, ya que, por medio de estos, se logra la intercomunicación entre los distintos dispositivos que componen la red.

Por ello, se consulta, al personal administrativo del Benemérito Liceo José Martí, si se realizan análisis de seguridad física a los dispositivos de red, los resultados obtenidos se muestran en el gráfico #2.

Gráfico #2

Análisis de seguridad física a los dispositivos de red según el personal administrativo



Fuente: Creación propia, 2019.

Tabla #10

Análisis de seguridad física a los dispositivos de red según el personal administrativo

Respuesta	Frecuencia	Porcentaje
Sí	2	20%
No	3	30%
No sé	5	50%
No contestó	0	0%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El 50% del personal administrativo indica desconocimiento si se ha realizado alguna vez un análisis de seguridad física a los dispositivos de red de la institución, 30% asegura que no se ha realizado, y el 20% restante afirma que sí han realizado análisis de seguridad física.

Del 20% del personal administrativo que asegura la realización de análisis de seguridad física, uno indica que los análisis son realizados cada tres meses, y el otro no contesta ninguna de las opciones, como se muestra en la tabla #11.

Tabla #11

Tiempo de análisis de seguridad física a los dispositivos de red en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Cada tres meses	1	50%
Cada seis meses	0	0%
Cada año	0	0%
No contestó	1	50%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

Por consiguiente, se corrobora, con el cuestionario aplicado al encargado de Tecnologías de la Información, que nunca se ha realizado un análisis de seguridad física a los dispositivos de red, situación que es muy preocupante, debido a que, constantemente, se deben estar analizando los equipos de la red con el fin de prevenir riesgos.

En cuanto a la seguridad y control del suministro de energía eléctrica, es fundamental para las instituciones, ya que permite mantenerse trabajando en caso de corte de electricidad y, así, guardar la información, que se está procesando, para no perderla por un corte repentino. Por lo anterior, se procede a consultar, al personal administrativo, sobre la existencia de un sistema de alimentación ininterrumpida, los resultados obtenidos se expresan en la tabla #12.

Tabla #12

Conocimiento del personal administrativo sobre la existencia de un sistema de alimentación ininterrumpida en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Sí	3	30%
No	6	60%
No contestó	1	10%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

En general, el 60% del personal administrativo no tiene conocimiento sobre la existencia de un sistema de alimentación ininterrumpida, 30% asegura que la institución sí cuenta con este dispositivo, y el último 10% no contesta ninguna de las opciones.

Al personal administrativo que indica la existencia del dispositivo de alimentación ininterrumpida, se le pregunta por el tiempo de autonomía, que brinda este, uno señala 15 minutos de autonomía, otro afirma que una hora, y el último no contesta ninguna de las opciones, como se muestra en la tabla #13.

Tabla #13

Tiempo de autonomía del sistema de alimentación ininterrumpida en el Benemérito Liceo José Martí según el personal administrativo

Respuesta	Frecuencia	Porcentaje
15 minutos	1	34%
30 minutos	0	0%
1 hora	1	33%
No sé	0	0
No contestó	1	33%
Total	**3**	**100%**

Fuente: Creación propia, 2019.

El encargado de Tecnologías de la Información indica que sí existe un sistema de alimentación ininterrumpida para cada computador del personal administrativo, la cual brinda 20 minutos de autonomía. El servidor del Liceo cuenta con una UPS de tres baterías de 1500 voltios en granja, cada una soporta 30 minutos, en total brinda una hora y media de autonomía en caso de corte de electricidad.

La continuidad, control y seguridad, que se debe realizar a las comunicaciones inalámbricas, es un punto por tomar en cuenta en las empresas, ya que estas son un canal, que debe estar siempre seguro, y, así, evitar que datos sensibles puedan ser capturados por un tercero. El encargado de TI opta porque todo el personal administrativo utilice solo la red cableada, esto teniendo en cuenta la seguridad, que se brinda en comparación con el hecho de que los computadores se conecten y envíen sus datos mediante WiFi. Por lo tanto, se corrobora que todo el personal administrativo realiza su trabajo mediante red cableada.

Tabla #14 Aspectos encontrados y Recomendaciones

Aspectos encontrados	Recomendaciones
• Nunca se ha realizado un análisis de seguridad a los dispositivos físicos de la red administrativa, lo cual es importante llevar a cabo con el fin de asegurar los equipos. • La mayoría de personal administrativo no tiene conocimiento de la existencia de un sistema de alimentación ininterrumpida y los pocos que conocen que existe no saben cuánto tiene de autonomía el equipo, lo cual es preocupante porque no saben cuánto tiempo tienen para trabajar después de un corte repentino de electricidad. • Según manifiesta el mismo encargado de informática, no se brinda ningún tipo de análisis, esto podría afectar, en un futuro, la red y sus equipos.	• Proponer que cada cuatro meses se realicen labores de análisis de seguridad de los dispositivos físicos de la red administrativa. • Informar, al personal, sobre la existencia y el tiempo de autonomía del sistema de alimentación ininterrumpida, con el que cuenta la institución, con el fin de que tomen las precauciones necesarias cuando suceda un corte repentino de electricidad.

5.8. Acceso de terceros

Gestionar el acceso de terceros es un punto importante, que se debe tener en cuenta, con el fin de poder resguardar y mantener seguros todos los recursos de la institución.

A pesar de que la institución mantiene un control en el ingreso al edificio, el acceso a la red administrativa no es tan seguro porque cualquier persona puede llegar a las oficinas del personal del Liceo sin ninguna dificultad y puede conectarse con un computador por medio de los puntos de red, ya que estos no se encuentran bloqueados y, pese a tener cuentas de usuarios, se puede lograr entrar al sistema por medio de programas. Al cuarto de Tecnologías de la Información, solo tiene acceso el encargado, el cual tiene la única llave que existe para acceder a dicha oficina.

Tabla #15 Aspectos encontrados y Recomendaciones

Aspectos encontrados	Recomendaciones
• El acceso al cuarto de Tecnologías de la Información se encuentra correctamente resguardado debido a que solo el encargado posee llave para acceder. • Se puede acceder a la red administrativa por medio de los puntos de red, ya que estos no se encuentran bloqueados.	• Recomendar bloqueo de puertos de puntos de red, que no estén en uso, con el fin de evitar el acceso de un tercero a la red.

5.9. Riesgos asociados con el ambiente

Los riesgos ambientales existentes son variados debido a la cercanía del Océano Pacífico, se da la peculiaridad de que el edificio, en donde está situado el cuarto de TI, es declarado el más seguro de la zona, esto es decretado por la Comisión Nacional de Emergencias de la República de Costa Rica, sumado a que se ubica en la segunda planta, la posibilidad de inundaciones es relativamente baja y, en caso de tsunamis, la altura del edificio reduciría el impacto de una ola, el edificio, al tener el nivel de seguridad mencionado, tiene una posibilidad sumamente alta de soportar un sismo de una magnitud considerable, existen áreas verdes alrededor de la institución para resguardar la seguridad de las personas, también se da la

aparición de salitre debido a que la institución se ubica a escasos cien metros del mar, esto ocasiona la corrosión de los equipos, a pesar de todo esto no se posee un plan de contingencias adecuado a las realidad de la institución.

Tabla #16 Aspectos encontrados y Recomendaciones

Aspectos encontrados	Recomendaciones
• La seguridad del edificio es elevada. • No se posee un plan de contingencias.	• Se denota que es de urgencia la implementación de un plan de contingencias adecuado a la realidad de la institución.

5.10. Administración y operación de la plataforma tecnológica

Según la Contraloría General de la República, en el apartado 4.2, “La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas”. (Contraloría General de la República, 2007, p.15)

Es de suma importancia el resguardo de las operaciones en la plataforma tecnológica existente en la institución, ya que, por medio de esta, se realizan las tareas diarias en el área administrativa de la institución.

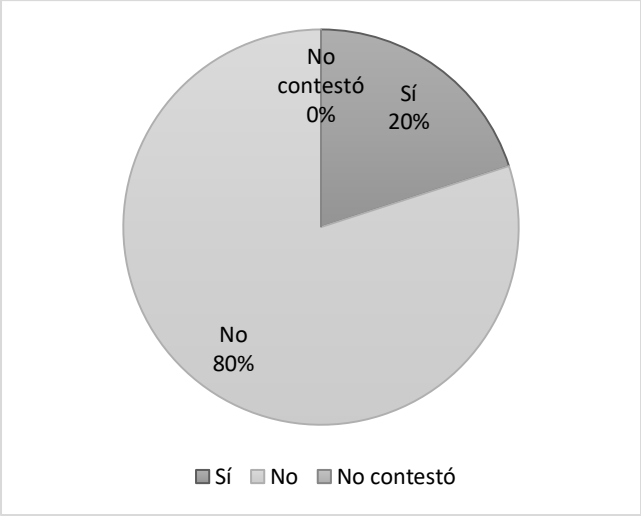
5.11. Documentación de procedimientos y responsabilidades con la operación de la plataforma

En general, la institución en el área de TI no posee documentación sobre los procesos y procedimientos de diaria ejecución, no se cuenta con un organigrama definido y tampoco hay un plan de contingencias, que pueda salvaguardar el equipo informático existente, a su vez, no se ha pactado un plan de respaldo de información.

En cuanto a la existencia de capacitaciones sobre el manejo del equipo informático, se indica lo siguiente.

Gráfico #3

Conocimiento sobre las capacitaciones del personal administrativo en el manejo de los dispositivos informáticos en el Benemérito Liceo José Martí



Fuente: Creación propia, 2019.

Tabla #17

Conocimiento sobre las capacitaciones del personal administrativo en el manejo de los dispositivos informáticos en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Sí	2	20%
No	8	80%
No contestó	0	0%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El 20% del personal administrativo indica haber recibido capacitación sobre el manejo de los dispositivos de red de la institución, un 80% asegura que no ha recibido.

Gráfico #4

Frecuencia con la que se imparten las capacitaciones del personal administrativo sobre el manejo de los dispositivos de red en el Benemérito Liceo José Martí

Fuente: Creación propia, 2019.

Tabla #18

Frecuencia con la que se imparten las capacitaciones del personal administrativo sobre el manejo de los dispositivos de red en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Una vez al año	1	50%
Dos veces al año	0	0%
Otra	1	50%
No contestó	0	0%
Total	**2**	**100%**

Fuente: Creación propia, 2019.

El 50% del personal administrativo indica haber recibido capacitación sobre el manejo de los dispositivos de red de la institución al menos una vez al año, 50% asegura que el intervalo entre capacitaciones es variable.

Según lo observado, al ocurrir un inconveniente con los equipos del personal administrativo, se presenta un reporte por medio del correo electrónico o una llamada al administrador del departamento de TI para que él proceda a la reparación, una vez que termina, procede a explicar cómo solucionar la problemática, en caso de ser un problema que requiera mayor tecnicismo, solo se explica para que el usuario tenga noción de lo sucedido.

Tabla #19 Aspectos encontrados y Recomendaciones

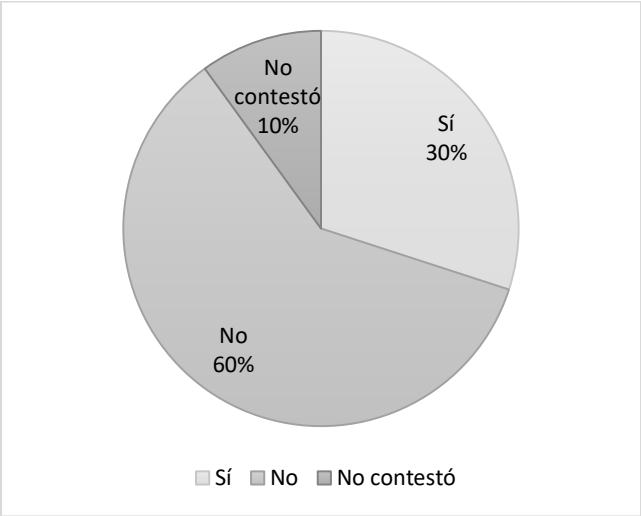
Aspectos encontrados	Recomendaciones
• No se posee documentación sobre el seguimiento de casos e incidentes con los equipos informáticos.	• El personal de TI de la institución debe acoger una política de generación de realimentación de casos. • Documentar toda la realimentación generada, en caso de un futuro cambio de personal de TI.

5.12. Disponibilidad, capacidad, desempeño y uso de la plataforma

Según lo observado en las diversas áreas en las que se encuentra la plataforma física de la red administrativa, se denota que el equipo cumple con las necesidades de la institución, la disponibilidad del equipo es exclusiva para sus funciones institucionales, en cuanto al desempeño de estos, se concluye con base en lo expresado por el encargado de TI, que son adecuados para sus funciones. En el momento de realizar las encuestas al personal administrativo, ocurre un aspecto importante, los administrativos afirman, en su mayoría, que los equipos no dan abasto, pero, en cuanto a equipos, mencionan que se refieren a los ordenadores y no a los dispositivos de red administrativa. En el siguiente gráfico, se observa la opinión de los administrativos.

Gráfico #5

Conocimiento sobre la calidad de los dispositivos de red en el Benemérito Liceo José Martí



Fuente: Creación propia, 2019.

Tabla #20

Conocimiento sobre la calidad de los dispositivos de red en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Sí	3	30%
No	6	60%
No contestó	1	10%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El 30% del personal administrativo indica que la institución posee dispositivos de red de calidad, 60% asegura que no son de calidad. Cabe destacar que un 10% de las personas no contesta de forma positiva o negativa.

Algunos de los equipos encontrados en la red administrativa son los siguientes.

Proxy

Proxy con pfSense, Servidor HP con 16gb RAM y un Intel Xeon 4 núcleos, 2 interfaces de red gigabit ethernet, como extra posee una tarjeta PCi con 4 interfaces de red gigabit ethernet.

El proxy se encarga de manejar todas las conexiones del colegio, el mismo funciona mediante VLANs, la red administrativa tiene su propia VLAN, que se encarga de controlar el liceo diurno y nocturno (ambos en la misma VLAN).

El servidor proxy está conectado con los *switches* de toda la red del liceo.

Switches

Todos los *switches* del liceo son de la marca HP, 24 puertos (algunos son PoE), existe un *switch* de 48 puertos, excepto un D-Link, pero, este es para pruebas, todos los *switches* son Gigabit Ethernet, poseen la posibilidad de conectarse por fibra óptica, pero todo se encuentra cableado mediante cable UTP categoría 6.

