Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

GUÍA DE ALTERNATIVAS PARA UN SISTEMA DE CONTROL Y SEGURIDAD EN USUARIOS APLICANDO INTERNET DE LAS COSAS (IOT)

Mauro Lenín Cán Chicol
Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, enero de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN

GUÍA DE ALTERNATIVAS PARA UN SISTEMA DE CONTROL Y SEGURIDAD EN USUARIOS APLICANDO INTERNET DE LAS COSAS (OIT)

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

MAURO LENÍN CÁN CHICOL
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, ENERO DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Francisco Javier González López
EXAMINADOR	Ing. Christian Antonio Orellana López
EXAMINADOR	Ing. Juan Carlos Córdoba Zeceña
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GUÍA DE ALTERNATIVAS PARA UN SISTEMA DE CONTROL Y SEGURIDAD EN USUARIOS APLICANDO INTERNET DE LAS COSAS (IOT)

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica con fecha 23 de septiembre de 2020.

Mauro Lenín Cán Chicol

Guatemala 15 de marzo 2021

Ingeniero
Julio César Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Apreciable Ingeniero Solares,

Me permito dar aprobación al trabajo de graduación titulado ¨**Guía de alternativas para un sistema de control y seguridad en usuarios aplicando Internet de las cosas (IOT)**¨, del señor **Mauro Lenín Cán Chicol**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones de este.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 19 de marzo de 2021

Señor Director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **GUÍA DE ALTERNATIVAS PARA UN SISTEMA DE CONTROL Y SEGURIDAD EN USUARIOS APLICANDO INTERNET DE LAS COSAS (IOT),** desarrollado por el estudiante **Mauro Lenín Cán Chicol**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF. EIME 154 2021.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; MAURO LENÍN CÁN CHICOL titulado: GUÍA DE ALTERNATIVAS PARA UN SISTEMA DE CONTROL Y SEGURIDAD EN USUARIOS APLIANDO INTERNET DE LAS COSAS (IOT), procede a la autorización del mismo.

Ing. Armando Alonso Rivera Carrillo

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA
RIA
MEC CTRICA
INGENIERIA

GUATEMALA, 25 DE OCTUBRE 2,021.

Facultad de Ingeniería

Decanato
24189101-
24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.034.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **GUÍA DE ALTERNATIVAS PARA UN SISTEMA DE CONTROL Y SEGURIDAD EN USUARIOS APLICANDO INTERNET DE LAS COSAS (IOT),** presentado por: **Mauro Lenín Cán Chicol,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, enero de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por darme la sabiduría necesaria, por iluminar siempre mi camino y destino para alcanzar este gran sueño.
Mi amada madre	María Delfina Chicol Ajsivinac, por darme la vida, amor, consejos y por ser mi mayor mentora y mi motivación en esta aventura que es la vida, muchas gracias.
Mi esposa	Lesly Boche, por tu amor, apoyo y consejos para lograr alcanzar mi gran sueño.
Mis hijos	Samantha, Othoniel, Fernanda y Maurito Can, que con esas sonrisas, energía y luz iluminan mi vida día con día.
Mis hermanos	Engel y David Can, por estar alentándonos con su alegría en los momentos que más lo necesitamos.
Mi señor padre	Mauro Can Ajquejay, por darme la vida, amor, consejos y por ser mi apoyo en los momentos difíciles.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	A mi *Alma mater,* la Universidad de San Carlos de Guatemala, por ser ente importante e influencia para mi carrera.
Facultad de Ingeniería	A mi segunda casa, mi querida y gloriosa Facultad de Ingeniería, gris y negro por excelencia, por permitirme estudiar una grandiosa carrera y hacer mi sueño realidad.
Mis amigos de la Facultad y Escuela	Por acompañarme en esta aventura que fue nuestra carrera y por compartir muchas experiencias a lo largo de estos años.
Los ingenieros	Muchas gracias por compartir sus conocimientos y consejos para mi carrera.
Al glorioso Comité de Huelga de la Facultad de Ingeniería.	Por darme amigos y enseñanzas que perdurarán toda la vida.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
A	Amperios
bps	Bits por segundo
4G	Cuarta generación de telefonía móvil
dBi	Decibelio de ganancia isotrópica
dBm	Decibelio-milivatio
fps	Fotogramas por segundo
GHz	Gigahercio
°C	Grados centígrados
kB	Kilobytes
kV	Kilovatio
Mbps	Megabits por segundo
φ	Phi minúscula

GLOSARIO

Aseguramiento de calidad	Vigilancia continua destinada a garantizar en todo momento que los protocolos de seguridad sean eficientes y efectivos.
Arduino	Placa robusta de microcontrolador con código abierto basado en emplear un microchip ATmega328P.
Auto inspección	Inspección efectuada por personal técnico calificado propio de la empresa que evalúa periódicamente la aplicabilidad y efectividad de los protocolos implementados.
Autoridad competente	Es la autoridad asignada con mayor nivel jerárquico dentro de la empresa.
Baud_rate	Unidad de medida que puede representar el número de símbolos por segundo empleado en un medio de transmisión digital.
Callback	Se nombra así a una función de tipo A que se emplea como un argumento de otra función de tipo B. Entonces la ocurrencia de llamar a B hace que ejecute automáticamente A.

GPRS	Servicio General de Paquetes de Radio. Estándar de comunicación para teléfonos móviles que transmite la información por grupos significativos o paquetes. Puede transmitir a una velocidad de 114 kbps y permite la conexión a internet. Es una tecnología de transición entre los sistemas GSM y UMTS.
GSM	Sistema global para las comunicaciones móviles.
Full-duplex	Se define así al sistema que es capaz de mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea.
Half-duplex	Una conexión semidúplex (a veces denominada una conexión alternada) es una conexión en la que los datos fluyen en una u otra dirección, pero no las dos al mismo tiempo. Con este tipo de conexión, cada extremo transmite uno después del otro.
IOT	Internet de las cosas (*Internet of things*).
Módem	Dispositivo que convierte señales digitales en analógicas, o viceversa, para ser transmitidas a través de líneas de teléfono, cables coaxiales, fibras ópticas y microondas; conectado a una computadora, permite la comunicación con otra computadora por vía telefónica.

RESUMEN

El incremento de la demanda de protocolos y sistemas de seguridad digital residencial o ejecutiva, hace que se plantee una respuesta eficiente, por medio del presente trabajo de investigación y desarrollo se pretende crear la guía de alternativas que permitan implementar sistema de control y seguridad en los usuarios vulnerables, con un conjunto de procesos y procedimientos que otorguen el panorama ideal, donde no se expongan los datos sensibles de estos usuarios.

Además, los altos índices de estafas y pesca (*phishing*) por obtener datos sensibles de los consumidores que se conectan a diario a la extensa web, otorgan diferentes canales para lograr estos malos beneficios, la infraestructura no es precisamente violentada por el intercambio de datos digitales, se han presentado vulnerabilidades desde sitos remotos, donde los usuarios han presentado quejas por ciberataques, sin la mínima capacidad de percibir estos acosos constantes y vulnerabilidades nace la inquietud de proponer soluciones efectivas y eficientes.

Las alternativas que se presentan en el entorno guatemalteco dependerán del acceso a la información del usuario, de lo contrario siempre podrán estar expuestos a cualquier situación nociva a su pensamiento crítico de emplear tecnologías y herramientas vanguardistas, la estimulación temprana que pueda promover un beneficio social y común propicia cambios a infraestructura en las redes existentes y en los modelos que se conocen, de cómo se pueden recrear e instalar estos dispositivos.

Los flujos de corrientes que alimentan los dispositivos de seguridad juegan un rol importante, cuando una corriente no es estable o presenta picos, los equipos de seguridad probablemente se presentan expuestos a los ciberataques, así nace el complemento de la guía de alternativas, involucrando el internet de las cosas, junto con infraestructura necesaria para sus respaldos.

OBJETIVOS

General

Realizar una guía de alternativas para un sistema de control y seguridad en usuarios aplicando internet de las cosas.

Específicos

1. Promover el modelo eficiente para el control de los dispositivos de internet de las cosas mediante una interfaz que muestre la información que permita identificar las acciones.

2. Delinear una red de internet de las cosas con dispositivos accesibles en costos, que permitan promocionar datos al usuario y le permita implementar ahorros de energía en la infraestructura presente.

3. Establecer aspectos importantes durante la implementación de un sistema de gestión de la seguridad informática (SGSI) en cualquier entidad con relación a los bienes informáticos que se utilizan y que logre garantizar el intercambio de datos digitales, preservando la identidad del usuario.

4. Proponer el modelo de gestión eficiente a cargo de la seguridad informática, que garantice la reserva de los datos sensibles del usuario.

5. Organizar y desarrollar la información complementaria y relacionada con internet de las cosas.

INTRODUCCIÓN

El desarrollo de la investigación tendrá la importancia de ser una guía práctica para el diseño completo de un sistema de control y seguridad en usuarios que emplean Internet de las cosas (IOT), ya sea para uso industrial, infraestructuras robustas como edificios, centros comerciales o proyectos habitacionales.

El aumento en el uso del internet y la modernización han permitido el avance y diseño de dispositivos comunes que ahora pueden comunicarse con la red. La implementación de estos sistemas permite controlar, analizar y estudiar los ambientes comunes; son accesibles para implementarse en los hogares, hoteles, restaurantes, entre otros.

Un sistema de internet de las cosas permite tener un control sobre los ambientes para la obtención de la información; esta información crea estadísticas y predicciones, por lo que es necesario tener transductores que obtengan los datos del medio para transformarlos en datos digitales. Este diseño muestra dos tipos de casos en los cuales se puede acceder al control de los ambientes y mantener siempre una conexión y actualización del estado. Se muestra cuáles son los problemas que se generan cuando se conecta varios dispositivos en una red de IoT. Se da a conocer la programación básica de los dispositivos utilizados.

1. CIRCUITOS QUE ALIMENTAN UNA RED DE DISTRIBUCIÓN

1.1. Definición de alimentador

"Todos los conductores de un circuito formado entre el equipo de acometida o la fuente de un sistema derivado separado y el dispositivo final de protección contra sobrecorriente del circuito derivado".[1]

1.2. Definición y conceptos de carga

"De acuerdo con lo que dispone el Sistema Internacional de Unidades la carga eléctrica se denomina culombio (c) y lo define como aquella cantidad de carga que pasa por la sección transversal de un determinado conductor eléctrico durante el lapso de un segundo y cuando la corriente eléctrica es de un amperio".[2]

Se reconoce la carga como una propiedad intrínseca que presentan algunas partículas subatómicas la cual se manifestará a través de atracciones y repulsiones que determinarán las interacciones electromagnéticas entre ellas, siendo las mismas cargas positivas y cargas negativas.

La materia cargada de manera eléctrica será influida por los campos electromagnéticos a la vez que los genera. La interacción entre carga y campo

[1] CONDUMEX. *Manual técnico de instalaciones en baja tensión*. p. 58.
[2] UCHA, Florencia. *Definiciones*. https://www.definicionabc.com/tecnologia/carga-electrica.php. Consulta: junio de 2020.

eléctrico dará origen a una de las cuatro interacciones fundamentales que es la interacción electromagnética.

Históricamente, a los electrones, cuarks y protones se les asignó diferentes cargas, por ejemplo, los electrones presentan carga negativa -1, también conocida como –e; por su lado, los protones presentan carga positiva +1 o también +e, en tanto, a los cuarks se les asignó una carga de tipo fraccionaria.

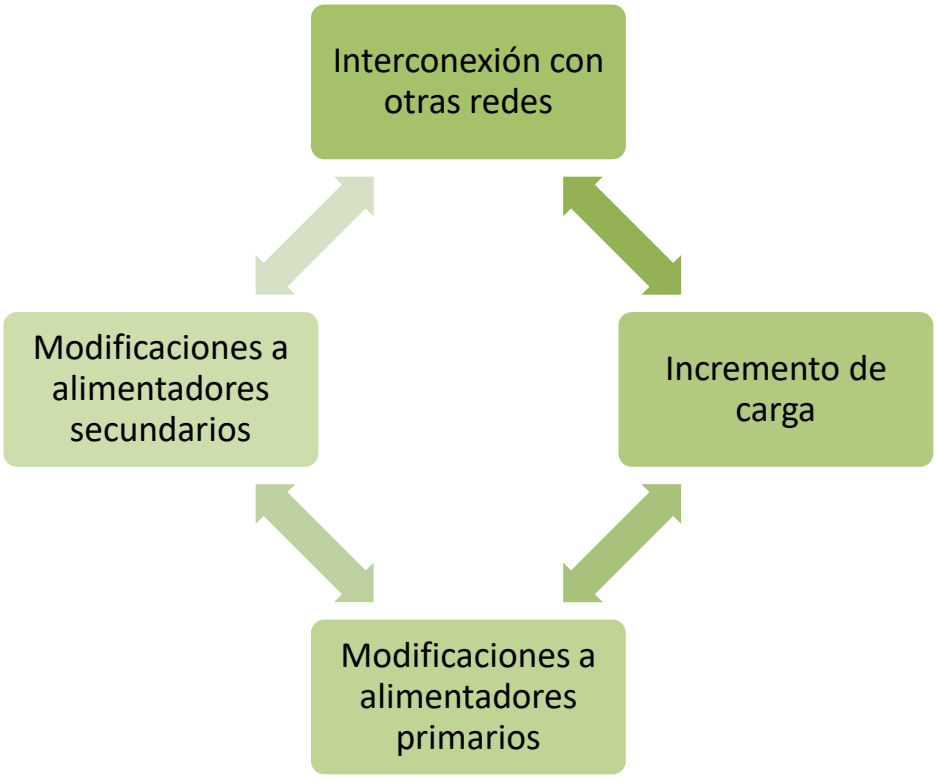
Figura 1. **Consideraciones básicas que deberán formar parte de un alimentador para la transferencia de carga**

Fuente: elaboración propia.

- Estudio de cargas

Se deberá comprobar el factor voltaje, el índice de corriente, potencia activa y reactiva, factor de potencia y un conjunto de parámetros adicionales que son propios del sistema, según sus condiciones operacionales presentes. Este conjunto de datos permitirá realizar el análisis de las condiciones y proyecciones de la red, además será importante y con alto nivel de criticidad realizar el estudio adecuado, ya que de estos estos resultados dependerán las diferentes maniobras que se puedan realizar en el circuito.

Figura 2. **Maniobras comúnmente realizadas dentro de un circuito**

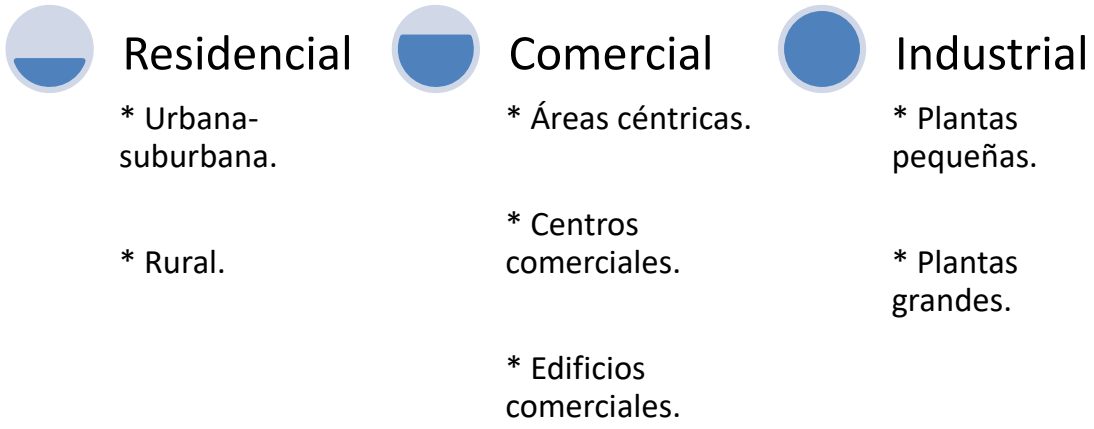


Fuente: elaboración propia.

- Tipos de carga

Se basará en los diferentes tipos de servicios donde es empleada o utilizada la energía eléctrica, ya que estos dependen directamente del tipo de consumidor y sus necesidades básicas. Además, se deberán considerar otros tipos de factores importantes, los cuales pueden modificar el sistema, no se pueden dejar por un lado la densidad de carga y la diversidad de los distintos consumidores por unidad de área.

Figura 3. **Clasificación de los tipos de carga**



Fuente: elaboración propia.

Se deberá considerar, que existen zonas activas donde puede detectar y encontrar todo tipo de cargas, debido a esto, la propuesta no puede ser diseñada puntualmente o con una carga específica, por lo que deberán adoptar otros tipos de criterios para la planeación estratégica.

Tabla I. **Clasificación y división de las cargas por su confiabilidad**

Tipo de carga	Descripción
De primera categoría	No podrán sufrir ningún desabastecimiento de energía, la mínima interrupción puede causar graves daños al usuario final, debido a la sensibilidad de sus equipos electrónicos o el nivel de criticidad de las actividades que se están desarrollando. Además, se considera que estas cargas deberán conformar grupos electrógenos de respaldo.
De segunda categoría	Acá se conforma un grupo de cargas, donde se pueden soportar interrupciones no mayores a cinco minutos. Se incluyen dentro de su segmento o grupo focal las plantas de producción con equipos mecánicos robustos, y empresas que emplean energía de forma intermitente.
De tercera categoría	La muestra abarca un conjunto de usuarios que puedan soportar la interrupción prolongada sin que sufran pérdidas considerables. Dentro de este grupo focal se incluyen los residenciales, poblaciones rurales, industrias fabriles pequeñas, y otros.

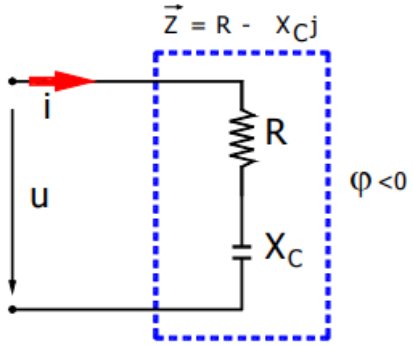
Fuente: elaboración propia.

Además, de considerar los aspectos relevantes y los factores que comprometen la carga, se deberán considerar los errores humanos y factores naturales poco predecibles, se obtiene la participación en acontecimientos inesperados del 1 % sobre factores naturales poco predecibles. Este factor de riesgo, por muy pequeño, nunca deberá ser pasado por alto, los diseños eficientes relacionados con las distribuciones de cargas afrontarán nuevos retos, desde el cambio climático hasta los problemas geográficos.

1.3. Potencia activa, potencia reactiva y potencia aparente

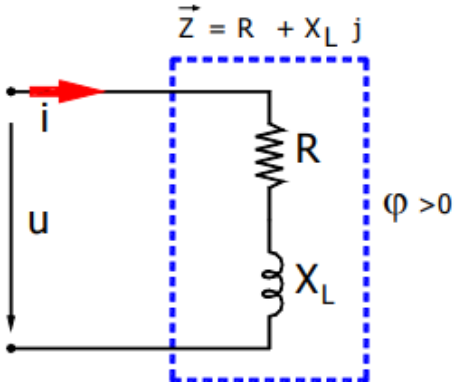
Los dipolos pasivos excitados que presentan una tensión alterna senoidal pueden ser reducidos a una resistencia en serie empleando un condensador (circuito capacitivo), o también puede ser empleada la resistencia en serie con una bobina (circuito inductivo).

Figura 4. **Circuito capacitivo**



Fuente: elaboración propia.