Computadoras portátiles

Para la red administrativa, se cuenta con un total de tres computadoras portátiles, son de uso discrecional, para el acceso a la red administrativa en el Liceo, el equipo se debe conectar por cable de red al estar en la oficina.

Telefonía

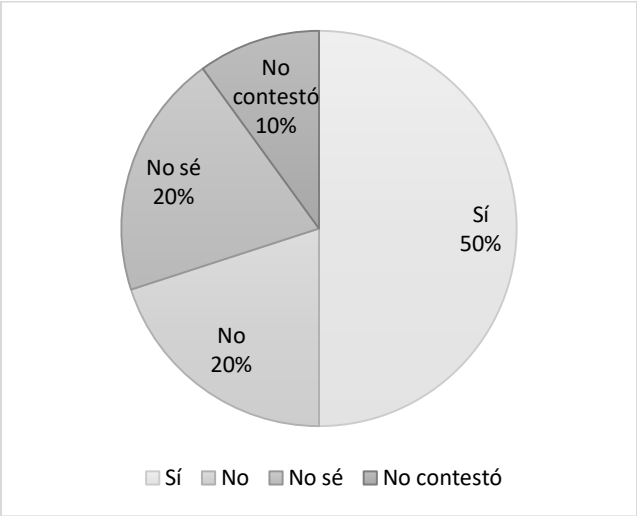
Para la telefonía, se utiliza un servidor Dell con 16GB RAM, Intel Xeon, 2TB de disco duro con sistema operativo Linux CentOS con la aplicación ELASTIX, la cual se encarga de controlar la central telefónica (diurno y nocturno), todas las oficinas cuentan con telefonía (Telefonía IP que posee su propia VLAN), la telefonía es brindada por el ICE por media de fibra óptica y la telefonía es digital.

Opinión

En general, la mayoría del equipo observado en la institución es de una calidad adecuada para el funcionamiento diario en cuanto a las labores del área administrativa.

Gráfico #6

Conocimiento sobre si los dispositivos de red son adecuados para sus labores en el Benemérito Liceo José Martí



Fuente: Creación propia, 2019.

Tabla #21

Conocimiento sobre si los dispositivos de red son adecuados para sus labores en el Benemérito Liceo José Martí

Respuesta	Frecuencia	Porcentaje
Sí	5	50%
No	2	20%
No sé	2	20%
No contestó	1	10%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El 50% del personal administrativo afirma que los dispositivos de red son adecuados para sus labores, 20% indica que dichos dispositivos no son adecuados, el 20% dice no saber si son adecuados y el 10% restante no responde ninguna de las opciones.

Los equipos encontrados en la institución a nivel de la red administrativa cumplen con las necesidades del personal; a nivel de usuarios, existe disconformidad en cuanto a los equipos que ellos utilizan, llámese, computadoras, debido a que no todas son de última tecnología, el área de redes se considera el fuerte de la institución, debido a que soporta, de forma continua y sin mayor complicación, el trasiego de información.

Tabla #22 Aspectos encontrados y Recomendaciones

Aspectos encontrados	**Recomendaciones**
• En general los equipos son de buena calidad. • Los miembros requieren ser capacitados constantemente para renovar y adquirir nuevos conocimientos.	• Capacitar al equipo en materia básica de redes para que, así, conozcan un poco más sobre la funcionabilidad de los dispositivos de red en general.

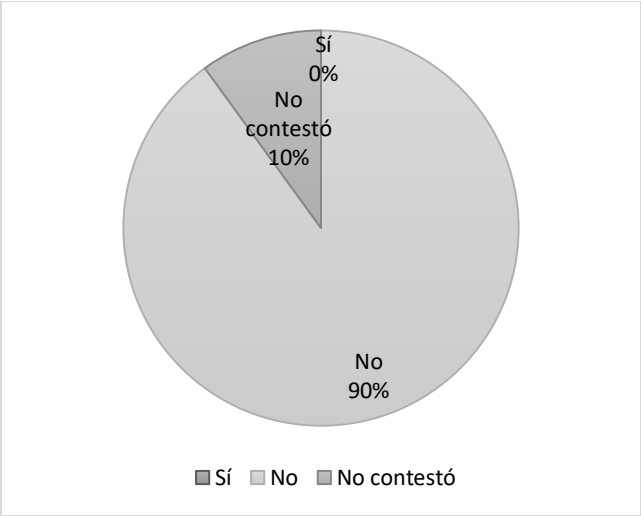
5.13. Requerimientos presentes y futuros, que garantizan la oportuna adquisición de los recursos de Tecnologías de la Información

Las instituciones deben poseer requerimientos futuros en cuanto al hardware, que garanticen la oportunidad de adquirir recursos de Tecnologías de la Información y, con esto, establecer planes para la satisfacción y debido funcionamiento de las áreas de trabajo, tomando en cuenta planes de contingencia y las tendencias tecnológicas de la actualidad.

En este caso en especial, se deduce que la institución no posee planes de contingencia orientados a salvaguardar los equipos, en cuanto a la actualización de equipos, se observa que se hace de forma frecuente, pero, no poseen un control debido a la obsolescencia, por otra parte, la institución posee una cantidad de equipos en el cuarto de TI muy competente.

Gráfico #7

Opinión del personal administrativo sobre si existen planes de contingencia, que salvaguarden la integridad de dispositivos de red en el Benemérito Liceo José Martí



Fuente: Creación propia, 2019.

Tabla #23

Opinión del personal administrativo sobre si existen planes de contingencia, que salvaguarden la integridad de dispositivos de red en el Benemérito Liceo José Martí

Respuesta	**Frecuencia**	**Porcentaje**
Sí	0	0%
No	9	90%
No contestó	1	10%
Total	**10**	**100%**

Fuente: Creación propia, 2019.

El 90% del personal administrativo afirma no saber si existen planes de contingencia, que salvaguarden la integridad de dispositivos de red en el Benemérito Liceo José Martí, y el 10% restante no responde ninguna de las opciones.

Tabla #24 Aspectos encontrados y Recomendaciones

Aspectos encontrados	**Recomendaciones**
• Los equipos observados son de alta gama y se consideran adecuados para el desarrollo de las labores. • No existe ningún tipo de plan de contingencia relacionado con la integridad de los dispositivos de red.	• Capacitar, al personal administrativo, en materia básica de redes para que, así, conozcan un poco más sobre la funcionabilidad de los dispositivos de red en general. • Se recomienda la implementación de planes de contingencia, que ayuden a salvaguardar, en su totalidad, los dispositivos de red en el liceo.

5.14. Composición y cambios de la plataforma

Tener un control de la composición y cambios de la plataforma es importante porque ayuda a conocer cómo se encuentra conformado todo el sistema de red de la institución y poder determinar la mejor manera de administrar dichos activos.

Para el control de la composición y cambios de la plataforma, la institución cuenta con un inventario, que contiene las características físicas de los dispositivos junto con un identificador o placa, los datos que contiene el inventario son: marca, modelo, número de serie, memoria RAM y procesador, pero no indican cada cuánto hacen revisión del inventario, debido a que no existe un plan definido por fechas, solamente se efectúa cuando se requiere algún insumo del inventario.

5.15. Control de la ejecución de los trabajos

El control de la ejecución de los trabajos del área administrativa es importante, ya que ayuda a verificar si determinadas funciones del área de redes se están realizando de la manera correcta y eficiente.

En cuanto al control de la ejecución de los trabajos, la institución no cuenta con este tipo de control, como entidad pública todos los funcionarios están sujetos a que cada año deben realizar la rendición de cuentas donde deben especificar todas las funciones realizadas durante todo el año con la mayor transparencia posible.

5.16. Ambientes de desarrollo y producción

Le separación del ambiente de desarrollo y de producción es sumamente importante, ya que permite, a la institución, evolucionar e implementar nuevos servicios sin afectar la operatividad de los sistemas funcionales en producción.

En la entrevista realizada al encargado de informática del Liceo, se indica que el ambiente de producción y de desarrollo se encuentran separados; para las pruebas de red, el departamento de Tecnologías de Información cuenta con solo un conmutador de la marca D-Link, pero el encargado no especifica qué procesos se llevan a cabo para realizar las pruebas en la red.

Conforme a lo expresado anteriormente, se determina que la institución no cuenta con algún ambiente de pruebas establecido, se puede decir que las pruebas las realizan en el ambiente de producción y el conmutador, que poseen, lo utilizan como un sistema de prueba rudimentario, lo cual permite solamente realizar pruebas pequeñas.

5.17. Soporte a los equipos principales y periféricos

El soporte técnico de los equipos principales y periféricos del liceo es importante, ya que, si llegase a suceder un fallo en algunos dispositivos, la continuidad de los servicios puede verse afectada de manera negativa y, al contar con el soporte respectivo, ayuda a reducir el impacto de alguna eventualidad.

Mediante la encuesta dirigida al encargado de informática, él indica que el soporte técnico de los equipos principales y periféricos están bajo su cargo, en caso de alguna eventualidad, se le comunica vía telefónica y este debe encargarse de dar el soporte respectivo.

5.18. Control, rutinas de respaldo y sus procesos de restauración

Los respaldos y procesos de restauración son importantes para la institución porque da la seguridad de que la información importante se encuentre segura en caso de alguna eventualidad y que la misma pueda ser recuperada rápidamente, minimizando las pérdidas que puedan existir.

Actualmente, el Liceo no cuenta con hardware específico para realizar respaldos, pero se menciona que los respaldos del sistema PIAD se realiza en la nube, se utilizan las cuentas administrativas del liceo, estas cuentas son proporcionadas por el servicio de Google, estos respaldos son protegidos por contraseña y solamente el director y el encargado de Tecnologías de la Información tienen acceso a estas. Además, las contraseñas son agregadas a un expediente, esto se realiza con el fin de que, si se cambia de director, la nueva persona que ocupe dicho puesto pueda tener acceso a las copias de seguridad.

En cuanto a la restauración de los respaldos, los lineamientos utilizados son los brindados por el Ministerio de Educación Pública.

5.19. Control de los servicios e instalaciones externas

Gestionar el control de los servicios es muy importante, ya que, de esta manera, la institución asegura un desempeño correcto de estos recursos y que las instalaciones externas, que se realicen en los recursos tecnológicos de la institución, sean de forma exitosa y segura.

Para determinar el control de los servicios e instalaciones externas, se procede a consultar qué tipo de control existe para los servicios e instalaciones externas en el Benemérito Liceo José Martí.

El encargado de Tecnologías de la Información indica, a través de una encuesta, que, en las licitaciones de la institución, se solicita que toda configuración o instalación debe ir acompañada de capacitación al coordinador de recursos tecnológicos.

El control de los servicios e instalaciones externas, que se realizan en el Benemérito Liceo José Martí, es eficaz debido a que llevan un control adecuado de sus servicios y, en caso de una instalación externa, esta se efectúa junto al encargado de informática, lo cual es idóneo, pues se vela por la seguridad de los recursos de la institución.

Hallazgos sobre la documentación de la red física administrativa del Liceo

Actualmente, la institución es regulada por los lineamientos del Ministerio de Educación Pública y, al ser una entidad pública, se basan en el reglamento de la Contraloría General de la República, pero, en el momento de hacer contraste con la realidad del Liceo y de solicitar los documentos que indican los procedimientos para la red física administrativa, no se obtiene hallazgo alguno de estos, por lo que se puede deducir que no se posee un reglamento especializado en dicha área. De forma general, se puede decir que no existe el reglamento y los encargados del área de la red física administrativa realizan los procesos de forma empírica.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Con base en el análisis de la gestión de la seguridad del hardware de la red física administrativa, se concluye lo siguiente.

- Los servicios de mantenimiento son efectuados cada tres meses por parte del encargado, lo cual es un tiempo prudencial para el funcionamiento de los equipos.
- El desecho de equipo informático se realiza con actas de desecho y se coordina con la Municipalidad de Puntarenas para que se recolecte el equipo.
- A los dispositivos de la red administrativa, nunca se les ha realizado un análisis de seguridad física, situación que puede afectar la seguridad y disponibilidad de la red y sus equipos.
- El personal administrativo podría verse afectado en sus labores diarias por un corte repentino de electricidad, por causa del desconocimiento del tiempo de autonomía, que brinda el sistema de alimentación ininterrumpida.
- Debido a la seguridad y ventajas, que brinda la red cableada, se ha establecido que, en toda la red física administrativa del liceo, se utilice cableado y no forma inalámbrica.
- A pesar de estudios realizados por el Comité Nacional de Emergencias en el Liceo Benemérito José Martí, que indica que la infraestructura física del lugar (obra gris) es idónea y puede resistir diversos fenómenos

atmosféricos, algunos equipos físicos de red no se encuentran bien resguardados.

- La oxidación en el área donde se encuentra el liceo debido al salitre es elevada y los equipos corren el riesgo de deteriorarse con rapidez por no darles el debido mantenimiento.
- La institución no cuenta con documentación alguna sobre planes de contingencia y reglamentos que, específicamente, se refieran a la gestión de la red física administrativa, tanto como los procesos y responsabilidades que esto conlleva, debido a esto es probable que, en el momento de ocurrir una emergencia relacionada con el tema, el tiempo de reacción no sea eficiente, lo que ocasiona la caída de la red por un tiempo prolongado.
- De acuerdo con las características detectadas en el equipo del personal administrativo de la institución, se considera que es adecuado para el desarrollo de las tareas designadas en su área.
- La composición y cambios de la plataforma tecnológica se controla a través de un inventario, sin embargo, el encargado de TI no toma en cuenta la obsolescencia de los equipos, como factor para realizar los cambios de estos.
- No se lleva un control de los cambios físicos, que se realizan en la red administrativa (cambio de equipos, cableado…), por lo tanto, no se puede determinar, con exactitud, las mejoras o desperfectos existentes en la red.

- La institución no cuenta con una mesa de servicios, que ayude a llevar un control de las incidencias en la red física administrativa.
- La institución no cuenta con dispositivos físicos de respaldo, que permitan sustituir, de inmediato, algún equipo que se dañe y, con eso, contribuir a que el servicio no se paralice por una incidencia debido a desperfectos en la red administrativa.
- No existen políticas de seguridad física y ambiental, ni reglamentos y manuales relacionados con la red física administrativa con base en lo que dicen las Normas Técnicas para la Gestión y el Control de la Tecnologías de la Información, que establece la Contraloría General de la República.

El liceo debe enfocarse en lo que dictan las Normas Técnicas para la Gestión y el Control de la Tecnologías de la Información establecidas por la Contraloría General de la República, ya que son una herramienta de suma importancia para que todas las instituciones públicas puedan funcionar de forma homogénea. Con el fin de evitar problemas en la red física administrativa, se concluye que estas normas brindadas por la Contraloría son útiles y de gran provecho para el Benemérito Liceo José Martí.

6.2. Recomendaciones

Una vez analizada la seguridad física de la red administrativa, se recomienda lo siguiente.

- Cumplir con lo establecido en las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República, enfatizando los puntos 1.4.3 **Seguridad física y ambiental** y 4.2 **Administración y operación de la plataforma tecnológica** para el aseguramiento de la red administrativa y sus dispositivos.
- Capacitar, al personal administrativo, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información por la Contraloría General de la República, con el propósito de que los administrativos cumplan sus labores de acuerdo con lo establecido en las normas.
- La creación de reglamentación interna para la gestión de la red física administrativa, que tenga como base lo estipulado en las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República, asimismo, capacitar, al personal de la red administrativa, para que realicen sus labores con el buen accionar en el uso de la red.
- Implementar medidas, que aumenten la seguridad de los equipos informáticos y de la red del Benemérito Liceo José Martí, que repercuta en el aseguramiento de la información de la institución.

- Desarrollar procedimientos, que contribuyan a la gestión de las diversas tareas, que se realizan, o incidentes que puedan ocurrir en el área de la red administrativa. También brindar capacitaciones, al personal, sobre los procedimientos creados para que ellos puedan seguirlos de acuerdo con los pasos que cada uno poseen.
- Desarrollar lineamientos, que promuevan las buenas prácticas en el uso de la plataforma tecnológica de la red administrativa, y brindar capacitaciones, al personal, sobre ellas para que conozcan el correcto uso que deben tener con el equipo que tienen a su cargo.
- Documentar todo cambio, que se realice en la red administrativa, también se deben incluir todas las gestiones realizadas internamente por terceros, eso con el fin de tener un registro de todas las acciones que se han realizado en la red y saber quiénes intervienen.
- Realizar revisiones periódicas del estado de los dispositivos de la red administrativa, para saber si los dispositivos se encuentran seguros y funcionan de manera óptima, por otra parte, se deben realizar pruebas al sistema de alimentación ininterrumpida para determinar su tiempo de autonomía y saber si el periodo, que brindan, es suficiente para que el personal de la institución tome las medidas necesarias en caso de algún corte del fluido eléctrico.

CAPÍTULO VII

PROPUESTA

7.1. Reglamento para la gestión de la red física administrativa del Benemérito Liceo José Martí

Capítulo I

Disposiciones generales

Artículo 01. Propósito del Reglamento

El Reglamento para la gestión de la red física administrativa del Benemérito Liceo José Martí tiene como objetivo orientar la gestión y el uso de la red física administrativa de la institución. Está basado en las **Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)**, esto con la finalidad de procurar el uso eficiente y garantizar la seguridad física de los recursos existentes en la institución.

Artículo 02. Definiciones generales

Para este reglamento, se define TI.

Tecnologías de la Información (TI): Es el conjunto de dispositivos, redes, software integrados, que forman un sistema interconectado, en el cual se almacena, transmite y recupera información.

Artículo 03. Criterios generales

Corresponde a los encargados de la red física administrativa del Benemérito Liceo José Martí lo siguiente.

a. Emplear los conocimientos técnicos en el área de la red física administrativa, que le compete, emitir criterios técnicos atinentes a la materia, implementar medidas que salvaguarden la integridad de los dispositivos de la institución.

b. Implementar, en la institución, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información.

c. Proponer políticas, procedimientos con base en los puntos de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información expresados en el capítulo IV - Prestación de servicios y mantenimiento, punto 4.2 Administración y operación de la plataforma tecnológica, los cuales se desarrollan más adelante.

d. Establecer o modificar cambios en la estructura de la red física administrativa, para resguardar los componentes físicos existentes.

e. Implementar la tercerización de servicios o “outsourcing” cuando la problemática escala al conocimiento, que poseen los encargados de red física administrativa, esto para reducir el tiempo de recuperación de la red.

f. Identificar los requerimientos de la red física administrativa, tomando en cuenta la obsolescencia de los dispositivos con el fin de lograr la adquisición oportuna de recursos de TI.

g. Vigilar y apoyar los recursos de la plataforma tecnológica, tomando en consideración la capacidad, disponibilidad y el desempeño para brindar un mantenimiento eficaz de la red física administrativa y su correcta operación.

Artículo 04. Uso de los recursos físicos de red administrativa

a. Los recursos de red física administrativa existentes en la institución, que son asignados a empleados del sector administrativo, poseerán calidad de herramienta laboral y serán dominio de la institución, al igual que le información que almacenen los mismos.

Capítulo II

Administración y operación de la plataforma tecnológica

Artículo 05. Disponibilidad, capacidad, desempeño y uso de la plataforma tecnológica

a. El encargado de Tecnologías de la Información tendrá que vigilar la disponibilidad, capacidad, desempeño y uso de la plataforma tecnológica, asegurando que esta funcione correctamente.
b. El encargado de TI deberá mantener un registro de todas las fallas, que ocurran en la plataforma tecnológica, por lo cual tendrá que tomar medidas preventivas, que eviten la materialización de errores que afecten la operación de dicha plataforma.

c. El encargado de TI tendrá que realizar pruebas de desempeño y rendimiento periódicamente para evaluar la capacidad y el debido funcionamiento de la plataforma tecnológica, con la finalidad de advertir sobre riesgos, impactos o daños importantes en los equipos.

Artículo 06. Requerimientos presentes y futuros de la plataforma tecnológica

a. El encargado del área de TI deberá desarrollar un análisis enfocado en los requerimientos tecnológicos presentes y futuros de la plataforma tecnológica de la institución, tomando en cuenta todos los tecnicismos necesarios para que el planteamiento sea atinado con las necesidades existentes y, a su vez, prever la escalabilidad, tanto como la compatibilidad de los equipos para garantizar la oportuna adquisición de estos.
b. Una vez efectuado el análisis especificado en el punto “a”, el encargado debe identificar los equipos, que tengan un nivel de obsolescencia avanzado para proceder con el descarte de estos, una vez que los equipos de reemplazo sean adquiridos por la institución.
c. En el momento de realizar el desecho de los equipos obsoletos, se deberá seguir al pie de letra el procedimiento de **“Plan de desecho”**, para la debida eliminación de los equipos, que no tienen valor sustancial en las operaciones de la plataforma, tomando en cuenta la tercerización; dependiendo del tipo de equipo a procesar, se deberá coordinar con la compañía para que retire el equipo.

d. El encargado de TI tendrá que contar con el detalle del desecho de activos de la plataforma tecnológica; para ello, deberá registrar información, tal como: marca, número de activo, acta, la debida justificación por la cual se desechó el equipo y el nombre de la compañía a cargo de su reciclaje.

Artículo 07. Control de composición y cambios de la plataforma tecnológica

a. El encargado del área de TI deberá mantener una documentación adecuada de todos los componentes (hardware) de los dispositivos informáticos, por lo tanto, es responsabilidad de este remover y cambiar las partes internas de los equipos, tanto como la verificación física y periódica de estas.

Artículo 08. Soporte de los equipos principales y periféricos

a. El encargado de TI deberá realizar un cronograma, con el fin de brindar el soporte respectivo a todo el equipo de la red física administrativa de la institución.
b. El soporte de los dispositivos será contemplado desde la perspectiva de cada tipo de equipo de la plataforma tecnológica.
c. El soporte se deberá realizar cada tres meses y, de ser necesario, se realizará antes del periodo indicado.
d. El desarrollo del soporte del equipo físico de red administrativa estará a criterio técnico del encargado.

e. El soporte de los equipos principales y periféricos podrá ser efectuado por un tercero contratado con los conocimientos necesarios para realizar la tarea.
f. El encargado de TI deberá documentar todas las actividades realizadas en las labores de soporte de los equipos informáticos.

Artículo 09. Servicios e instalaciones externas

a. De requerirse un servicio tercerizado de instalación, se deberá justificar con fundamentos teóricos, por parte del encargado de TI, el por qué se requiere dicho servicio.
b. En relación con el punto anterior, el encargado de TI deberá efectuar un seguimiento completo de todas las actividades realizadas por el contratado.
c. Según el punto anterior, al finalizar las actividades, el personal contratado deberá realizar un informe completo de todos los cambios realizados.
d. El encargado de TI deberá elaborar un documento con todas las actividades realizadas por el tercero.

7.2. Plan de contingencia

> Un plan de contingencia es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas. En muchos casos, es un instrumento de gestión para el gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño. (EcuRed, s.f., p.1)

De igual forma, “es una manera de definir los procedimientos, objetivos y organización para que, en caso de una situación de desastre o emergencia, se disminuyan y minimicen las pérdidas, daños o víctimas del fenómeno natural o tecnológico que haya ocurrido”. (DiccionarioActual, s.f., p.1)

En general, se contextualiza como los pasos a seguir en caso de un altercado, que afecte directamente la funcionalidad de la institución, por lo que se requiere un manual, el cual brinde, de antemano, una solución atinada a la necesidad del momento.

7.2.1. Introducción

El siguiente documento enfatiza en el desarrollo de un plan de contingencias para el Benemérito Liceo José Martí en el área de la red física administrativa. Esta institución está ubicada en Puntarenas centro, el plan será basado acorde con lo planteado por la Contraloría General de la República en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).

Establece el objetivo principal y específico, además incluye el análisis y evaluación de los riesgos por cada punto de los capítulos de la Contraloría previamente especificados, así como los tipos de amenazas y vulnerabilidades, a los que se puede estar expuesto y la forma en que se puede efectuar el plan de contingencia para solventar el problema.

El plan de contingencia permite mantener la red física administrativa en operación frente a amenazas, que puedan ocurrir en el Liceo, minimizando el impacto negativo que puede repercutir en las operaciones de la institución.

7.2.2. Objetivo principal

Desarrollar un plan de contingencias, que permita disminuir el impacto de un altercado a nivel de la red física administrativa, mediante la implementación de una serie de pasos a seguir en caso de que alguna incidencia suceda, con el fin de disminuir o mitigar el impacto, que pueda ocasionar en la red administrativa y, por ende, en las labores que se realizan en la institución.

7.2.3. Objetivos específicos

Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre, por medio del plan de contingencias por realizar en el Liceo, para afrontar posibles improvistos.

Identificar los tipos de amenazas y vulnerabilidades, que existen en la red física administrativa.

Priorizar las actividades, que se deben llevar a cabo una vez que suceda algún altercado.

7.2.4. Plan de contingencia

A continuación, se desarrollará el plan de contingencias enfocado en la red física administrativa del Benemérito Liceo José Martí, con la finalidad de reforzar la acción del personal administrativo en torno a las contingencias, que pueden manifestarse.

7.2.4.1. Seguridad física y ambiental

Según la Contraloría General de la República, el punto que se refiere a la seguridad física y ambiental plantea que “La organización debe proteger los recursos de TI, estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos”. (Contraloría General de la República, 2007, p.3)

7.2.4.2. Controles de acceso a la institución

Para los controles de acceso a la institución, se identifican las siguientes amenazas y vulnerabilidades, así como la forma de solventar un incidente en caso de que suceda.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
Acceso no autorizado	Red física administrativa	• No existen separaciones entre los cubículos de la dirección del personal administrativo. • Inexistencia de límites físicos (puertas) hacia el área de administración. • Inexistencia de control de	Alta

		accesos en áreas administrativas. • No se realiza monitoreo CCTV (Circuito cerrado de televisión) de las personas que se encuentran en el área administrativa. • Robo o daño de equipos. • Pérdida o robo de información. • Daño a la credibilidad de la institución.	

En cuanto a los controles de acceso a la institución, es importante tener en cuenta los siguientes aspectos.

- Los límites físicos (puertas) del área administrativa deben estar siempre cerradas.

- Cada funcionario es responsable de sus llaves, no pueden prestarlas.
- Si se pierde la llave de una puerta, se debe cambiar el llavín; en caso de pérdida de la llave maestra, se debe cambiar el llavín de todas las puertas de la institución.
- En caso de que un funcionario salga a vacaciones, debe entregar las llaves de la oficina.
- Cuando un funcionario es despedido, debe entregar las llaves y, además, se debe cambiar el llavín de la oficina.
- Compra e implementación de un CCTV (Circuito cerrado de televisión), que se ubique en lugares estratégicos de la institución y sea monitoreado continuamente por el guarda de seguridad.
- Mejorar la distribución de los cubículos administrativos (separación adecuada de las oficinas), evitando el acceso no autorizado.
- Contratar seguro en contra de robo de equipo tecnológico, con el fin de recuperar la inversión del activo.
- Limitar la información en caso de amenaza para que, únicamente, el personal administrativo tenga conocimiento, de ser necesario se divulgará la información a todas las personas en la institución.
- En caso de que las personas corran peligro en la institución, debe seguirse el procedimiento de evacuación del edificio “Plan de evacuación”.

- Comprobación de todo el inventario del equipo de la red física administrativa, constatando que no haya habido ningún tipo de robo.
- En caso de robo, se debe revisar el registro de la boleta de entrada al Liceo, con el fin de verificar el ingreso de personal no autorizado, de esta manera, se toman las medidas respectivas.
- Negar el acceso o salida de personas no autorizadas al recinto durante una amenaza.
- En caso de robo, debe seguirse el procedimiento “Plan de acción ante robos y hurtos”, con el fin de comunicarlo a las autoridades correspondientes.

7.2.4.3. Ubicación física de los recursos de Tecnologías de la Información

Es muy importante tener en cuenta la ubicación física de los recursos de Tecnologías de la Información; por ello, se identifican las siguientes amenazas y vulnerabilidades, así como la forma de solventar un incidente en caso de que suceda.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
Fenómenos naturales (sismo o temblor).	Dispositivos informáticos de la red física administrativa.	• Los escritorios del equipo de cómputo son abiertos y no poseen rodines, lo que puede provocar la caída del dispositivo en caso de sismo. • Daño de los componentes internos de los equipos. • Pérdida de información. • Daño externo al equipo informático.	Alta

En cuanto a la ubicación física de los recursos de TI, es fundamental tener presente los siguientes aspectos.