Figura 5. **Circuito inductivo**



Fuente: elaboración propia.

La potencia instantánea que es consumida por el dipolo pasivo será, calculada por la siguiente fórmula:

Fórmula 1

$$p(t) = P(1 - \cos(2\omega t)) - UI\ sen\ \varphi\ sen\ (2\omega t)$$

Donde el primer término es conocido como la potencia consumida por la resistencia R, de la impedancia y el segundo término establecido es la potencia requerida por la reactancia X, de la impedancia.

Además, la energía eléctrica se reconoce como la rapidez o velocidad con que la energía eléctrica que puede asumir otra forma. En un sistema de tipo mecánico, se conoce la potencia como la rapidez con la que se puede realizar un trabajo, donde la cantidad de trabajo puede realizar sobre una cantidad específica de tiempo.

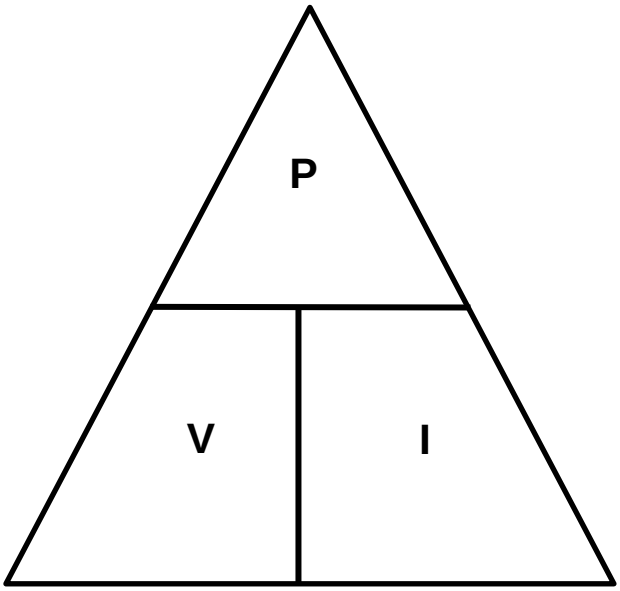
La potencia eléctrica, o mejor conocido como el porcentaje del cual la energía eléctrica puede ser convertida en otra forma de energía, es nada más que la corriente multiplicada por el voltaje. Donde la unidad de medida de la potencia eléctrica es el vatio (W), de esto parte el principio didáctico que propone que un voltaje de 1 volt, al empujar una corriente de 1 amperio, logra producir 1 vatio de potencia.

Fórmula 2

$$P = I\ x\ V$$

De esta fórmula principal derivan dos más, las cuales relacionan la corriente y el voltaje expresado en términos de otras variables conmutables.

Figura 6. **Triángulo de memoria**



Fuente: CONDUMEX. *Manual técnico de instalaciones eléctricas en baja tensión*. p. 33.

Donde se derivan las siguientes fórmulas:

Fórmula 3

$$I = \frac{P}{V}$$

Fórmula 4

$$V = \frac{P}{I}$$

1.3.1. Potencia activa

Es la potencia que representa la capacidad de un circuito para realizar un proceso de transformación de la energía eléctrica en trabajo. Los diferentes dispositivos eléctricos existentes convierten la energía eléctrica en otras formas de energía tales como: mecánica, lumínica, térmica, química, y otras.

Esta potencia es, por lo tanto, la realmente consumida por los circuitos. Cuando se habla de demanda eléctrica, es esta potencia la que se utiliza para determinarla:

Fórmula 5

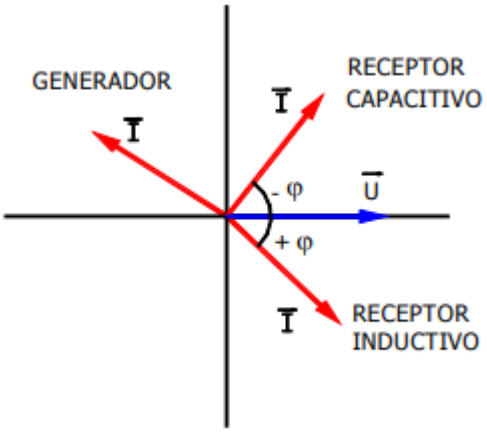
$$P = U \text{ x } I \cos\varphi = R\, I^2$$

Donde; la potencia activa dependerá directamente del desfase que se presenta en u e i, por lo cual a cos φ se le llama factor de potencia.

Además, esto implica que, en un dipolo pasivo P ≥ 0 pues en el no hay fuentes de energía, por consiguiente, el factor de potencia ha de ser: cos φ ≥ 0. Si cos φ < 0, el dipolo está suministrando energía y, por tanto, ha de contener fuentes energéticas lo que quiere decir que no puede ser pasivo.

Se puede realizar una representación gráfica, tomando como origen la tensión aplicada al dipolo y logrando representar i e u, donde la intensidad estará dentro del primer cuarto y cuadrante siempre que el receptor sea pasivo (P > 0 > cos φ > 0), si es que se ocupa el segundo y tercer cuadrante el circuito actúa como generador, suministrando energía.

Figura 7. **Diagrama del factor de potencia activa**



Fuente: GARCÍA, Néstor. *Potencia en circuitos monofásicos*. https://es.slideshare.net/NUVILDE/potencia-elctrica-monofsica. Consulta: junio de 2020.

1.3.2. Potencia reactiva

Su carácter real no es de ser consumida, solamente se presenta cuando existan bobinas o condensadores en los circuitos. Esta potencia reactiva se presenta con un valor medio nulo, por lo que, no produce trabajo necesario. Para ello, es necesario una potencia desvatada (sin producir vatios), se debe medir en volt amperios reactivos (VAR) y se deberá designar con la letra Q.

También puede ser denominada potencia reactiva al valor máximo obtenido de la potencia fluctuante positiva y negativa de valor medio nulo. Ahora bien, si la potencia fluctuante (+) (-) puede valer –UI sen φ sen 2φt el valor máximo sería:

Fórmula 6

$$Q = U \text{ x } I \operatorname{sen} \varphi \;\; Potencia\ Reactiva$$

Fórmula 7

$$\mathrm{Q}\ (+)\ \text{para}\ \varphi\ (+) \qquad Carga\ inductiva$$

Fórmula 8

$$\mathrm{Q}\ (-)\ \text{para}\ \varphi\ (-) \qquad Carga\ capacitiva$$

Para esta potencia, su unidad es el voltamperio reactivo (VAr)

La potencia reactiva se representa por el bombeo de energía necesaria para el funcionamiento del receptor, pero, el inconveniente es que no presenta energía útil.

En algunas bibliografías se le conoce como potencia magnetizante, por ser la consumida en los circuitos magnéticos de las máquinas para crear el flujo, aunque esta no sea consumida (solamente sus pérdidas), esta logra ser almacenada en el campo magnético para ser devuelta más tarde en la desconexión.

1.3.3. Potencia aparente

Se le denomina así al resultado del producto de la tensión eficaz por intensidad eficaz.

Fórmula 9

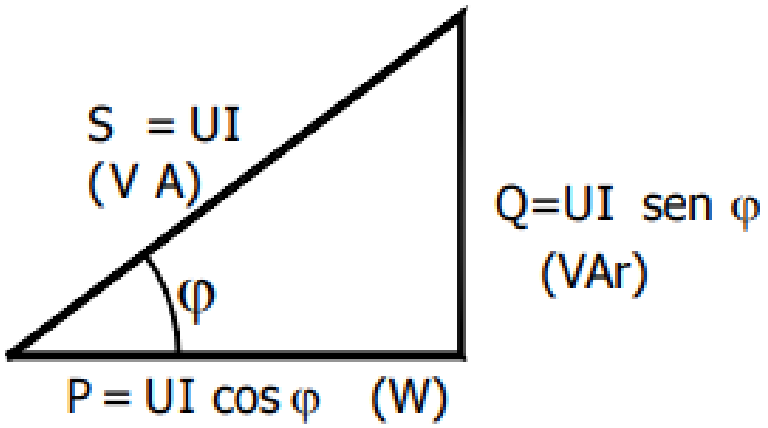
$$S = UxI$$

Su factor de unidad es el voltamperio (VA).

En corriente continua la potencia transferida es el producto UxI. En corriente alterna la potencia aparente S coincide con la potencia activa P, cuando la impedancia se compone solo de resistencia.

Este conjunto de conceptos, propician la base para recrear el triángulo de potencias, en este triángulo se hace la representación sobre la potencia activa, reactiva y aparente.

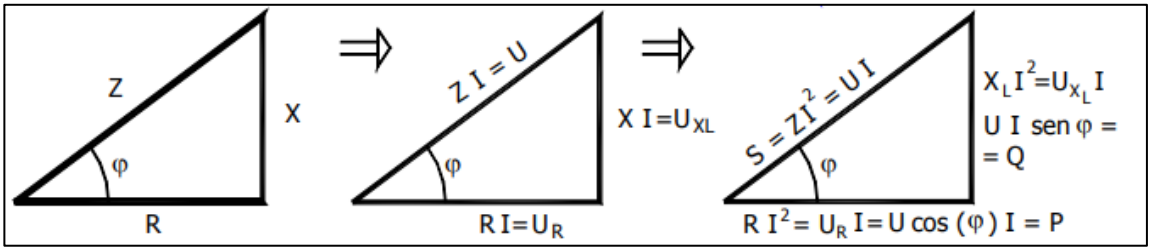
Figura 8. **Triángulo de potencias**



Fuente: GARCÍA, Néstor. *Potencia en circuitos monofásicos*. https://es.slideshare.net/NUVILDE/potencia-elctrica-monofsica. Consulta: junio de 2020.

El triángulo de potencias se obtiene a partir del triángulo de impedancias, empleando, además, una impedancia inductiva genérica y otra capacitiva.