- Asegurarse que el equipo informático siempre esté en un lugar adecuado.
- Cada equipo de cómputo debe tener su propio escritorio y tomar las medidas de seguridad, de manera que los dispositivos queden sujetos a este y no se muevan en caso de alguna eventualidad.
- Todo dispositivo informático debe estar alejado de las ventanas.
- El escritorio del equipo informático debe tener rodines o algún otro mecanismo, que le permita su movilización en caso de que suceda un sismo.
- Contratación de un seguro en contra de pérdida de equipo tecnológico por eventos, como fenómenos naturales, con el fin de recuperar la inversión del activo.
- En caso de que las personas corran peligro en la institución, debe seguirse el procedimiento de evacuación del edificio “Plan de evacuación”.
- Revisar el estado de todo el equipo informático con el que cuenta la institución.
- En caso de daño de los dispositivos informáticos, debe seguirse el procedimiento “Plan de acción ante daños de equipos informáticos”, con el fin de comunicarlo a la aseguradora correspondiente.

- Sí el equipo queda completamente inutilizable, debe seguirse el procedimiento “Plan de desecho” para eliminarlo adecuadamente.

7.2.4.4. Ingreso y salida de equipos de la institución

Para el ingreso y salida de equipos de la institución, se identifican las siguientes amenazas y vulnerabilidades, así como la forma de solventar un incidente, en caso de que suceda.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
Falta de conocimiento del control (boleta o bitácora) para el ingreso y la salida de dispositivos informáticos.	Dispositivos informáticos de la red física administrativa.	• Falta de comunicación por parte del encargado sobre la existencia de las políticas (boleta o bitácora).	Alta
• Robo de equipo informático. • Pérdida o robo de información. • Pérdida de componentes internos o externos de los equipos.		• Descontrol en el ingreso y salida de los equipos informáticos.	

Con el propósito de que se realice de manera correcta el ingreso y salida de equipos de la institución, se deben considerar los siguientes aspectos.

- Tener conocimiento sobre las políticas de entrada y salida de equipo informático de la institución.
- Brindar capacitaciones al personal sobre el uso de las boletas para el ingreso y salida de equipo informático.
- Tener un registro con las características, tanto físicas como lógicas, de todos los dispositivos informáticos con los que cuenta la institución.
- Establecer a cuáles funcionarios se les puede prestar el equipo informático, tomando en cuenta las labores que realiza, para determinar si se le puede otorgar el permiso para la salida del equipo.
- Comprobar que el equipo prestado se devuelva con las mismas condiciones en las que se entregó.
- Verificar continuamente que todos los componentes internos de los dispositivos funcionen correctamente.
- Revisar el registro de la boleta de entrada y salida de equipo informático, con el fin de verificar los activos, y, de esta manera, tomar las medidas respectivas.
- Actualizar el inventario para corroborar la existencia de los activos de la institución.

- Contratar seguro en contra de robo de equipo tecnológico, con el fin de recuperar la inversión del activo.
- En caso de robo, debe seguirse el procedimiento “Plan de acción ante robos y hurtos”, con el fin de comunicarlo a las autoridades correspondientes.

7.2.4.5. Control de los servicios de mantenimiento

El control de los servicios de mantenimiento es un punto fundamental, ya que los dispositivos informáticos requieren un mantenimiento prudente; por ello, se identifican las siguientes amenazas y vulnerabilidades.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
Inexistencia de un control (bitácora) sobre el mantenimiento, que se les brinda a los dispositivos informáticos.	Dispositivos informáticos de la red física administrativa.	• Descontrol en el mantenimiento de los equipos informáticos. • Deterioro o daño de los componentes internos del dispositivo informático. • Pérdida de información por daño del disco duro del computador.	Alta

En este caso, es fundamental tener en cuenta los siguientes aspectos.

- A los dispositivos informáticos, se les debe realizar el mantenimiento preventivo cada tres meses.
- Las áreas de la institución recibirán un cronograma donde se indicará el horario, en que se realizará el mantenimiento a los equipos de cómputo.
- Todo equipo informático debe estar en constante revisión, con el fin de que obtenga las actualizaciones más recientes.
- El mantenimiento preventivo del equipo informático debe ser controlado a través de una bitácora para tener un registro adecuado de los servicios de mantenimiento.

7.2.4.6. Controles para el desecho y reutilización de recursos de Tecnologías de la Información

Es necesario gestionar adecuadamente el desecho y reutilización de todo el equipo informático; por ello, se identifican las siguientes amenazas y vulnerabilidades.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
Inexistencia de un control para el desecho y la reutilización de recursos informáticos.	Dispositivos informáticos de la red física administrativa.	• Eliminación inadecuada del equipo o los componentes internos. • Contaminación por desechos tecnológicos. • Pérdida de componentes internos funcionales. • Pérdida del control de activos. • Pérdida de información por eliminación del disco duro o	Alta

		dispositivo de almacenamiento en buen estado.	

En este caso, es importante tener claro los siguientes aspectos.

- Los dispositivos informáticos, que presenten fallas, deben ser comunicadas inmediatamente al encargado de Tecnologías de la Información.
- En caso de que el dispositivo informático deba ser desechado, debe seguirse el procedimiento “Plan de desecho” para eliminarlo adecuadamente.

7.2.4.7. Continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas

Es importante mantener controlados, funcionando y seguros los equipos, que brindan el suministro de energía eléctrica, así como el cableado de datos y las comunicaciones inalámbricas; se identifican las siguientes amenazas y vulnerabilidades que pueden surgir en esta área.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
• Latencia o pérdida de conexión por cableado de datos en mal estado.	Cableado de datos de la red física administrativa.	• No se realizan las revisiones adecuadas al cableado de datos.	Alta
• La UPS no brinda la energía necesaria para mantener el equipo.	Dispositivos de suministro de energía eléctrica de la red física administrativa.	• La capacidad de la UPS es inferior a la que necesita el equipo. • No se realizan las revisiones adecuadas a las UPS.	Alta
• Pérdida de información.	Información del Liceo.	• Pérdida del fluido eléctrico. • Falla técnica del suministro de	Alta

		energía eléctrica en el momento del corte de electricidad.	

En cuanto a la continuidad, seguridad y control de suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas, es importante tener claro los siguientes aspectos.

- Cada cuatro meses se debe realizar un análisis de seguridad física a los dispositivos de suministro de energía eléctrica y al cableado de datos, por lo tanto, cada área de la institución recibirá un cronograma donde se indicará el horario, con el fin de que se retiren del área para que el encargado de informática realice las revisiones necesarias.
- El análisis de seguridad física a los dispositivos de suministro de energía eléctrica y al cableado de datos debe ser controlado a través de una bitácora para tener un registro adecuado de los equipos y áreas, en que se realizó el análisis.
- Si un dispositivo de suministro de energía eléctrica no funciona correctamente y debe ser desechado, debe seguirse el procedimiento “Plan de desecho” para eliminarlo adecuadamente.
- Los funcionarios del departamento de Tecnologías de la Información están en la obligación de brindar capacitaciones, al

personal, sobre el tiempo de autonomía, que brindan los dispositivos de suministro de energía eléctrica con los que cuenta la institución, con el fin de que tomen las precauciones necesarias en caso de un corte repentino de electricidad.

- Todo dispositivo informático de la institución debe estar conectado mediante la red cableada.
- El encargado de TI debe desinstalar el controlador de los dispositivos, que poseen conexión inalámbrica, con el fin de que ningún computador se logre conectar mediante WIFI.

7.2.4.8. Acceso de terceros

El acceso de terceros a la institución es un punto muy importante, ya que se debe gestionar adecuadamente el ingreso de estos, teniendo en cuenta la seguridad de los equipos de la red física administrativa; por ello, se identifican las siguientes amenazas y vulnerabilidades.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
• Acceso no autorizado de terceros. • Robo o daño de equipos. • Pérdida o robo de información.	Dispositivos informáticos de la red física administrativa.	• Inexistencia de límites físicos (puertas) hacia el área de administración.	Alta
• Conexiones de terceros a la red cableada.	Dispositivos informáticos de la red física administrativa.	• Puertos de puntos de red sin bloqueo.	Alta

En cuanto al acceso de terceros, es importante considerar los siguientes aspectos.

- Toda persona, que desee ingresar a la institución, debe llenar una boleta para poder llevar a cabo esta acción.

- Si algún tercero trae consigo un dispositivo informático que permita la conexión a la red cableada, deberá registrarlo e indicar el motivo por el cual quiere ingresar con dicho equipo y se comunicará al encargado de Tecnologías de la Información.
- Todos los puertos de los puntos de red sin utilizar deben estar bloqueados, esto con el fin de evitar el acceso no autorizado de un tercero a la red física administrativa.
- Los límites físicos (puertas) de todas las áreas de la institución deben estar siempre cerradas.
- En caso de robo, debe seguirse el procedimiento “Plan de acción ante robos y hurtos”, con el fin de comunicarlo a las autoridades correspondientes.
- En caso de que las personas corran peligro en la institución, debe seguirse el procedimiento de evacuación del edificio “Plan de evacuación”.

7.2.4.9. Riesgos asociados con el ambiente

Para los riesgos asociados con el medio ambiente, se identifican las siguientes amenazas y vulnerabilidades, así como la forma de solventar un incidente en caso de que suceda.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
Tormentas eléctricas y temporales pronunciados.	Dispositivos informáticos de la red física administrativa	• Choques eléctricos. • Daños por humedad	Alta
Incendios.	Dispositivos informáticos de la red física administrativa.	• Pérdida de equipo calcinado. • Pérdida de la instalación en general. • Daño a la instalación eléctrica, teniendo en cuenta que esta tiene una posibilidad baja.	Alta
Polvo	Dispositivos informáticos de la red física administrativa.	• Pérdida de equipos por altas temperaturas. • Cortos circuitos debido a la	Alta

		acumulación de polvo.	
Humedad	Dispositivos informáticos de la red física administrativa.	• Pérdida de equipos por altas concentraciones de humedad. • Cortos circuitos debido al exceso de humedad. • Sulfatado y oxidación de equipos de red debido a humedal y al salitre del mar.	Alta

En este caso en particular, las amenazas asociadas con riesgos del ambiente se dividen en cuatro: incendios, polvo, humedad, tormentas eléctricas y temporales pronunciados.

Tormentas eléctricas y temporales pronunciados

En caso de tormentas eléctricas y temporales pronunciados, se deberán de realizar las siguientes acciones.

- Evaluar, con especialistas en el área de la electricidad, cuáles son las mejoras, que se deben adaptar a la institución, para mitigar riesgos en cuanto a la caída de rayos y sus choques eléctricos.
- Valorar, en manos de expertos, en el área de la construcción, si la estructura, en la cual se albergan todos los dispositivos del área de la red física administrativa, cuenta como protección estructural ante filtraciones de agua por temporales pronunciados, de esta forma, se evita pérdida de equipo por filtraciones de agua.
- Realizar una inspección de las UPS utilizadas en los equipos de la red física administrativa, con la finalidad de mitigar un choque eléctrico de baja densidad.
- En caso de existir un peligro de mayor gravedad para la población de la institución, se deberá evacuar el edificio o el área afectada y seguir, al pie de letra, el “Plan de evacuación” de la institución.
- Analizar a profundidad los daños ocurridos para, de esta forma, iniciar con la reparación de lo ocurrido en el entorno de la red física, todo esto dirigido por los responsables del área y, a su vez, se deberá efectuar documentación, que realimente en caso de circunstancias similares en el futuro, todo esto con ayuda del “Registro de responsabilidades asociadas con la operación de la plataforma”.

Incendios

En caso de incendios, se deberán realizar las siguientes acciones.

- Inspeccionar la infraestructura para determinar si existen puntos vulnerables ante un incendio.
- Asegurar los equipamientos con pólizas, que cubran los daños en caso de un incendio y, así, no perder la totalidad de la inversión.
- Capacitar, a los responsables del área de informática, en la lucha contra incendios.
- Adquirir equipo de lucha contra incendios.
- Instalar sistemas de detección de incendios especializados en laboratorios informáticos.
- En caso de incendio, se deberá seguir el protocolo de “Plan de evacuación” para salvaguardar las vidas de las personas.

Polvo

En caso de exceso de polvo, se deberán realizar las siguientes acciones.

- Capacitar, a los responsables del área de informática, en torno a las buenas prácticas y el mantenimiento preventivo de los equipos físicos de la red administrativa.
- Adquirir equipo de limpieza especializado en equipo de cómputo.
- Aislar lo posible el equipo de red física administrativa del medio ambiente, por medio de estructuras de metal especializadas en equipo de cómputo.

- Realizar limpiezas periódicas.
- En caso del incendio debido a un corto circuito por el polvo, se deberá seguir el protocolo de “Plan de evacuación” para salvaguardar las vidas de las personas.
- Plantear rutinas de limpieza y adecuarse a la temporada del año en la que se encuentre, debido a que, en los inviernos, la cantidad de polvo es inferior al verano, esto debido a las lluvias que humedecen la tierra.

Humedad

En caso de exceso de humedad, se deberán realizar las siguientes acciones.

- Inspeccionar la infraestructura para determinar si existen puntos en los que exista mucha humedad para eliminarla y evitar una problemática.
- Adquirir equipos de enfriamiento de precisión, ya que estos regulan la temperatura y, a la vez, mantienen un nivel óptimo de humedad.
- Instalar sistemas de detección de humedad especializados en laboratorios informáticos.
- Revisar si existen posibles daños estructurales, que infieran directamente en la filtración de agua en cualquiera de los equipos físicos de la red administrativa.

- En caso del incendio debido a un corto circuito por la humedad, se deberá seguir el protocolo de “Plan de evacuación” para salvaguardar las vidas de las personas.
- En caso de corto circuito, se deberán desconectar los equipos afectados para evitar un posible incendio.
- Realizar inspecciones periódicas para evitar problemáticas en torno a la humedad.
- Aislar los equipos de las áreas en riesgo de humedad.

7.2.4.10. Administración de la plataforma tecnológica

Según la Contraloría General de la Republica, el punto relacionado con la administración y operación de la plataforma tecnológica, se refiere “La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas”. (Contraloría General de la República, 2007, p.15). Para lo anterior, se debe tener en consideración lo siguiente.

7.2.4.11. Documentación de los procedimientos y las responsabilidades asociados con la operación de la plataforma

La documentación de procedimientos y responsabilidades asociadas con la operación de la plataforma es una alternativa eficiente para poseer un control general del estado actual de la plataforma de la red física administrativa del Benemérito Liceo José Martí y los posibles cambios efectuados en la misma en el momento de efectuar mejoras.

De no poseer una documentación eficiente, se pueden presentar diversas amenazas y vulnerabilidades asociadas al descontrol, en cuanto a los procesos y responsabilidades sujetas a la operación en la red física administrativa.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
Evasión de responsabilidades ante un desastre debido a que no existe documentación de responsabilidades a nivel operativo de la plataforma.	Red física administrativa.	• Inexistencia de responsabilidades establecidas a nivel documental en la operación de la plataforma.	Alta

En cuento a este punto, es imprescindible considerar los siguientes aspectos.

- Organizar, de forma concreta y escrita, los responsables de atender las problemáticas existentes a nivel operativo de la plataforma en el “Registro de responsabilidades asociadas con la operación de la plataforma”.
- Documentar cualquier cambio o procedimiento por realizar en el área operativa de la plataforma en el “Registro de procedimientos asociados a la operación de la plataforma”.
- Comprobación de los procesos de la red física administrativa, de esta forma, constatar la problemática y la forma en la que deberá ser abordada.
- En caso de alguna problemática, se debe avisar a los usuarios para que dejen sus labores diarias por el tiempo, que determine el encargado de Tecnologías de la Información.
- Si se solventa algún problema y todo ha sido abordado de forma satisfactoria, se deberá apuntar en el “Registro de procedimientos asociados a la operación de la plataforma”, el resultado de lo realizado para normalizar las operaciones de la plataforma, esto con la finalidad de poseer un registro de todo lo realizado en torno a la operación de la plataforma para, en el futuro, abordar, de forma rápida y eficiente, una amenaza similar a la ocurrida.

7.2.4.12. Vigilancia en torno a la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas

La vigilancia en torno a la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas, son medidas, que deben emplearse en la red física administrativa del Benemérito Liceo José Martí, ya que permite obtener un conocimiento general sobre el estado de la plataforma y de su fiabilidad en el momento de hacer uso de esta. El rendimiento de los equipos se ve afectado debido al grado de exigencia infringido en los mismos, aumentando el tiempo de respuesta de estos.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
Fallas inesperadas.	Red física administrativa.	• Inexistencia de un registro de fallas frecuentes. • La disponibilidad de los servicios es afectada por problemas que afectan la red física administrativa.	Alta

		• Pérdida de equipos de red. • Obsolescencia de equipos.	
Bajo rendimiento de los dispositivos.	Red física administrativa.	• La plataforma puede no desempeñarse de forma idónea. • Pérdida de capacidad, desempeño y disponibilidad, debido a no realizar pruebas de esfuerzo en la red para determinar el estado de esta.	Alta

En cuanto a la disponibilidad, desempeño y uso de la plataforma, es necesario considerar los siguientes puntos.

- Emplear rutinas de rendimiento en el equipo físico, con el fin de no sobrecargar los dispositivos y los procesos, que se realizan en la institución.

- Evaluar periódicamente la calidad de los equipos para evitar la obsolescencia de estos y realizar un calendario de cambios de dispositivos o efectuar un arrendamiento de equipos con una compañía especializada en la materia.
- En caso de que un equipo sea de alta prioridad y presente desperfectos, se deberá desplegar el “Plan de acción ante daños de equipos informáticos”.
- Al ocurrir un desperfecto, el cual pueda ser solucionado por los encargados del área, se deberá llenar el “Registro de procedimientos asociados a la operación de la plataforma”.
- Emplear el concepto de las 3 V (vigilar, verificar y validar) para corroborar la disponibilidad de los servicios ofrecidos por la red administrativa del Benemérito Liceo José Martí diariamente.

7.2.4.13. Identificación de eventuales requerimientos presentes y futuros, planes para su satisfacción y oportuna adquisición de recursos de TI requeridos, tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas

En el momento de plantear los nuevos requerimientos de la red física administrativa del Benemérito Liceo José Martí, se deberán tener en cuenta los requerimientos presentes y futuros para el desarrollo satisfactorio de la infraestructura física de la red, es necesario hacer énfasis en la obsolescencia del equipo, el tipo de contingencias, que, frecuentemente, se puedan presentar, carga de trabajo y las nuevas

tendencias tecnológicas en torno a las redes para la oportuna adquisición de los equipos.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
Incompatibilidad de equipo en la red actual.	Red física administrativa.	• Los equipos no funcionarían adecuadamente a la necesidad. • Todos los procesos que implique el uso de la red se verían afectados.	Alta
Pérdidas y daños en equipos.	Red física administrativa.	• Obsolescencia de equipos físicos de red.	Alta

Para la identificación de eventuales requerimientos presentes y futuros, planes para la satisfacción y oportuna adquisición de recursos en la red física administrativa, se ha de priorizar, en manos del encargado de informática, un estudio continuo de las nuevas tecnologías en el área de las redes físicas para desarrollar los proyectos de mejora a corto y largo plazo, en cuanto a la infraestructura de la red física administrativa del

liceo, al reducir, considerablemente, los riesgos antes mencionados respecto al tema.

El encargado del departamento de informática será quien realice los análisis requeridos para realizar las adquisiciones de los equipos, acordes con la necesidades actuales y futuras.

Consideraciones en el momento de realizar el análisis.

- Escalabilidad y retrocompatibilidad de los equipos.
- Espacio físico, en el cual los equipos serán localizados.
- Marcas y casas comerciales predilectas.
- Coste de inversión.
- Presupuesto.
- Necesidades actuales y necesidades futuras.

El criterio del ingeniero informático encargado será la base por utilizar para las futuras adquisiciones de equipos para la red física administrativa del Benemérito Liceo José Martí.

7.2.4.14. Control de la composición y cambios de la plataforma, registro actualizado de sus componentes (hardware y software), custodia adecuada de licencias de software y verificaciones físicas periódicas

Para el control de la composición y cambios de la plataforma de la red física administrativa del Benemérito Liceo José Martí, se deberá poseer un registro completo de todos los componentes físicos y lógicos de la red física, lo cual permite saber la ubicación, número del activo, fecha de

compra y otros datos primordiales, que sirven en el momento de custodiar la integridad de estos.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
Pérdida de equipos.	Dispositivos físicos de la red administrativa.	• Robo de equipos. • Equipos extraviados. • Confusión de equipos al no estar documentados.	Alta

Para poseer un control completo en torno a este tema, se generó el “Control de la composición de la red física administrativa”, que tiene la particularidad de ser útil para el control de la composición de carácter físico y lógico de los equipos de red. En el momento de adquirir equipos nuevos, se deben documentar de forma en la que se posea una fuente amplia de datos para tener una referencia del estado actual de los equipos y software en los mismos.

Consideraciones al efectuar un control de composición de los equipos de red del Liceo.

- En el momento que la institución adquiera los equipos por medio del plan de adquisición, se deberá documentar todo el equipo entrante en el “Control de la composición de la red física administrativa”.
- Se deberá hacer, eventualmente, una actualización del estado de los equipos al menos dos veces al año.
- Cuando un equipo es retirado de la institución, se deberá documentar el retiro en el “Control de la composición de la red física administrativa”.

7.2.4.15. Control de ejecución de los trabajos mediante programación, supervisión y registro

El control de ejecución de los trabajos realizados por medio de programación, supervisión y registro, consiste en una observación en la cual se abordarán los procesos realizados en la red física administrativa, esto con el fin de crear un registro de cambios realizados a la misma, y, de esta forma, abordar incidentes futuros de una manera más efectiva.

Este control permite llevar a cabo, eficazmente, los trabajos de mantenimiento por ejecutar periódicamente, es por esto que es importante realizar un registro de las labores realizadas en la red.

Existen diversas amenazas y vulnerabilidades, al no existir un control de ejecución de los trabajos mediante programación, supervisión y registro en la institución, a continuación, se muestran en el siguiente recuadro.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
Daños en equipos de red.	Dispositivos físicos de la red administrativa.	• Los procedimientos o trabajos no se efectúan de forma paulatina, propician desperfectos en los equipos de red al no realizar ningún mantenimiento en tiempo prudencial. • Negligencias al no registrar los trabajos desarrollados, sumado a la no vigilancia de lo realizado.	Alta

Consideraciones al efectuar un control de ejecución de los trabajos mediante programación, supervisión y registro en la red del Liceo.

- Se requiere establecer los responsables del control de ejecución de trabajos mediante programación, supervisión y registro, por medio del “Registro de responsabilidades asociadas a la operación de la plataforma” para definir el encargado de realizar los trabajos o procedimientos en la red administrativa.
- Para el registro de trabajos realizados, se deberá emplear el “Registro de procedimientos asociados a la operación de la plataforma” para que, en el momento de realizar un trabajo, se efectúe realimentación.
- El director o un superior del área informática deberá realizar una revisión general sobre todos los procesos y trabajos realizados en la red de la institución.
- Se requiere establecer las fechas y los rangos de tiempos máximos en torno a los procesos y trabajos por realizar en la red, esto por mano de los especialistas del lugar, con la finalidad de no prolongar tiempos de mantenimiento de los equipos.

7.2.4.16. **Soporte requerido a los equipos principales y periféricos**

Es importante brindar el soporte requerido a todos los equipos principales y sus periféricos, con el fin de mantenerlos en buen estado y, así, estos trabajen correctamente; por ello se identifican las siguientes amenazas y vulnerabilidades.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
• Daño o deterioro de los equipos y periféricos. • La continuidad de los servicios puede verse afectada debido al daño de un equipo principal.	Dispositivos principales y periféricos de la red física administrativa.	• No se realiza el soporte respectivo a los equipos y periféricos.	Alta

En cuanto al soporte de los equipos principales y periféricos, es importante tener en consideración los siguientes aspectos.

- A los equipos informáticos y sus periféricos, se les debe realizar el soporte respectivo cada tres meses, con el fin de alargar el tiempo de vida útil de estos, por lo tanto, cada área de la institución recibirá un cronograma donde se indicará el horario, con el fin de que se retiren del área para que el encargado de informática realice dicha tarea.
- El soporte técnico del equipo informático o periféricos debe ser controlado a través de una bitácora para tener un registro adecuado del soporte brindado.
- En caso de daño menor, como un periférico, debe seguirse la boleta “Reporte de daños menores”, con el fin de comunicarlo al departamento de Tecnologías de la Información.

7.2.4.17. Rutinas de respaldo, custodio de medios de respaldo en ambientes adecuados, acceso a dichos medios y procedimientos de control para los procesos de restauración

Los respaldos, así como el proceso de restauración y el control de acceso a dichos medios, son fundamentales, ya que poseen la información diaria de las labores, que se realizan en la institución; por ello, se identifican las siguientes amenazas y vulnerabilidades.

Tipos de amenazas y vulnerabilidades

Amenazas	Sistemas afectables	Vulnerabilidades o posibles incidentes	Prioridad
• Daño físico y lógico de los respaldos. • Robo de las contraseñas y las copias de seguridad.	Información de la red física administrativa.	• El ambiente, donde se encuentran los respaldos y sus contraseñas, es inadecuado e inseguro.	Alta
• Respaldos sin cifrar.	Información de la red física administrativa.	• No se indicó una contraseña en el momento de realizar el respaldo.	Alta
• Pérdida de información.	Información de la red física administrativa.	• Falla del proceso de restauración. • Copia de seguridad realizada.	Alta

		incorrectamente .	
• Rutinas de respaldo inadecuadas.	Información de la red física administrativa.	• No se realizó, de manera idónea, el plan para los respaldos.	Alta

Con el propósito de que se realice un buen manejo de los respaldos de la institución, se deben considerar los siguientes aspectos.

- Solamente el director y el encargado de informática tendrán acceso a las copias de los respaldos y sus contraseñas.
- Todo tipo de respaldo realizado debe ir cifrado por contraseña.
- La contraseña de los respaldos **NO** debe ser menor a ocho caracteres y debe contener caracteres especiales.
- Se deberán realizar respaldos automáticos en el siguiente orden: un respaldo diferencial cada tres horas, iniciando a las 7 a.m., el respaldo incremental cada hora; y, por último, un respaldo completo a las 4 y 30 p.m. cuando se haya terminado el horario lectivo, se efectuará esta rutina de copias de seguridad de lunes a viernes.
- Todo dispositivo, que se utilice para realizar copias de seguridad, debe estar resguardado bajo llave y en un ambiente adecuado fuera de la institución (Banco).

- El proceso de restauración de la información solo debe ser realizado por el encargado de informática.

7.2.4.18. Servicios e instalaciones externos

Actualmente, la tercerización de servicios en las empresas es una opción viable para reducir tiempos de respuesta en el momento de instalar equipos físicos de red o resolver problemáticas no conocidas, para las cuales los responsables de la red física no han sido previamente capacitados.

Existen diversas amenazas y vulnerabilidades en torno a los servicios tercerizados en el Liceo, los cuales se denotan en la siguiente tabla.

Tipos de amenazas y vulnerabilidades

Amenazas	**Sistemas afectables**	**Vulnerabilidades o posibles incidentes**	**Prioridad**
Daños en equipos de red.	Dispositivos principales y periféricos de la red física administrativa.	• Los encargados de realizar el servicio tercerizado ocasionan daños en equipos.	Alta

		• El contratado para realizar el trabajo no posee el conocimiento necesario para desarrollar lo requerido.	

Para mitigar problemáticas en torno al presente punto, se deberán tener en cuenta los siguientes pasos.

- Realizar contratos para los servicios tercerizados, de esta forma, se esclarecerían las responsabilidades, que posee la persona o ente, que ofrezca los servicios tercerizados a la institución, especificando las garantías y procedimientos efectuados.
- El especialista encargado del área deberá supervisar los trabajos realizados por el contratado.
- En cuanto a lo relacionado con la instalación y otros servicios brindados por un tercero en la red física administrativa del Liceo, se establece que, en el momento de realizar cualquier tipo de actividad, el tercero y encargado del área deben recopilar información relativa en el “Registro de procedimientos asociados a la operación de la plataforma”.

- En el momento de finalizar los procedimientos realizados, se deberá verificar que se cumpla con todo lo establecido en el contrato, de no cumplirse con lo acordado en el contrato, el tercero deberá solventar el inconveniente.
- Verificar que la empresa o el tercero posea experiencia en el procedimiento por realizar, esto por medio de títulos, certificaciones y recomendaciones generadas por otras instituciones a las que se les haya realizado algún trabajo.