Figura 9. **Triángulo de impedancia**



Fuente: GARCÍA, Néstor. *Potencia en circuitos monofásicos*. https://es.slideshare.net/NUVILDE/potencia-elctrica-monofsica. Consulta: junio de 2020.

Dada una impedancia inductiva, el triángulo de impedancias será un triángulo rectángulo cuyos catetos son la resistencia y la reactancia, y la hipotenusa es el módulo de la impedancia Z. Luego de multiplicar cada lado del triángulo de impedancias por el valor eficaz de la intensidad I, se logra obtener un nuevo triángulo cuya hipotenusa representa la caída de tensión en la impedancia en valor eficaz U, y cuyos catetos representan, respectivamente las caídas de tensión en la resistencia y en la reactancia de la carga, también con valor eficaz.

A ese nuevo triángulo se le denomina triángulo de tensiones, donde:

Tabla II. **Conceptos sobre la caída de tensión**

Lugar	Fórmula de representación
En la resistencia	U_R = I.R (representado por el cateto horizontal)
En la reactancia	U_X = I.X (representado por el cateto vertical)
En la impedancia	U = U_Z = I.Z (representado por la hipotenusa del triángulo)

Fuente: GARCÍA, Néstor. *Potencia en circuitos monofásicos*. https://es.slideshare.net/NUVILDE/potencia-elctrica-monofsica. Consulta: junio de 2020.

Acá se logra mantener la semejanza entre los dos triángulos, implica que el ángulo comprendido entre la hipotenusa y el cateto horizontal es el mismo en los dos triángulos, o sea, el desfase entre la tensión y la intensidad, dicho de otro modo, el argumento de la impedancia compleja.

Si después de ese procedimiento, se multiplica de nuevo, cada uno de los lados del triángulo de tensiones por el valor eficaz de la intensidad I, se obtiene un nuevo triángulo, a este se le denominará triángulo de potencias, cuya hipotenusa representa a la potencia aparente, el cateto horizontal representa la potencia activa y el cateto vertical representa a la potencia reactiva.

Al multiplicar cada lado del triángulo de tensiones por I, tal como sucedía anteriormente, se mantiene la semejanza con el triángulo de tensiones, con lo que el ángulo comprendido entre la hipotenusa y el cateto horizontal sigue siendo φ.

La longitud de la hipotenusa del nuevo triángulo será: UI, es decir la potencia aparente, S = UI.

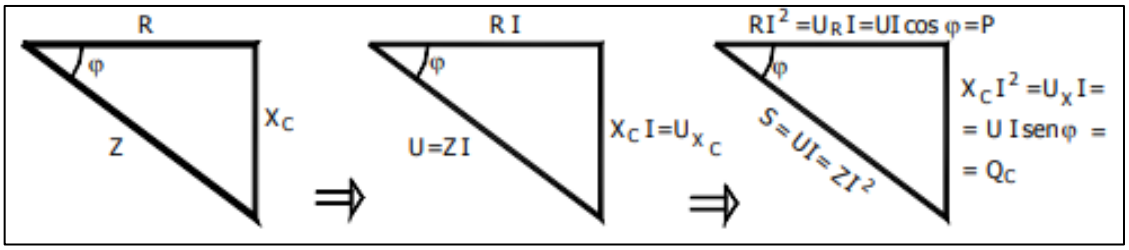
La longitud del cateto horizontal será: U_R I = RI^2, ahora bien, esta longitud también es igual a U.I cos φ= P, la potencia activa de la impedancia, por lo que se puede concluir que la potencia activa de un receptor que posea una resistencia equivalente R es igual al producto de la resistencia por el cuadrado de la intensidad que circula por ella, es decir RI^2.

Por otra parte, la longitud del cateto vertical del nuevo triángulo será: U_X I = XI^2, ahora bien, esta longitud también es igual a U.I sen φ= Q, la potencia reactiva de la impedancia, por lo que se podría concluir que la potencia reactiva

de un receptor que posea una reactancia equivalente X es igual al producto de la reactancia por el cuadrado de la intensidad que circula por ella, es decir XI^2.

Con esto, queda visto, que el triángulo de potencias se puede obtener a partir del triángulo de impedancias para una impedancia inductiva genérica.

Figura 10. **Triángulo de potencias**



Fuente: GARCÍA, Néstor. *Potencia en circuitos monofásicos*. https://es.slideshare.net/NUVILDE/potencia-elctrica-monofsica. Consulta: junio de 2020.

1.3.4. Factor de potencia

Se podrá definir a la relación geométrica existente y proporcional representada entre la potencia activa y la potencia aparente.

Fórmula 10

$$fdp = \frac{P}{S} = Cos\ \phi$$

Donde ϕ = ϕv – ϕi; este factor de potencia presenta la cantidad inmediata de potencia activa o la cantidad que se está consumiendo por la carga resistiva. También se entiende, que mientras más cerca de la unidad se encuentre, la carga

podrá ser mayormente resistiva y si fdp= 1, entonces la carga es puramente resistiva y la potencia aparente será igual a la activa (se reconoce como adimensional el factor de potencia) y si fdp = 0, la carga será exclusivamente reactiva => 0 ≤ fdp ≤ 1.

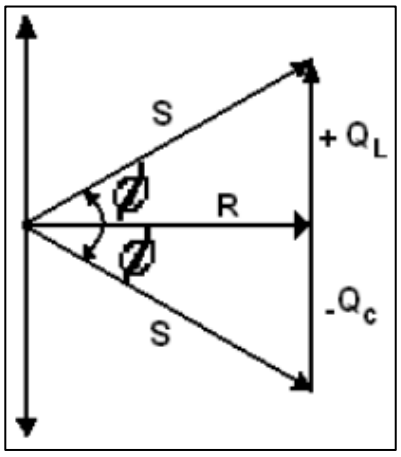
Además, en un circuito si la corriente pasa o adelante a la tensión, representará que la carga tiene reactancia capacitiva y si la corriente se atrasa respecto de la tensión, la carga será conocida como reactancia inductiva, donde se tomará de referencia a la corriente para definir el factor de potencia, dicho de en notación matemática:

Fórmula 11

$$FdP\ (\downarrow)\ en\ atraso\ (-)\ carga\ inductiva$$

$$FdP\ (\uparrow)\ en\ atraso\ (+)\ carga\ capacitiva$$

Figura 11. **Triángulo de potencias resultante**



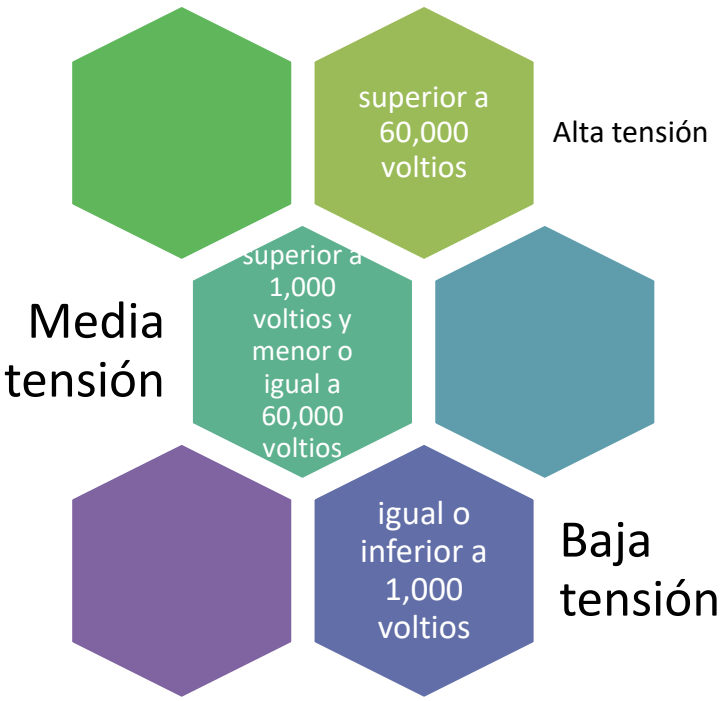
Fuente: DORF, Richard. *Circuitos eléctricos*. p. 175.

Así es como se lograría definir a la potencia aparente con el producto del voltaje por la corriente, en general la mayoría de los equipos que emplean o trabajan con CA, deberán especificar su potencia en VA o KVA (kilovolt-amperios) y su respectivo voltaje, ya que con estos valores se podrá calcular de forma inmediata la corriente necesaria para realzar el trabajo requerido.

1.4. Aplicación de los niveles óptimos de voltaje de distribución

Según el reglamento de la Ley General de Electricidad en Guatemala, se establecen los siguientes criterios para clasificar y dividir la tensión.

Figura 12. **Niveles de tensión en Guatemala**



Fuente: Reglamento de la Ley General de Electricidad. *Acuerdo Gubernativo Número 256-97*. p. 21-23.

Los niveles óptimos para el enfoque académico son lograr establecer y permitir la continuidad del flujo de suministro de potencia, sin interrupciones, además disminuir valles en la continuidad del traslado de propio suministro para conseguir este nivel de eficiencia y aceptación, se deberán satisfacer un conjunto de acciones y eventos que estarán a cargo del responsable de las líneas de trasmisión.

Tabla III. **Distancia de seguridad verticales de conductores sobre el nivel del suelo, carreteras, vías férreas y superficies con agua (todas las tensiones son dadas de fase a tierra)**

Naturaleza de la superficie bajo los conductores.	Conductores de comunicación aislados, retenidas aterrizadas, conductores neutros y cables eléctricos aislados (m)	Conductores suministradores aislados de más de 750 V y conductores suministradores en línea abierta de 0 – 750 V (m)	Conductores suministradores en línea abierta arriba de 750 V a 22 kV. (m)	Conductores suministradores en línea abierta arriba de 22 a 470 kV. (m)
Vías férreas	7,2	7,5	8,1	8,1 + 0.01 m por cada kV arriba de 22 kV.
Carreteras, calles, caminos y otras áreas usadas para tránsito.	4,7	5,0	5,6	5,6 m +0.01 m por cada kV arriba de 22 kV.
Aceras o caminos accesibles sólo a peatones.	2,9	3,8	4,4	4,4 m + 0.01 m por cada kV arriba de 22 kV.
Agua donde está permitida la navegación.	4,0	4,6	5,2	5,2 m + 0.01 m por cada kV arriba de 22 kV.
Aguas navegables incluyendo lagos, ríos, estanques, arroyos y canales con un área de superficie sin obstrucción de: • Hasta 8 ha. • Mayor a 8 hasta 80 ha. • Mayor de 80 hasta 800 ha. • Arriba de 800 ha.	5,3 7,8 9,6 11,4	5,6 8,1 9,9 11,7	6,2 8,7 10,5 12,3	6,2/8,7/10,5 ó 12,3 m +0.01 m por cada kV arriba de 22 kV.

Fuente: CNEE. *Normas técnicas de diseño y operación de las instalaciones de distribución*. p. 9.

Se podrá relativizar los niveles óptimos de transmisión preservando las medidas técnicas y medidas establecidas en la norma técnica, así sea un diseño estructural moderno o arquitectónico, no se permitirá irrumpir las medidas establecidas.

Estas normas se diseñan por hacer eficiente el traslado de potencia, considerando las pérdidas permisibles, al actuar de manera ordenada, los accidentes estructurales podrán ser mitigados desde su diseño, así se mejorará las actividades que permitirán hacer eficiente el recurso del voltaje en su distribución.

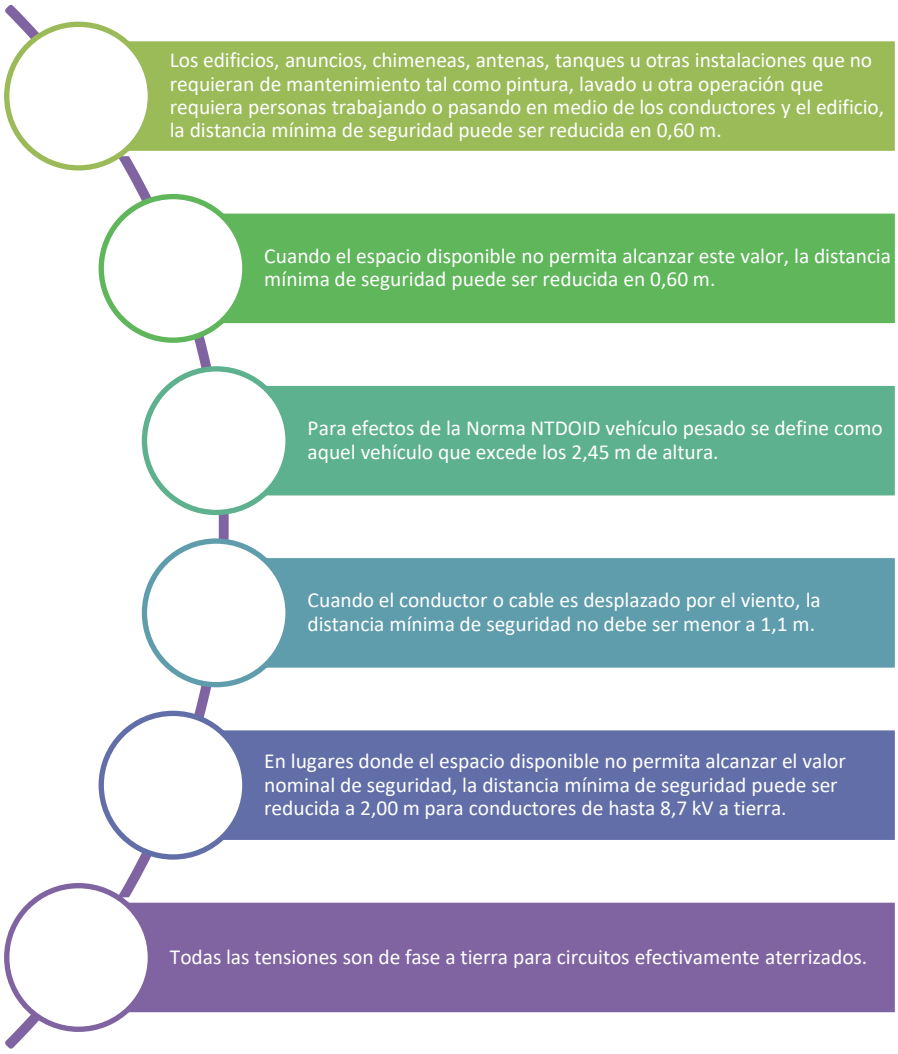
Tabla IV. **Distancias mínimas de seguridad verticales de conductores sobre vías férreas, el suelo o agua**

Nivel inferior	Nivel Superior			
	Conductores neutrales que cumplen con 18,1E1, retenidas aéreas (m).	Cables y conductores, mensajeros, retenidas de comunicación (m).	Conductores suministradores de línea abierta de 0 a 750 V (m).	Conductores suministradores de línea abierta de 750 v – 22 kV (m).
Conductores neutrales que cumplen con 18.1E1, retenidas aéreas.	0,60 (1)	0,60 (1)	0,60	0,60
Cables y conductores, mensajeros, retenidas de comunicación.	-	0,60 (1)	1,20	1,50
Conductores suministradores de línea abierta de 0 a 750 V.	-	-	0,60	0,60
Conductores suministradores de línea abierta de 750 V – 22 kV.	-	-	-	0,60

Fuente: CNEE. *Normas técnicas de diseño y operación de las instalaciones de distribución*. p. 10.

Las distancias mínimas de seguridad verticales entre los conductores y los cables estarán sujetos a las medidas establecidas en la Norma, así mismo, los diseños estructurales estarán sometidos al patrón establecido en la Norma.

Figura 13. **Distancias mínimas de seguridad de conductores a edificios y otras instalaciones**



Fuente: CNEE. *Normas técnicas de diseño y operación de las instalaciones de distribución*. p. 14.

Tabla V. **Distancia horizontal entre conductores soportados por la misma estructura**

Clase de circuito	Distancia mínima de seguridad (cm)
De 0 a 8,7 kV	30
De 8,7 a 50 kV	30 más 1,0 cm por cada kV en exceso de 8,7 kV
Mayor de 50 kV	No hay valor especificado
De 0 a 8,7 kV	30
De 8,7 a 50 kV	30 más 1,0 cm por cada kV en exceso de 8,7 kV
De 50 a 814 kV	72,5 más 1,0 cm, por cada kV de exceso de 50 kV

Fuente: CNEE. *Normas técnicas de diseño y operación de las instalaciones de distribución*. p. 23.

Tabla VI. **Factores de resistencia para, estructuras, cruceros, retenidas, cimientos y anclas, para ser utilizados con los factores de sobrecarga**

Factores de resistencia	Clase B	Clase C
Estructuras de metal y concreto pretensado	1,0	1,0
Estructuras de madera y concreto reforzado	0,65	0,85
Cable de retenida	0,9	0,9
Ancla de retenida y cimientos	1,0	1,0
Factores de resistencia para estructuras cuyos elementos estén instalados a 18,0 m o más sobre el nivel del suelo		
Estructuras de metal y concreto pretensado	1,0	1,0
Estructuras de madera y concreto reforzado	0,75	0,75
Cable de retenida	0,9	0,9
Ancla de retenida y cimientos	1,0	1,0

Fuente: CNEE. *Normas técnicas de diseño y operación de las instalaciones de distribución*. p. 33.

Se plantean las tablas anteriores, con la intencionalidad de recrear un modelo eficiente operativo, esto permitirá satisfacer el sostenimiento de los niveles óptimos de voltaje de distribución. Se sabe que existen pérdidas físicas, naturales y accidentales, ejecutando el conjunto de patrones analizados en la Norma NTDOID que regula las buenas acciones en Guatemala, permitirá hacer un trabajo eficiente para la empresa de transmisión.

No obstante, este es un conjunto de pequeños factores que permitirán hacer efectivo el alcance de producción y satisfacción de la demanda, para competir entre un mercado exigente donde la demanda principal sobre la permanencia del servicio es el nivel continuo y sostenido del voltaje, esperando que no presenten valle, picos o ritmos armónicos.

1.5. Circuitos alimentadores de iluminación y potencia

Los sistemas eléctricos están constituidos directamente sobre su sistema de distribución, el cual estará conformado por el conjunto de equipos y los diferentes métodos empleados para trasladar la potencia del equipo de acometida hacia los diferentes dispositivos de sobrecorriente que sirven para proteger los circuitos ramales.

Los destacados dispositivos de sobrecorriente se posicionan en el centro de la carga principal la cual es perteneciente a la acometida. Según la NFPA 70 (código NEC), todo o cualquiera que sea el centro de carga principal de una acometida, así como sus dispositivos que sirven de protección serán participes o pertenecientes al sistema de distribución principal de la acometida.

Entonces, los circuitos alimentadores serán comprendidos con los conductores que preceden de los dispositivos principales de protección de

sobrecorriente del equipo de la acometida hacia los tableros subalimentadores o también los que se encuentran directamente hacia los tableros de circuitos ramales finales, hasta el tablero de distribución y su respectiva protección.

Además, existe un sinfín de variables o factores que influirán para diseñar el eficiente sistema de distribución, algunas variables que se pueden parametrizar y cuantificar previamente al diseño son el tipo de edificación, naturaleza y tamaño de la carga eléctrica, limitante económica, las condiciones circundantes del proyecto y las condiciones propias de la región donde se ejecutará. Asimismo, un sistema de distribución no estará limitado para operar en condiciones de simples voltajes, por lo cual se podrán necesitar de uno o varios transformadores eléctricos para diferentes o distintos voltajes.