7.2.5. Procedimientos

7.2.5.1. Plan de acción ante daños de equipos informáticos

a. Introducción

El siguiente plan establecerá el procedimiento a seguir en caso de que algún dispositivo informático del Benemérito Liceo José Martí se dañe por eventos como fenómenos naturales.

b. Objetivo

Definir los procedimientos que se deberán seguir ante el daño de equipo informático del Benemérito Liceo José Martí.

c. Alcance

Los pasos de este plan deberán ser seguidos por docentes, administrativos o responsables de los activos después de ocurrido un daño a los dispositivos informáticos.

d. Definiciones

Empresa de seguro: Se refiere a la institución encargada de brindar pólizas con el fin de asegurar vehículos, dispositivos tecnológicos, casas, entre otros.

e. Procedimiento

En caso de que un dispositivo informático sufra algún daño se deberán realizar los siguientes pasos.

Actividad		Responsable
1	Informar la incidencia al director de la institución verbalmente y por escrito (En la carta deberá detallar el lugar, fecha y detallar lo sucedido).	Responsable del activo.
2	Verificar la incidencia reportada con el fin de confirmar los hechos.	Director, responsable del activo y el encargado de informática.
3	Comunicar el daño del equipo informático a la empresa de seguro correspondiente.	Director.
4	Se deberá esperar que la empresa de seguro revise el daño del equipo y evalué la reintegración del componente o dispositivo informático.	Director.
5	Sí la empresa aseguradora notifica que el equipo o componente informático ya no podrá volver a ser utilizado deberá seguirse el procedimiento “Plan de desecho”.	Empresa de seguros, director.

7.2.5.2. Plan de acción ante robos y hurtos

a. Introducción

El siguiente plan se establecerá el procedimiento a seguir en caso de suceda un robo o hurto de los activos fijos del Benemérito Liceo José Martí y así proceder de manera adecuada en estos casos.

b. Objetivo

Definir los procedimientos que se deberán seguir ante la situación de un robo o hurto de los activos fijos del Benemérito Liceo José Martí.

c. Alcance

Los pasos de este plan deberán ser seguidos por docentes, administrativos o responsables de los activos después de ocurrido un robo o hurto.

d. Definiciones

Robo: Es un delito penado por ley, donde los artículos son tomados utilizando la violencia, fuerzo o miedo.

Hurto: Es un delito penado por ley, donde los artículos son tomados contra la voluntad de las personas, ya sea por descuido ú olvido de los mismo.

Autoridades competentes: Se refiere a las autoridades más cercanas a la institución, ya sea una Delegación Policial o el Organismo de Investigación Judicial.

e. Procedimiento

En caso de robo o hurto se deberán realizar los siguientes pasos.

Actividad		**Responsable**
1	Informar la incidencia al director de la institución verbalmente y por escrito (En la carta deberá detallar el lugar, fecha y detallar lo sucedido)	Responsable del activo
2	Coordinar con el responsable del activo para determinar cuáles fueron los artículos sustraídos para corroborar que los activos faltantes coincidan con los descritos en la carta del funcionario afectado.	Director y asignación de activos
3	Interponer la denuncia ante las autoridades competentes.	Director
4	Se deberá esperar que la investigación realizada por las autoridades finalice y brindarle la información que ellos requieran.	Director
5	Determinar la responsabilidad del funcionario, analizando las evidencias y los criterios brindados por la	Director

	investigación realizada por las autoridades competentes.	
6	Ejecutar la baja contable del activo robado o hurtado	Contabilidad
7	Valorar la reposición del activo robado o hurtado	Contabilidad

7.2.5.3. Plan de desecho

a. Introducción

El siguiente plan establecerá el procedimiento a seguir en caso de que se deba desechar algún dispositivo informático del Benemérito Liceo José Martí.

b. Objetivo

Definir los procedimientos que se deberán seguir en caso de que un equipo informático quede completamente inutilizable y se deba realizar la eliminación adecuada del activo.

c. Alcance

Los pasos de este plan deberán ser seguidos por el jefe de informática, contabilidad y el director, en el momento en que el encargado de informática decida que el activo debe ser retirado.

d. Definiciones

Institución encargada de la recolección de desechos: Se refiere a la institución encargada del reciclaje de todo tipo de materiales y a la recolección de los desechos tecnológicos.

e. Procedimiento

En caso de tener que desechar un dispositivo informático se deberán realizar los siguientes pasos.

Actividad		Responsable
1	Revisar todo el equipo informático con el fin de comprobar si todos los componentes internos se encuentran dañados.	Encargado de informática.
2	Retirar los componentes internos que sirvan para ser reutilizados en otro dispositivo.	Encargado de informática.
3	En caso de que se haya dañado el disco duro del equipo informático o cualquier otro dispositivo de almacenamiento se deberá formatear a bajo nivel y perforarlo con múltiples agujeros.	Encargado de informática.
4	Realizar el acta de desecho del equipo o componente informático.	Encargado de informática.
5	Informar al departamento de contabilidad sobre el desecho para que realice la baja contable.	Encargado de informática.
6	Ejecutar la baja contable del equipo o componente informático.	Contabilidad.
7	Coordinar con la institución encargada para que realice la recolección del dispositivo o componente informático.	Director.

7.2.5.4. Plan de evacuación

a. Introducción

El siguiente plan se establecerá el procedimiento a seguir en caso de requerir evacuar las instalaciones del Benemérito Liceo José Martí y así proceder de manera adecuada en estos casos.

b. Objetivo

Definir los procedimientos que se deberán seguir ante la situación de evacuación de las instalaciones del Benemérito Liceo José Martí.

c. Alcance

Los pasos de este plan deberán ser seguidos por docentes, administrativos o responsables al momento de efectuar una evacuación.

d. Definiciones

Evacuación: Se refiere a evasión cuando se debe abandonar totalmente el edificio en el menor tiempo posible (incendios, terremotos, anuncio de bomba, hundimiento parcial del edificio, explosiones, daños graves en la estructura, fugas de gases, etc.)

Coordinadores de evacuación: conjunto de personas entrenadas para afrontar la evacuación de forma ordenada y respetando los márgenes de seguridad establecidos.

Profesor: docente encargado de impartir las lecciones que al momento de proceder con una evacuación pasa a ser ayudante de los coordinadores para así obtener la calma y el orden necesario para efectuar la evacuación.

e. Procedimiento

En caso de una evacuación se deberán realizar los siguientes pasos.

Actividad		**Responsable**
1	Emitir la señal de alarma o sirena para avisar que se inicia el plan de evacuación.	Coordinadores de evacuación y profesor responsable de cada grupo
2	Al escuchar la señal de alarma se deberá seguir a cabalidad lo indicado por el coordinador respectivo para desalojar el edificio, teniendo en cuenta que los primeros ocupantes a desalojar serán los de la plata baja.	coordinadores de evacuación y profesor responsable de cada grupo
3	Una vez evacuada la primera planta, la segunda se deberá dirigir de forma ordenada hacia la salida de emergencias más cercana, esto sin bajar a las plantas inferiores hasta que los ocupantes de la planta baja hayan salido en su totalidad por los coordinadores.	Coordinadores de evacuación y profesor responsable de cada grupo
4	El desalojo de los sectores se llevará acabo de la siguiente forma, será por grupos y las aulas más cercanas a las	Coordinadores de evacuación y profesor responsable de cada grupo

	salidas de emergencia serán las primeras en ser evacuadas, se deberá siempre respetar las señalizaciones existentes en el colegio sobre las salidas y las áreas seguras de la institución.	
5	Al desalojar por completo el edificio el profesor responsable de cada grupo deberá comprobar que todos los alumnos que se encontraban en la clase que impartía se encuentren fuera de la institución y en caso de faltar uno dar aviso a los coordinadores.	Coordinadores de evacuación y profesor responsable de cada grupo
6	En caso de que existan heridos de cualquier índole se deberá llamar al 911 para hacer el llamado de una ambulancia al lugar y así atender al herido.	Coordinadores de evacuación y profesor responsable de cada grupo

7.2.5.5. Registro de procedimientos asociados a la operación de la plataforma

a. Introducción

A continuación, se establecerán un formulario, mediante el cual se determinarán los procedimientos realizados o por realizar en la red física administrativa en el Benemérito Liceo Diurno José Martí, la finalidad de este informe será dar a conocer el estado de los procedimientos realizados y por realizar para poseer un respaldo informativo de los posibles escenarios que atenten contra la red y el cómo afrontarlos de forma rápida y precisa.

b. Objetivo

Establecer un informe por medio del cual se reportarán los cambios efectuados en la red física administrativa, de modo en que quedarán registros acerca de los cambios realizados, fecha en que se realizó y persona encargada de efectuar dichos cambios.

c. Alcance

Su alcance se enfoca principalmente en el personal administrativo encargado de la red física administrativa del Benemérito Liceo Diurno José Martí.

d. Formulario de informes

El siguiente formulario será empleado para poseer un registro completo de todos los procesos y cambios realizados a nivel de la infraestructura física de la red administrativa del Liceo Benemérito José Martí. El formulario es de carácter obligatorio para el encargado, ya que este mismo le permitirá tener una idea amplia sobre el cómo abordar casos con algún parentesco y así retornar la operación de la plataforma en un tiempo prudente y no demorando la operación de todo el personal administrativo.

Formulario de informes

Benemérito Liceo Diurno José Martí

Registro de cambios efectuados en la red física administrativa

Fecha: __ / __ /_____.

Hora: _____

Datos del encargado
Nombre:
Departamento:
Número de teléfono:
Cédula:
Firma:

Descripción del equipamiento				
Tipo de Equipo	Marca y modelo	Ubicación	Administrativo que realizo el reporte	Prioridad

Diagnóstico de la problemática		
Fallo	Motivo del cambio	Cambio efectuado

Observaciones:

_____.

Firma

7.2.5.6. Registro responsabilidades asociadas a la operación de la plataforma

a. Introducción

A continuación, se establecerán una serie de actividades, mediante las cuales se determinarán las responsabilidades que deberán realizar los encargados del área de la red física administrativa en la institución Benemérito Liceo Diurno José Martí.

b. Objetivo

Establecer las actividades y responsabilidades que deberán realizar los encargados del área de la red física administrativa en la institución Benemérito Liceo Diurno José Martí

c. Alcance

Su alcance se enfoca principalmente en el personal administrativo encargado de la red física administrativa del Benemérito Liceo Diurno José Martí.

d. Procedimientos y responsabilidades

Actividad		**Responsable**	**Periodos de revisión**
1.	Mantenimiento preventivo de la red administrativa.	Ingeniero Informático encargado o un tercero contratado por la institución	Cada 3 meses

2.	Reparaciones	Ingeniero Informático encargado o un tercero contratado por la institución	Cada vez que se requiera y prioridad este por encima de las tareas cotidianas
3.	Documentación de reparaciones realizadas	Ingeniero Informático encargado o un tercero contratado por la institución	Cada vez que se realiza una reparación
4.	Analizar el rendimiento de los dispositivos de la red para dar recomendaciones periódicas sobre la compra de nuevos equipamientos para mejorar la red física administrativa.	Ingeniero Informático encargado o un tercero contratado por la institución	Al menos una vez cada 6 meses
5.	Realizar cambios en la red física administra	Ingeniero Informático encargado o un tercero contratado por la institución	Cada vez que se requiera

7.2.5.7. Registro de daños menores

a. Introducción

A continuación, se establecerán un formulario, mediante el cual se efectúan los daños menores en la red física administrativa en el Benemérito Liceo Diurno José Martí, la finalidad de este informe será dar aviso de la existencia de un daño menor en la red.

b. Objetivo

Establecer un informe por medio del cual se reportarán los daños de poca gravedad en la red.

c. Alcance

Su alcance se enfoca principalmente en daños de baja prioridad y no impiden el funcionamiento de la red.

d. Formulario de informes

El siguiente formulario será empleado para daños menores a nivel de la infraestructura física de la red administrativa del Benemérito Liceo José Martí. El formulario es de carácter obligatorio para el encargado del activo, ya que este mismo permitirá a los encargados del área respectiva iniciar con el soporte y dar la solución.

Formulario de informes

Benemérito Liceo Diurno José Martí

Reporte de daños menores en la red física administrativa

Fecha: __ / __ /_____.

Hora: _____

Datos del Reporte
Nombre:
Departamento:
Número de teléfono:
Cédula:
Firma:

Descripción del equipo dañado				
Numero de activo:				
Tipo de Equipo	Marca y modelo	Ubicación	Administrativo que realizo el reporte	Prioridad

Observaciones:

_____.

Firma

7.2.5.8. Control de la composición de la red física administrativa

La siguiente imagen muestra una tabla de la forma de realizar el inventario y retiro de hardware. (Ver anexo #5)

BIBLIOGRAFÍA

Abad, A. (2013). *Redes locales*. Recuperado de https://ebookcentral.proquest.com/lib/biblioutnsp/reader.action?docID=3212697&query=+Abad+Domingo

Alonso, A., García, L., León, I., García, E., Gil, B., Ríos, L. (s.f.). *Métodos de investigación de enfoque experimental*. Recuperado de http://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/10.pdf

Ayala, E., Gonzáles, S. (2015). *Tecnologías de la información y la comunicación*. Recuperado de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/1189/Libro%20TIC%20%282%29-1-76%20%281%29.pdf?sequence=1&isAllowed=y Libro en línea

Barrantes Echavarría, Rodrigo. Investigación: un camino al conocimiento, un enfoque cualitativo, cuantitativo y mixto / Rodrigo Barrantes Echavarría. – 2 ed. – San José, C.R.: EUNED

Bernal, C. (2010). Metodología de la investigación, administración, economía, humanidades y ciencias sociales (3a ed.). Colombia: Prentice Hall.