Tabla VII. **Elementos complementarios de un circuito alimentador**

Elemento	**Descripción**
Alimentador de iluminación	Son mejor conocidos como tomacorrientes, donde se puede obtener una fuente de carga.
Alimentador de potencia	Es una carga de circuitos ramales, diseñado para motores, acceso a la calefacción u otro tipo de cargas de potencia.
Subalimentador	Conductor que representa un circuito que alimenta uno o varios tableros de distribución de circuitos ramales, que se origina en un centro de carga (no en el principal) soportado por un alimentador.
Tablero de piso (*Switchboards*)	Tablero o panel grande, colocado en piso enmarcado o ensamblado por paneles con *switches*, dispositivos de protección variados, y usualmente con instrumentos de medición y control en el frente. Estos son accesibles por delante y por atrás.
Tablero o panel (*panelboards*)	Contiene barras aprovechadas por portafusiles, con o sin *switches*, o por *circuit breakers*, proveyendo protección y control para circuitos de iluminación, otros y de potencia. Estos circuitos pueden ser ramales o subalimentadores. Un tablero o panel esta designado para ser colocado en un gabinete o caja de corte colocado generalmente en paredes y particiones accesibles solo por el frente.

Fuente: elaboración propia.

Por esto, se contempla que un sistema de distribución a través de los alimentadores y subalimentadores llevará la energía distribuida hacia los tableros de iluminación y a los tableros de potencia que pueden comprender los centros de control, donde se concentraran las cargas para los equipos y dispositivos varios de proyección de circuitos ramales de cargas individuales. Además, se contemplan cargas de equipos de alto consumo de potencia.

1.6. Medios y métodos de distribución eléctrica

Para un trabajo eficiente y diseño efectivo en la distribución de eléctrica se podrán tomar en consideración diferentes variables, pero no obstante la simpleza en una ecuación compleja se verá optimizada por el mínimo de esfuerzo requerido. Así es como se necesitará de ejecutar técnicas y medios comunes para el ordenamiento en su infraestructura.

Las tuberías metálicas son reconocidas como uno de los medios efectivos, eficientes y rentable, por durabilidad, maleabilidad y practicidad de colocación en las obras grises, estas tuberías galvanizadas poseen la facultad de ponerlas a tierra, dentro de ellas se pueden colocar o dirigir diferentes conductores eléctricos de diferentes calibres.

Además, se pueden emplear conductores con propiedades físicas y químicas de aislamiento con diferentes rangos permisibles de temperatura, ya que en estos se pueden presentar temperaturas arriba de los 90 ^{o}C.

Los distintos tipos de conductores que se encuentran en el marcado eléctrico se incorporan dentro de las diferentes tuberías que son trasladadas o recorridas por la extensión necesaria en la instalación de influencia, están

conectan los tableros de distribución y los tableros ramales que, a su vez, alimentan las cargas demandadas.

Otra opción o medio viable es emplear el electroducto, también se le conoce como ducto barra, esencialmente utilizado para las instalaciones eléctricas con influencia moderna, práctico y con bajo nivel de complejidad para lograr ser instalado, su precio influirá según el proveedor.

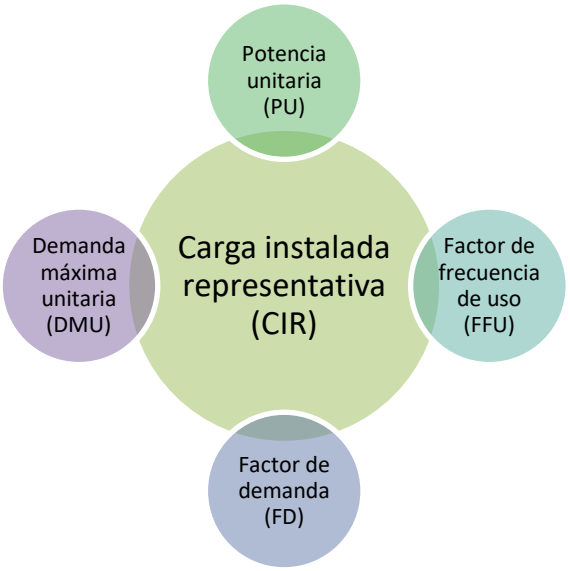
Además, estos métodos propuestos pueden transportar los requerimientos de potencia permisibles según las tablas NEC, se realiza el diseño desde el punto inicial o mejor conocido como la fuente, hasta los diferentes puntos dentro de la instalación de referencia en la planta o el edificio. La estructura conforme su diseño arquitectónico demandará el volumen total necesario para cumplir con las especificaciones diseñadas en el proyecto, estos diferentes métodos pueden incluir uso de conductores alimentadores de tamaño grande, su presentación es en barras o también en cables dentro de las canaletas, si se trabaja en barras serán cerradas en ductos ventilados.

Otro método un poco obsoleto pero eficiente, es utilizar barras de cobre incrustadas en las electromallas, se proyectan y trasladan a lo largo de las instalaciones sobre el área que se desea cubrir, además son empleadas también para trasladar la potencia requerida en los tableros instalados, no importando el nivel horizontal que complementará toda la red de distribución de potencia. Los métodos y medios propuestas estarán influidos por diferentes factores, el principal en todo proyecto es el costo. No se podrá sacrificar durabilidad por economía, o distancia cubierta por simetría arquitectónica, acá estará el pilar del diseño y el método eficiente, siempre se velará porque la instalación cumpla con todos los instrumentos de calidad y seguridad a largo plazo.

1.7. Alimentadores y subalimentadores

En una instalación eléctrica, el alimentador y los subalimentadores son los únicos responsables o encargados de trasladar la corriente demandada hacia la instalación, donde se encuentra concentrado el grupo de cargas que la consume. Para el adecuado diseño en su dimensionamiento se deberán adoptar algunos parámetros relevantes y que influenciarán el diseño.

Figura 14. **Parámetros propios que influencia en el diseño**



Fuente: elaboración propia.

1.7.1. Circuitos alimentadores a tierra

El sistema eléctrico de distribución de potencia completo debe estar a tierra en todos los puntos, tableros, tubería, partes, equipos, dispositivos y cargas. Todos los partes de la instalación deben estar sólidamente conectados a tierra.

Los conductores alimentadores comienzan en el dispositivo de protección del equipo de acometida. Estos viajan por distintos medios de distribución como las tuberías o canaletas o bandejas de cableado. Los conductores alimentadores se conectan con tableros de carga o subdistribución y juntamente con ellos en la tubería viaja el conductor de tierra, llamado conductor de equipos a tierra y se conecta en el borne a tierra que hay en cada tablero.

El alimentador se deriva de un dispositivo automático de distribución de 300 A, el conductor a tierra que conectará el tablero siguiente debe ser el # 4 TW de cobre o el # 2 TW de aluminio y su tubería donde viaja el conductor a tierra deberá conectarse también a él por medio de un conector de tierras en el principio de la tubería, el conector debe ser certificado por UL.

Además, se presenta tubería que hace de conductor a tierra entre los tableros de distribución, y es una forma eficiente de conexión a tierra por su nivel de conductor, más efectiva, debido a la mayor área de contacto de la tubería. Esta tubería debe tener impreso el símbolo de tierra, tendrá 3 hilos más de rosca y deberá apretarse debidamente para evitar un aumento de resistencia. Igualmente, con una bandeja de cableado al aire libre, debe tener impreso también el símbolo de tierra eléctrica, para usarse como conductor de tierra.

Muy importante es, que las resistencias estarán en serie sobre el sistema diseñado de tierras, por lo que se persigue disponer de baja impedancia en todos sus sistemas. La NFPA 70 propone y exige que un valor del sistema eléctrico a tierra permisible, deberá ser reportado menor a 5 ohmios medidos en la punta de conexión del conductor y la malla de electrodos.

Comúnmente este valor puede ser optimizado y reducido hasta 2 o 3 ohmios de resistencia a tierra, se recomendará cuando existen equipos sensibles

presentes, para un nivel más crítico y optimizado se recomendaría poder llevar ese valor hasta 1 ohmio.

El conductor de equipo a tierra deberá ser llevado hasta el último tablero de cargas, y de allí deberá ser trasladado en tubería por los circuitos ramales a todas las cargas eléctricas conectadas. En el tablero final de circuitos ramales, el conductor de tierra también tendrá el valor que le asigne según la Norma NFPA 70 para la carga demandada o el tipo de carga que será servida.

1.7.2. Acciones para minimizar la caída de voltaje

Aspectos relevantes que influyen en las caídas de voltaje que pueden pasar por alto, es considerar los dimensionamientos de los conductores que serán instalados, además de realizar corridas de cálculos para simular diferentes condiciones que representen picos y valles de sobrealimentación en las cargas.

La caída de voltaje, por lo tanto, deberá ser simulada por factores plenos de carga desde 120V, 208V, 240V y 480V, iniciando en el punto de conexión de la acometida, también se podrá considerar como referencia un punto secundario, el transformador, que se realizará supliendo al alimentador principal de la acometida, se considera que la caída nominal del servicio es representada por caída de voltaje.

Se podrá disponer o colocar verticalmente un alimentador de cargas, para considerar la operación del balanceo de cargas y así sus caídas de voltaje, considerando equitativamente las distancias de cada alimentador y sus respectivas cargas.

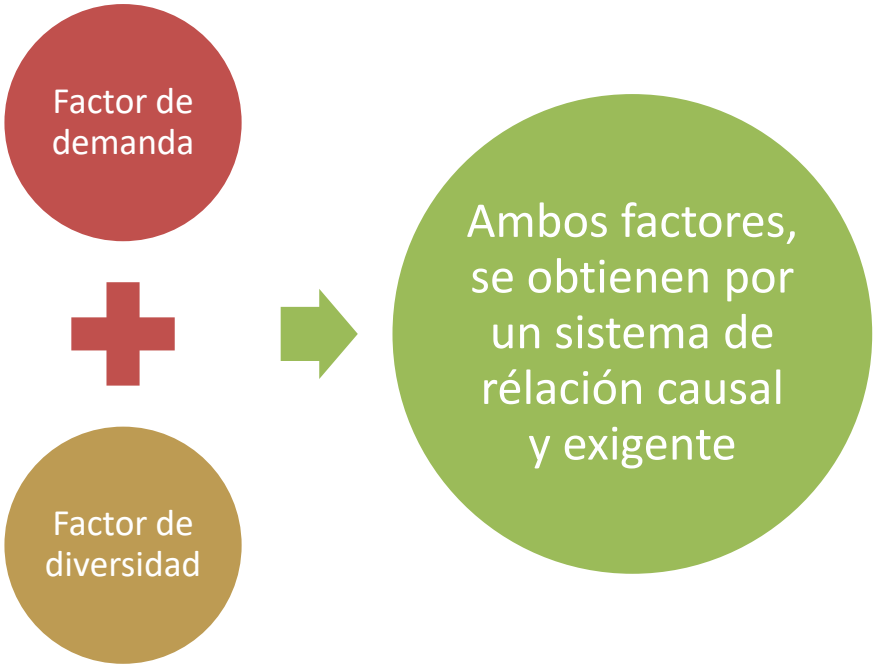
El rol del ingeniero profesional es un pilar sumamente importante, ya que deberá buscar y seleccionar los puntos óptimos donde se concentra la carga, además deberá colocar su equipo de distribución en la última carga que alimentará.

1.7.3. Otros factores de demanda importantes

Con la regulación de tensiones sobre los dispositivos eléctricos y electrónicos, se puede plantear una diversidad de factores demandados, pero con el avance de la ciencia y la tecnología, se han logrado reducir en dos importantes vertientes o ramales de interés para los profesionales.

Por lo cual el movimiento constante de investigación sobre ciertas variables que podrían llegar a ser considerables, descartando las de menor relevancia o impacto según la demanda de los consumidores, hace frente a dos factores que generan mayor interés o análisis de estudio. Estos factores se dividen por su complejidad y relación de demanda, por el tipo de carga consumida y la cantidad de carga demandada de un sistema.

Figura 15. **Factores relevantes o importantes por su demanda**



Fuente: elaboración propia.

Idealmente el factor de demanda se obtiene por la relación que exige la demanda máxima operando en un sistema, se podría contemplar subdivisiones o sectores activos, contemplándolos también como partes del sistema activo, así es como su carga total es obtenida por permanecer activamente conectado al sistema vivo, o por cierta fracción. Se reconoce que el factor de demanda es < 1.

A comparación el factor de diversidad se obtiene por la sumatoria de las demandas máximas individuales obtenidas de las diferentes subdivisiones de un sistema, también se toma en cuenta y no son despreciadas las partes de ese sistema sobre la demanda máxima del sistema completo o parte del sistema considerado, aquí se reconoce un factor variable ente 1,00 y 2,00.

Estos factores ya mencionados, son empleados constantemente en los diseños de sistemas eléctricos. Cuando se realiza balance de cargas se expresa por medio de su sumatorias, donde las cargas suplidas por el alimentador son multiplicadas por un factor de demanda, al realizar este procedimiento se está determinando la carga. La carga encontrada, es denominada máxima demanda por el alimentador (según la NFPA 70 su capacidad mínima permisible estará dada por el calibre del conductor).

Desde el punto de vista unifilar se reconoce como un único conductor, se le llama conductor alimentador, entonces, este conductor podrá estar alimentando diferentes subalimentadores (tableros) al mismo tiempo. Acá se da la premisa que, si ese alimentador es de 300 KVA en los circuitos de potencia conectada, sucesivamente después se podrá multiplicar por un factor de demanda máxima sobre su 80 %, además, la capacidad que será estimada como mínima permitida a ser instalada o suplida será de 240 KVA, asumiendo que los datos y cálculos serán para ese alimentador de circuitos de potencia.

De esa forma y sucesivamente, se deberán analizar los siguientes alimentadores dentro del circuito y proyecto de interés. Donde cada una de las cargas que se encuentra conectada de forma real, es multiplicada por su demanda máxima para ese mismo alimentador, por lo tanto, la capacidad en KVA que se programa instalar en el alimentador, deberá ser la multiplicación de ambos términos.

Fórmula 11

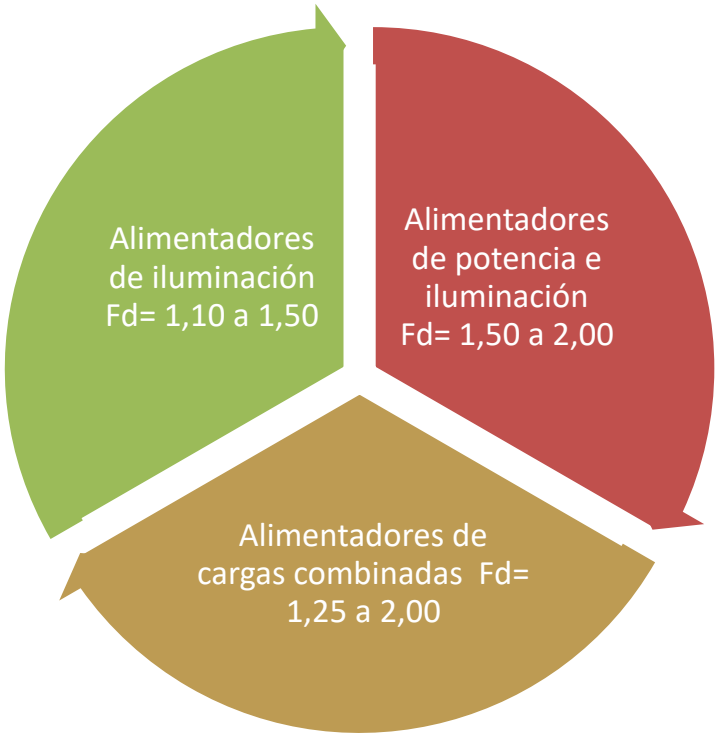
$$(Demanda\ máxima)x(carga\ conectada) = capacidad\ mínima\ del\ conductor - potencia\ (KVA)$$

Fórmula 12

$$Potencia\ (KVA) = \ (voltaje)\ x\ (corriente)$$

Se podrán emplear límites aparentes para la carga futura, según la Norma NFPA 70 establece que un 25 % a un 50 % de la carga calculada podría ser operativamente viable. Luego de realizar el cálculo de la carga, está será la carga total por instalarse, sin olvidar que la carga que se encuentra conectada será la carga real ya instalada en cualquier momento que sea necesario.

Figura 16. **Diversidad de factores según sus cargas requeridas**



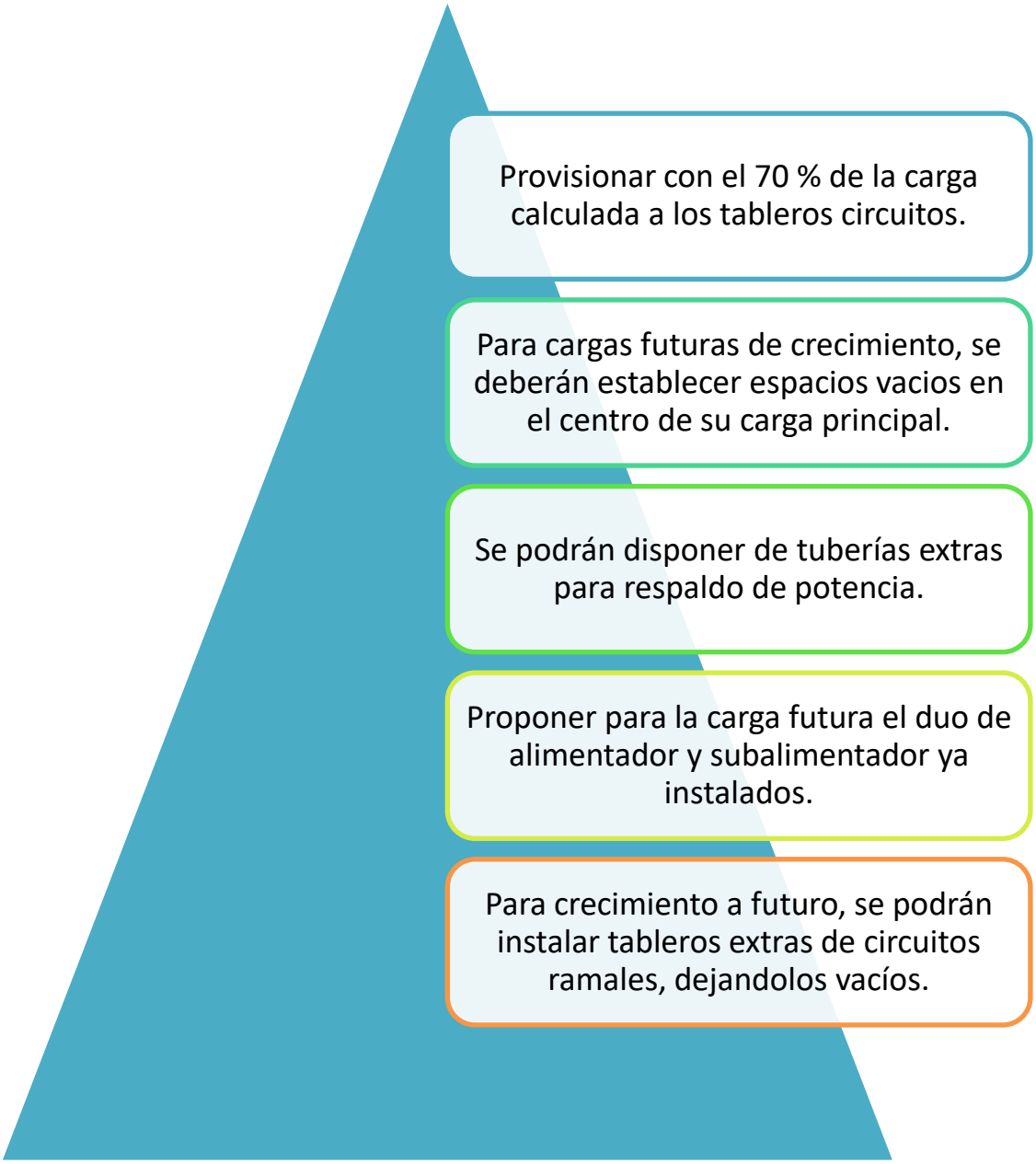
Fuente: elaboración propia.