Bellido, E. (2014). *Equipos de interconexión y servicios de red (UF1879).* Recuperado de https://ebookcentral.proquest.com/lib/biblioutnsp/reader.action?docID=4310541&query=Modelo+TCP%2FIP

Castaño, R., López, J. (2013). *Redes locales*. Recuperado de https://ebookcentral.proquest.com/lib/biblioutnsp/reader.action?docID=3217345&query=redes+de+telecomunicaciones

Cedeño, N. (2012). *La investigación mixta, estrategia andragógica fundamental para fortalecer las capacidades intelectuales superiores*. Recuperado de http://biblio.ecotec.edu.ec/revista/edicion2/LA%20INVESTIGACI%C3%93N%20MIXTA%20ESTRATEGIA%20ANDRAG%C3%93GICA%20FUNDAMENTAL.pdf

Centro de Investigaciones Sociológicas. (s.f.). *¿Qué es una encuesta?* Recuperado de http://www.cis.es/cis/opencms/ES/1_encuestas/ComoSeHacen/queesunaencuesta.html

Cisco NetAcad. (2018). *Introducción a las redes*. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#6.0.1.1

Cisco NetAcad. (2018). Introducción a las redes. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#7.0.1.1

Contraloría General de la República. (2007). *Normas técnicas para la gestión y el control de las Tecnologías de Información*. Recuperado de https://cgrfiles.cgr.go.cr/publico/docsweb/documentos/auditoria/normas-tecnicas-gestion-ti-n-2-2007-co-dfoe.doc

Dirección Regional Educación Puntarenas. (s.f.). *Benemérito Colegio José Martí*. Recuperado de http://www.drep.go.cr/index.php/circuitos-educativos/circuito-05/centro-educativos/colegio-jose-marti

Dirección Regional Educación Puntarenas. (s.f.). *Circuito 05*. Recuperado de http://www.drep.go.cr/index.php/circuitos-educativos/circuito-05/informacion

Espinosa, L. (2015). *Influencia de las auditorías dentro de las organizaciones.* Recuperado de http://cmas.siu.buap.mx/portal_pprd/work/sites/contaduria/resources/LocalContent/243/2/No.%202%20Influencia%20Auditoria%20en%20las%20Organizaciones.pdf

EcuRed. (s.f.). *Conmutación (redes de comunicación).* Recuperado de https://www.ecured.cu/Conmutaci%C3%B3n_(Redes_de_comunicaci%C3%B3n)

EcuRed. (s.f.). *Control de acceso*. Recuperado de https://www.ecured.cu/Control_de_acceso

Ex Libris. (s.f.). *Cuerpo general de la tesis o trabajo de investigación.* Recuperado de http://ex-libris.weebly.com/uploads/8/4/4/6/8446807/4.4_cuerpo_del_trabajo_de_investigacin.docx

Gamez, D. (2012). *Metodología para el análisis y diseño de redes, fundamentos en ITIL 4, para empresas de servicio.* [PDF]. Recuperado de https://repository.unilibre.edu.co/bitstream/handle/10901/6372/GamezPrietoDanielAlberto%202012.pdf?sequence=1&isAllowed=y

Guelmes, E., & Nieto, L. (2015). Algunas reflexiones sobre el contexto mixto de la investigación pedagógica en el contexto cubano. *Revista Universidad y Sociedad*. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202015000100004

Hamui-Sutton, A. (2013). *Un acercamiento a los métodos mixtos de investigación en educación médica.* [PDF]. Recuperado de https://ac.els-cdn.com/S2007505713727145/1-s2.0-S2007505713727145-main.pdf?_tid=aa8301cd-c6e4-4a33-8053-ff4cc637b643&acdnat=1543784696_345f7df477a47cfa5c3612a90b1ed838

ISACA. (s.f.). *Preguntas frecuentes: COBIT 2019.* Recuperado de http://www.isaca.org/COBIT/Pages/FAQs-COBIT-2019.aspx

ISOTools. (s.f.). *Normas ISO.* Recuperado de https://www.isotools.org/normas/

Jensy Campos Céspedes. (2015). *Cómo hacer un trabajo final de graduación: lineamientos para la Escuela de Ciencias de la Educación.* San José, C.R: EUNED.

Joskowicz, J. (2015). *Breve historia de las telecomunicaciones*. Recuperado de http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Historia%20de%20las%20Telecomunicaciones.pdf

Leguia, J. (s.f.). *Qué es un marco metodológico.* Recuperado de http://www.academia.edu/7235451/Que_es_un_marco_metodologico

López, P., Fachelli, S. (2015*). Metodología de la investigación social cuantitativa.* Recuperado de https://ddd.uab.cat/pub/caplli/2016/163567/metinvsoccua_a2016_cap2-3.pdf

Ludewig, C. (s.f.). *Universo y muestra. [PDF].* Recuperado de http://www.smo.edu.mx/colegiados/apoyos/muestreo.pdf

Martin, G., Olmedo, V., Andoney, J. (2017). *Uso de las tecnologías de la información y comunicación (TIC) en las residencias médicas en México.* Recuperado de http://www.scielo.org.mx/pdf/amga/v15n2/1870-7203-amga-15-02-00150.pdf

Mora, A. (2016). *Gestión de la prevención. Control de accesos* (tesis de maestría). Universidad Politécnica de Cartagena, Murcia, España. Recuperado de http://repositorio.upct.es/bitstream/handle/10317/5636/tfm-mor-ges.pdf?sequence=3

Parson, A. (s.f.). *¿Cuáles son las diferencias entre acceso lógico y acceso físico?* Recuperado de https://techlandia.com/cuales-son-diferencias-acceso-logico-acceso-fisico-info_202346/

Pérez, D. (2017). *Auditoría informática.* Recuperado de http://fernando123ldu.blogspot.com/p/objitivos-de-la-auditoria.html

Psyma. (2015). *La etnografía como herramienta en la investigación cualitativa.* Recuperado de http://www.psyma.com/company/news/message/la-etnografia-como-herramienta-en-la-investigacion-cualitativa

Escárcega, D. (s.f.). *¿Qué es la investigación correlacional?* Recuperado de https://www.questionpro.com/blog/es/investigacion-correlacional/

Real Academia Española. (s.f.). *Norma.* Recuperado de http://dle.rae.es/srv/search?m=30&w=norma

Rivas, J. (s.f.). *El enfoque mixto en los procesos de investigación*. Recuperado de http://biblo.una.edu.ve/documentos/enfoque.pdf

Roca, J. (s.f.). *¿Qué son las TI?* Recuperado de http://www.informeticplus.com/que-son-las-tecnologias-de-la-informacion

Rodríguez, R. (2014). *Desarrollo del proyecto de la red telemática (UF1870*). Recuperado de https://ebookcentral.proquest.com/lib/biblioutnsp/reader.action?docID=4310537&query=Redes+de+conmutaci%C3%B3n

Rosero Álvarez, E. (2014*). Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado.* Recuperado de http://www.dspace.uce.edu.ec/bitstream/25000/2464/1/T-UCE-0011-81.pdf

Sancler, V. (s.f.). *Redes de computadoras*. Recuperado de https://www.euston96.com/redes-de-computadoras/

Santín, O. (2018). Seguridad del entorno informático, unidad III. Puntarenas, Costa Rica. Universidad Técnica Nacional.

Sanz, R. (2017). *¿Qué es el método cuantitativo?* Recuperado de https://cursos.com/metodo-cuantitativo/

Seas Tencio, J. (2017). *Didáctica General I*. San José. CR: EUNED

Significados. (2018). *Significado de marco teórico.* Recuperado de https://www.significados.com/marco-teorico/

Tapia, E. (2016). *Investigación educativa: fundamentos para la investigación formativa*. Enciclopedia Virtual [versión electrónica]. eumed.net: Enciclopedia Virtual., http://www.eumed.net/libros-gratis/2016/1553/narrativas.htm

Tipos de investigación. (2018). *Tipos de investigación.* Recuperado de https://www.tesiseinvestigaciones.com/tipo-de-investigacioacuten-a-realizarse.html

Torres, Mariela., Paz, Karim. (2014). *Métodos de recolección de datos para una investigación.* [PDF]. Recuperado de https://s3.amazonaws.com/academia.edu.documents/33095415/METODOS_DE_RECOLECCION_DE_DATOS_PARA_UNA_INVESTIGACION.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1542840147&Signature=28rcIXHaSsoWPf7jPzwrrl8PiUA%3D&response-content-

disposition=inline%3B%20filename%3D6_02_14_METODOSDERECOLECCIONDEDATOSPARAU.pdf

Ulloa, A. (2012). *Población y tamaño de la muestra en la investigación científica*. Revista Alternativa Financiera. Recuperado de http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=4&sid=dcbb226c-bf82-476a-b75b-75b7c92fd204%40sdc-v-sessmgr06

Universidad Autónoma del Estado de Hidalgo. (s.f.). *Comunicaciones en* redes*, conmutador.* Recuperado de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/483_conmutador.html

Universidad Autónoma del Estado de Hidalgo. (s.f.). *Comunicaciones en redes, Ruteadores.* Recuperado de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/485_ruteadores.html

Universidad Autónoma del Estado de Hidalgo. (s.f.). *Comunicaciones en redes, repetidores.* Recuperado de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/481_repetidor.html

Universidad de Granada. (s.f.). *Arquitecturas de red: transmisión de datos y redes de ordenadores*. Recuperado de https://elvex.ugr.es/decsai/internet/pdf/2%20Arquitecturas%20de%20red.pdf

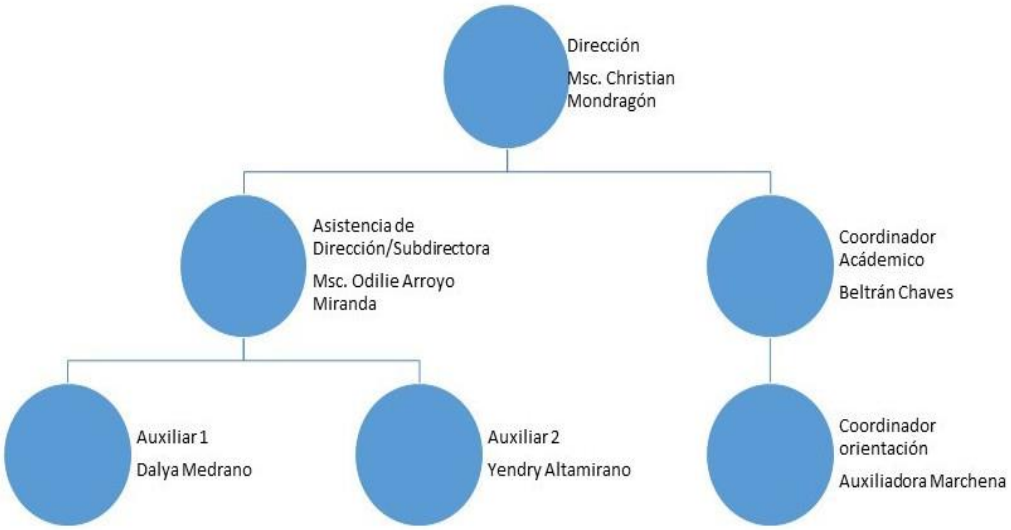
Vera, L. (s.f.). *La investigación cualitativa*. Recuperado de http://www.trabajosocial.unlp.edu.ar/uploads/docs/velez_vera__investigacion_cualitativa_pdf.pdf

XITH. (s.f.). *Auditorías de seguridad en TI.* [PDF]. Recuperado de https://www.xith.com.mx/services/Auditorias%20de%20Seguridad%20-%20XITH.pdf

Yanez, D. (s.f.). Características, técnicas y ejemplos. Recuperado de https://www.lifeder.com/investigacion-explicativa/

ANEXOS

Anexo #1: Organigrama del Benemérito Liceo José Martí



Fuente: Creación propia, 2019.

Anexo #2: Cuestionario para el personal administrativo

El siguiente cuestionario tiene como objetivo obtener los conocimientos, que posee el personal administrativo del Benemérito Liceo José Martí, en cuanto a la administración de la seguridad física de la red administrativa. La forma de llenar el cuestionario será por medio de una letra “X” en la respuesta pertinente al criterio personal de cada uno de los encuestados, solo una “X” por cada pregunta.

1. ¿Cuenta la institución con políticas de seguridad física y ambiental para sus dispositivos informáticos? Si la respuesta es “No” o “No sé”, pase a la pregunta número 6.

   Sí ( ) No ( ) No sé ( )

2. ¿Tiene conocimiento de las políticas anteriormente mencionadas?

   Sí ( ) No ( )

3. ¿Tiene acceso a las políticas de seguridad físicas y ambientales?

   Sí ( ) No ( )

4. ¿Ha recibido alguna capacitación con respecto al tema de la seguridad física y ambiental? Si la respuesta es “No”, pase a la pregunta número 6.

   Sí ( ) No ( )

5. ¿Con qué frecuencia recibe este tipo de capacitaciones? De ser otra su respuesta, llene en el espacio “Especifique”.

   Una vez al año ( ) Dos veces al año ( ) Otra ( )

   Especifique:

   _____

   _____

6. ¿Se ha realizado alguna vez un análisis de seguridad física a los dispositivos de red? Si la respuesta es “No” o “No sé” pase a la pregunta número 8.

   Sí ( ) No ( ) No sé ( )

7. ¿Con qué frecuencia se realizan dicho análisis?

   Cada tres meses ( ) Cada seis meses ( ) Cada año ( )

8. ¿Conoce la ubicación de los dispositivos físicos de la red?

   Sí ( ) No ( )

9. ¿Con qué frecuencia se realiza el mantenimiento de los dispositivos físicos de la red?

   Cada tres meses ( ) Cada seis meses ( ) Cada año ( )

10. ¿Cuenta la institución con un control para el desecho y reutilización de los dispositivos de red? Si la respuesta es “No” o “No sé”, pase a la pregunta número 13.

    Sí ( ) No ( ) No sé ( )

11. ¿Tiene conocimiento de dichos controles?

    Sí ( ) No ( )

12. ¿Tiene acceso a la información sobre los controles para el desecho y reutilización de los dispositivos de red?

    Sí ( ) No ( )

13. ¿Ha recibido alguna capacitación sobre el manejo del equipo informático, que se encuentra bajo su cargo? Si la respuesta es “No”, pase a la pregunta número 16.

    Sí ( ) No ( )

14. ¿Con qué frecuencia recibe este tipo de capacitaciones? De ser otra su respuesta, llene en el espacio “Especifique”

    Una vez al año ( ) Dos veces al año ( ) Otra ( )

    Especifique:

    _____

    _____

15. ¿Quién es el encargado de brindar dichas capacitaciones?

    Especifique:

    _____

    _____

16. ¿Conoce la existencia de un plan de contingencias en el área de informática, que resguarde la integridad de los dispositivos de red? Si la respuesta es “No”, pase a la pregunta número 22.

    Sí ( ) No ( )

17. ¿Tiene conocimientos de cómo utilizar el plan de contingencia?

    Sí ( ) No ( )

18. ¿Ha recibido alguna capacitación sobre el plan de contingencias?

    Sí ( ) No ( )

19. ¿Con qué frecuencia recibe este tipo de capacitaciones? De ser otra su respuesta, llene en el espacio “Especifique”

    Una vez al año ( ) Dos veces al año ( ) Otra ( )

    Especifique:

    _____

    _____

20. ¿Tiene acceso a la documentación sobre este plan de contingencias?

    Sí ( ) No ( )

21. ¿Considera usted que dicho plan será efectivo ante alguna eventualidad en el área de informática en torno a los dispositivos de red? Debe justificar su respuesta.

    Sí ( ) No ( )

    Justifique:

    _____

    _____

22. ¿Considera usted que los dispositivos físicos de red encontrados en la institución brindan una buena calidad de servicios? Si la respuesta es “No,” debe justificar.

    Sí ( ) No ( )

    Justifique:

    _____

    _____

    _____

23. ¿Considera usted que los dispositivos físicos de red en la institución son adecuados para la realización de sus labores? Si la respuesta es “No”, debe justificar.

    Sí ( ) No ( ) No sé ( )

    Justifique:

    _____

    _____

    _____

24. ¿Existe alguna política para la extracción de equipos de la institución? Si la respuesta es “No” o “No sé,” pase a la pregunta número 27.

    Sí ( ) No ( ) No sé ( )

25. ¿Tiene conocimiento de la política anteriormente mencionada? De ser “Sí” su respuesta, especifique brevemente qué procede cuando se extrae un equipo de la institución.

    Sí ( ) No ( )

    Especifique:

    _____

    _____

    _____

    _____

26. ¿Tiene acceso a la política de extracción de equipos de la institución?

    Sí ( ) No ( )

27. ¿Existe un sistema de alimentación ininterrumpida? De ser “Si” su respuesta, conteste la pregunta número 28.

    Sí ( ) No ( )

28. ¿Cuánto tiempo de autonomía brinda el sistema de alimentación ininterrumpida?

    15 minutos ( ) 30 minutos ( ) 1 hora ( ) No sé ( )

Anexo #3: Cuestionario para el personal de tecnologías de información

El cuestionario, a continuación, tiene el objetivo de recabar la información de cómo el personal de tecnologías de información realiza la administración de la seguridad física de la red administrativa del Benemérito Liceo José Martí. La forma de llenar el cuestionario será por medio de una letra “X” en la respuesta pertinente al criterio personal de cada uno de los encuestados, solo una “X” por cada pregunta.

1. ¿Cuenta la institución con políticas de seguridad física y ambiental para sus dispositivos informáticos? Si la respuesta es “No”, pase a la pregunta número 5.

   Sí ( ) No ( )

2. ¿El personal de la institución posee acceso a la información de las políticas anteriormente mencionadas?

   Sí ( ) No ( )

3. ¿El personal de la institución ha recibido alguna capacitación sobre la seguridad física y ambiental? Si la respuesta es “No”, pase a la pregunta número 5.

   Sí ( ) No ( )

4. ¿Con qué frecuencia se brinda este tipo de capacitaciones? De ser otra su respuesta, llene en el espacio “Especifique”

   Una vez al año ( ) Dos veces al año ( ) Otra ( )

   Especifique:

   _____

   _____

5. ¿Se ha realizado alguna vez un análisis de seguridad física a los dispositivos de red? Si la respuesta es “No”, pase a la pregunta número 7.

   Sí ( ) No ( )

6. ¿Con qué frecuencia se realiza dicho análisis?

   Cada tres meses ( ) Cada seis meses ( ) Cada año ( )

7. ¿Existe el debido control de los servicios de mantenimiento en los equipos físicos de la red administrativa?

   Sí ( ) No ( )

8. ¿Qué tipo de mantenimiento se realiza en los dispositivos físicos de red? Especifique:

   _____

   _____

   _____

   _____

   _____

9. ¿Con qué frecuencia se realiza el mantenimiento de los dispositivos físicos de la red?

   Cada tres meses ( ) Cada seis meses ( ) Cada año ( )

10. ¿Cuenta la institución con un control para el desecho y reutilización de los dispositivos de red? Si la respuesta es “No”, pase a la pregunta número 12.

    Sí ( ) No ( )

11. ¿El personal de la institución posee acceso a la información sobre los controles para el desecho y reutilización de los dispositivos de red?

    Sí ( ) No ( )

12. ¿Se realiza un borrado seguro de los archivos y configuraciones de todos los dispositivos antes de ser reciclados? Si la respuesta es “No”, pase a la pregunta número 14.

    Sí ( ) No ( )

13. ¿Qué tipo de proceso se sigue para el desecho del equipo informático?

    Especifique:

    _____

    _____

    _____

    _____

14. ¿El personal de la institución ha recibido alguna capacitación sobre el manejo del equipo que se encuentra a su cargo? Si la respuesta es “No”, pase a la pregunta número 16.

    Sí ( ) No ( )

15. ¿Con qué frecuencia se brinda este tipo de capacitaciones? De ser otra su respuesta, llene en el espacio “Especifique”

    Una vez al año ( ) Dos veces al año ( ) Otra ( )

    Especifique:

    _____

16. ¿Existe algún plan de contingencias en el área de informática, que resguarde la integridad de los dispositivos de red? Si la respuesta es “No”, pase a la pregunta número 20.

    Sí ( ) No ( )

17. ¿El personal de la institución ha recibido alguna capacitación sobre el plan de contingencias en el área de informática, que resguarde la integridad de los dispositivos de red? Si la respuesta es “No”, pase a la pregunta número 20.

    Sí ( ) No ( )

18. ¿Con qué frecuencia se brinda este tipo de capacitaciones? De ser otra su respuesta, llene en el espacio “Especifique”.

    Una vez al año ( ) Dos veces al año ( ) Otra ( )

    Especifique:

    _____

19. ¿Considera usted que dicho plan será efectivo ante alguna eventualidad en el área de informática en torno a los dispositivos de red? Debe justificar su respuesta.

    Sí ( ) No ( )

    Justifique:

    _____

    _____

    _____

    _____

    _____

20. ¿Considera usted que los dispositivos físicos de red encontrados en la institución brindan una buena calidad de servicios? Si la respuesta es “No”, debe justificar.

    Sí ( ) No ( )

    Justifique:

    _____

    _____

    _____

    _____

    _____

21. ¿Considera usted que los dispositivos físicos de red en la institución son adecuados para realizar las labores de la institución? De ser negativa su respuesta, debe justificar.

    Sí ( ) No ( )

    Justifique:

    _____

    _____

    _____

    _____

    _____

22. ¿Existe alguna política para la entrada y salida de equipos de la institución? Si la respuesta es “No”, pase a la pregunta número 25.

    Sí ( ) No ( )

23. ¿El personal de la institución ha recibido información sobre la política anteriormente mencionada? Si la respuesta es “No”, pase a la pregunta número 25.

    Sí ( ) No ( )

24. ¿A través de cuál medio da a conocer estas políticas al personal de la institución? Si la respuesta es “Otro”, debe especificar

    Correo Electrónico ( ) Capacitaciones ( ) Otro ( )

    Especifique:

    _____

    _____

25. ¿Existe un sistema de alimentación ininterrumpida? Si la respuesta es “No”, pase a la pregunta número 27.

    Sí ( ) No ( )

26. ¿Cuánto tiempo de autonomía brinda el sistema de alimentación ininterrumpida?

    15 minutos ( ) 30 minutos ( ) 1 hora ( )

27. ¿Con cuántos proveedores de internet cuenta la institución?

    1 Proveedor ( ) 2 Proveedores ( ) 3 Más ( )

28. ¿Existe algún plano de la instalación del cableado de red de toda la institución? Si la respuesta es “No”, pase a la pregunta número 30.

    Sí ( ) No ( )

29. ¿Con qué frecuencia se actualiza el plano de la instalación del cableado de red? Si la respuesta es “Otra”, llene en el espacio “Especifique”

    Una vez al año ( ) Dos veces al año ( ) Otra ( )

    Especifique:

    _____

    _____

30. ¿Cuentan con un control de acceso a terceros en el área en la que se encuentran los equipos físicos de la red administrativa?

    Sí ( ) No ( )

Anexo #4: Encuesta para el personal de tecnologías de información

La encuesta tiene el objetivo de obtener información sobre la administración y operación de los dispositivos físicos de la red administrativa del Benemérito Liceo José Martí.

1. ¿Qué procedimiento se sigue para asignarle un dispositivo tecnológico a una persona?
2. ¿Existe algún control sobre las responsabilidades que tiene el personal con el equipo informático y cómo se cercioran que se cumpla?
3. ¿Qué tipo de procesos se realizan para corroborar que la red administrativa funcione de forma correcta?
4. ¿Poseen un control de fallas de la red, se toma nota cuando ocurre una incidencia?
5. ¿Prevén dentro del plan operativo la compra de nuevo equipo informático y qué se toma en cuenta para hacer el cambio de dispositivos?
6. ¿Cómo se lleva el control sobre los equipos informáticos dentro de la institución?
7. ¿Cómo se resguardan los dispositivos físicos, que se utilizan para los respaldos?
8. ¿Qué procesos se siguen para la restauración de los respaldos?
9. ¿Qué tipo de control existe para los servicios e instalaciones realizadas por personal externo a la institución?

Anexo #5: Control de la composición de la red física administrativa

INVENTARIO - RETIRO DE HARDWARE

HARDWARE			
No. ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO
A123	MacBook Pro	Descripción artículo	MacBook Air

COMPRA			
FECHA DE COMPRA	PROVEEDOR	VALOR DE COMPRA POR ARTÍCULO	FECHA DE VENCIMIENTO DE GARANTÍA
20/5/2019	Cole	₡ 1 000 000.00	20/5/2022

INFORMACIÓN DE HARDWARE			
MODELO	No. SERIE	OBSERVACIONES	FECHA DE RETIRO DE EQUIPO
MacBook Air 3.0	VX123456	Observación	8/8/2020

INVENTARIO - HARDWARE

HARDWARE			
No. ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO
A123	MacBook Pro	Descripción artículo	MacBook Air

UBICACIÓN	
DEPARTAMENTO	LUGAR
Arte	Oficina 1

COMPRA			
FECHA DE COMPRA	PROVEEDOR	VALOR DE COMPRA POR ARTÍCULO	FECHA DE VENCIMIENTO DE GARANTÍA
20/5/2019	Cole	₡ 1 000 000.00	20/5/2022

CONDICIÓN / VALOR	
CONDICIÓN	VALOR ACTUAL DEL ACTIVO
Excelente	$1 000.00

INFORMACIÓN DE HARDWARE				
MODELO	No. SERIE	OBSERVACIONES	FECHA DE ULTIMA REVICIÓN	FOTO / ENLACE
MacBook Air 3.0	VX123456	Observación	8/8/2020	

Anexo #6: Carta de entrega de la propuesta

mep
Ministerio de Educación Pública

Benemérito Liceo José Martí

Circuito 05 – Código Presupuestario: 4116
Teléfonos: 21057071
liceo.josemarti@mep.go.cr

Puntarenas, lunes 02 de marzo del 2020

MSc. Antonieta González Esquivel
Directora de Carrera Ingeniería en Tecnologías de Información
Universidad Técnica Nacional
Sede del Pacífico

Estimada señora:

Sirva la presente para informarle que los estudiantes Isaac Alejandro Arguedas Leitón, Luis Gerardo Barquero Aguilar, Marcos Daniel Herrera Madrigal, se presentaron al Benemérito Liceo José Martí y realizaron el trabajo:

"Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República"

Los estudiantes el día de hoy hicieron entrega de la propuesta y los documentos del dicho trabajo.

Sin más por el momento se suscribe,

Atentamente,

Msc. Jonathan Vindas Benavides
Coordinador de Recursos Tecnológicos
Benemérito Liceo José Martí
Cc.Archivo
jv

"Educar para una nueva ciudadanía"

Anexo #7: Carta de autorización para uso y manejo de los Trabajos Finales de Graduación

CARTA DE AUTORIZACIÓN PARA USO Y MANEJO DE LOS TRABAJOS FINALES DE GRADUACIÓN
UNIVERSIDAD TÉCNICA NACIONAL

Ciudad y Fecha. Puntarenas, 26 de febrero del 2020

Señores
Vicerrectoría de Investigación Transferencia
Sistema Integrado de Bibliotecas y Recursos Digitales.

Nombre completo de sustentantes	Número de identificación
Isaac Alejandro Arguedas Leitón	604140826
Luis Gerardo Barquero Aguilar	604400973
Marcos Daniel Herrera Madrigal	604370102

Nosotros en calidad de autores del trabajo de graduación titulado:

Análisis de la gestión de la seguridad del hardware de la red administrativa en el Benemérito Liceo José Martí, en Puntarenas, para el tercer cuatrimestre del año 2019, de acuerdo con las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información de la Contraloría General de la República

El cual se presenta bajo la modalidad de:

____Seminario de Graduación

__X__Proyecto de Graduación

____Tesis de Graduación

Autorizamos a la Universidad Técnica Nacional para que nuestro trabajo sea manejado bajo los siguientes parámetros:

Ver CAPÍTULO V, DISPOSICIONES, FINALES. Artículo 4. RTFG.	
Conservación y diseminación en las bibliotecas de la Universidad	X
Almacenado en el Repositorio institucional.	X
Divulgado en el Repositorio institucional.	X
Resumen (Describe en forma breve el contenido del documento)	X
Consulta electrónica con texto protegido	X
Descarga electrónica del documento en texto completo protegido	X
Inclusión en bases de datos y sitios web que se encuentren en convenio con la Universidad Técnica Nacional contando con las mismas condiciones y limitaciones aquí establecidas.	X

Por otra parte, declaramos que el trabajo que aquí presentamos es de plena autoría, es un esfuerzo realizado de forma conjunta, académica e intelectual con plenos elementos de originalidad y creatividad. Garantizamos que no contiene citas, ni transcripciones de forma indebida que puedan devenir en plagio, pues se ha utilizado la normativa vigente de la American Psychological Asociation (APA). Las citas y transcripciones utilizadas se realizan en el marco de respeto a las obras de terceros. La responsabilidad directa en el diseño y presentación son de competencia exclusiva, por tanto, eximo de toda responsabilidad a la Universidad Técnica Nacional.

Conocedores de que las autorizaciones no reprimen mis derechos patrimoniales como autor del trabajo, insto a la Universidad Técnica Nacional a que respete y haga respetar mis derechos de propiedad intelectual.

Nombre completo del estudiante	**Número de identificación**	**Firma**
Isaac Alejandro Arguedas Leitón	6-0414-0826	
Luis Gerardo Barquero Aguilar	604400943	Luis Barquero Aguilar
Marcos Daniel Herrera Madrigal	6 0437 0102	

Fecha: 26 de febrero del 2020