Por otro lado, al analizar específicamente al factor de diversidad, se deberá tratar de concretar cómo trabaja su modelo o sistema, el cual, por medio de la observación en secuencias de tiempo programadas a lo largo de una jornada o período establecido, se tratará de establecer un conteo de sus demandas parciales con índices máximos sobre cada alimentador lograron operar a su máxima capacidad en los picos determinados. Se entenderá para su síntesis, que no todos los alimentadores presentes en su análisis presentarán una máxima demanda.

También se puede analizar otra variable, la que muestra representativa que se obtiene al incrementar el factor de diversidad, por lo tanto, su capacidad en KVA será menor. Además, la infraestructura o instalación será totalmente dependiente del factor económico sobre la inversión del proyecto. Se considera evaluar la flexibilidad, capacidad, confiabilidad y seguridad en cada uno de los proyectos que puedan ser presentados, posiblemente así el sistema eléctrico final pueda ser el adecuado para las actividades programadas y destinadas.

Cada uno de los alimentadores presentes y planteados en el proyecto de incidencia, tendrá su demanda máxima, se realizará la sumatoria de los alimentadores sobre su demanda real aplicada, proporcionando un valor total de la sumatoria de las demandas máximas del conjunto de alimentadores, pero su demanda máxima en el sistema será diferente se esa sumatoria de demandas. La diferencia estará directamente proporcional al tiempo transcurrido para cada muestra.

Tabla VIII. **Conjunto de técnicas adicionales que permiten hacer un cálculo aproximado de la carga futura**



Fuente: elaboración propia.

Se deberá diseñar la protección idónea, esta dependerá a la carga conectada en un tiempo *t* al sistema, además de que los conductores y la capacidad de las barras en el tablero deberán ser dimensionadas según la carga final calculada, a eso se le deberá adicionar la capacidad de carga futura.

2. SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA

2.1. Proceso de planificación

Parte inicial e importante del proyecto, es crear las condiciones efectivas para la realización debida del diseño, implementación y gestión del SGSI, para esto la empresa o el usuario interesado deberá realizar el estudio sobre la situación del sistema informático desde una perspectiva que mitigue la vulnerabilidad ante las amenazas.

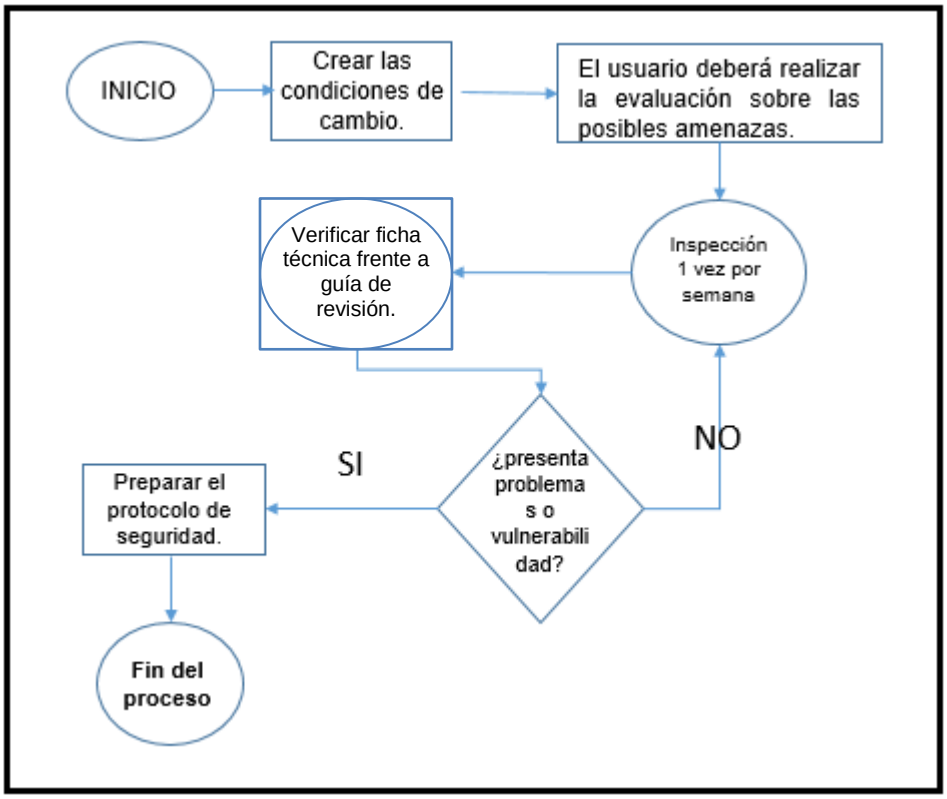
Su fin principal será lograr determinar cuáles pueden ser las acciones que se puedan ejecutar en función de las necesidades detectadas y con ello iniciar el protocolo para establecer las políticas internas, los objetivos, procesos y procedimientos de seguridad totalmente apropiados para gestionar el riesgo y mejorar la seguridad informática, trabajando apegados y en conjunto a las políticas y objetivos específicos de la organización.

Los bienes informáticos que dispone una entidad no representan el mismo valor, algunos no se encuentran expuestos a los mismos riesgos, por lo que será primordial y fundamental, realizar un análisis de riesgo, esto es idóneo para ofrecer un valor estimado de los bienes informáticos y el tipo de amenazas a las cuales pueden estar expuestos, además de incluir las guías técnicas de respuesta ante los riesgos suscitados indicando la forma de accionar para mitigarlos o reducirlos.

La parte final en la planificación es establecer prioridades en las tareas asignadas o las tareas por realizar que permitan minimizar los riesgos. Ya que el

constante asedio hace que los riesgos se permanezcan constantes, acá se deberá comprometer el desarrollo de la dirección para que asuma el riesgo residual y así incluir en nivel restante de riesgo luego de su tratamiento.

Figura 17. **Proceso perfecto de planificación del sistema de gestión de la seguridad informática**



Fuente: elaboración propia, empleando Visio 2016.

2.1.1. Preparación

Parte vital del proyecto, se deberán crear las condiciones para que el diseño de implementación pueda considerar diferentes aspectos relevantes. Además, la

dirección administrativa deberá apoyar constantemente con los protocolos de seguridad dentro de la organización mediante una guía clara y ordenada que a la misma vez sea una orientación básica.

Así mismo, la dirección poseerá el compromiso y la tarea de asignar responsabilidades explícitas de seguridad informática y el reconocimiento de las variables que vulneran los datos privados de los usuarios. Otro aspecto que se debe considerar en la gestión de preparación es lograr enmarcar sistemáticamente un contexto que se conforme por diferentes procesos, estos deberán estar asegurados e incluidos en la gestión de la preparación.

Tabla IX. **Criterios que fundamentan la ruta lógica para establecer un contexto general en la preparación**

Fundamento de la acción	**Tipo de argumento que permitirá adoptar una implicación a establecer**
Criterios básicos necesarios para la gestión del riesgo	Criterios de evaluación, de impacto y de aceptación del riesgo.
Definir los alcances y límites	Garantizar que todos los activos se tomen en consideración, de acuerdo con su relevancia y jerarquización de importancia.
Establecer una organización adecuada que opere la gestión de riesgo	identificar las dependencias involucradas, asignarles funciones y responsabilidades y establecer una ruta para escalar decisiones y especificar los registros que se deben conservar.
Valoración del riesgo	Implica la identificación y descripción cuantitativa y cualitativa del riesgo lo que permite priorizar frente a los criterios de evaluación del riesgo establecidos para la organización.
Identificación del riesgo	Permite inferir por una pérdida potencial y cómo y dónde podría generarse esta pérdida.

Continuación de la tabla IX.

Identificación de los activos	Relaciona la cantidad de activos y su relevancia, así como el propietario o responsable del mismo.
Identificación de las amenazas	Buscar información sobre las amenazas y sus orígenes. Generar una línea de tiempo de exposición al riesgo y a sus transformaciones tecnológicas.
Identificación de los controles existentes	Realizar un inventario de los controles implementados en la organización, evaluando su funcionamiento y su efecto para reducir la vulnerabilidad. Revisando los documentos que lo sustentan, verificando con el personal que lo maneja y verificando la estructura física relacionada.
Identificación de las vulnerabilidades	Relacionar las amenazas con los riesgos para determinar la vulnerabilidad. Debe identificarse en cada una de las dependencias de la organización y en cada uno de los pasos de los procesos de gestión.
Identificación de las consecuencias	Identifica los daños que podrían ser causados por un escenario de incidente.

Fuente: LÓPEZ, Ricardo. *Sistema de gestión de la seguridad informática*. p. 55.

La implementación en la etapa de preparación del sistema de alerta temprana en la gestión de riesgo buscará mitigar al máximo las posibles consecuencias adversas al evento de riesgo; se podrá adoptar la inversión proporcional de recurso humano y monetario, con esto se espera beneficiar los rubros importantes del usuario o de la empresa que implemente las acciones correspondientes.

2.1.2. Compromiso de la dirección con la seguridad informática

Trabajo intermitente, de valoración inmediata y constante, donde la alta dirección o la persona responsable del proyecto por implementar, deberá apoyar en todo momento la seguridad dentro de la empresa o el conjunto de usuarios que puedan ser vulnerados a través del uso de IOT, empleando la orientación clara, a través del compromiso y la asignación explícita de las responsabilidades de seguridad informática y su reconocimiento.

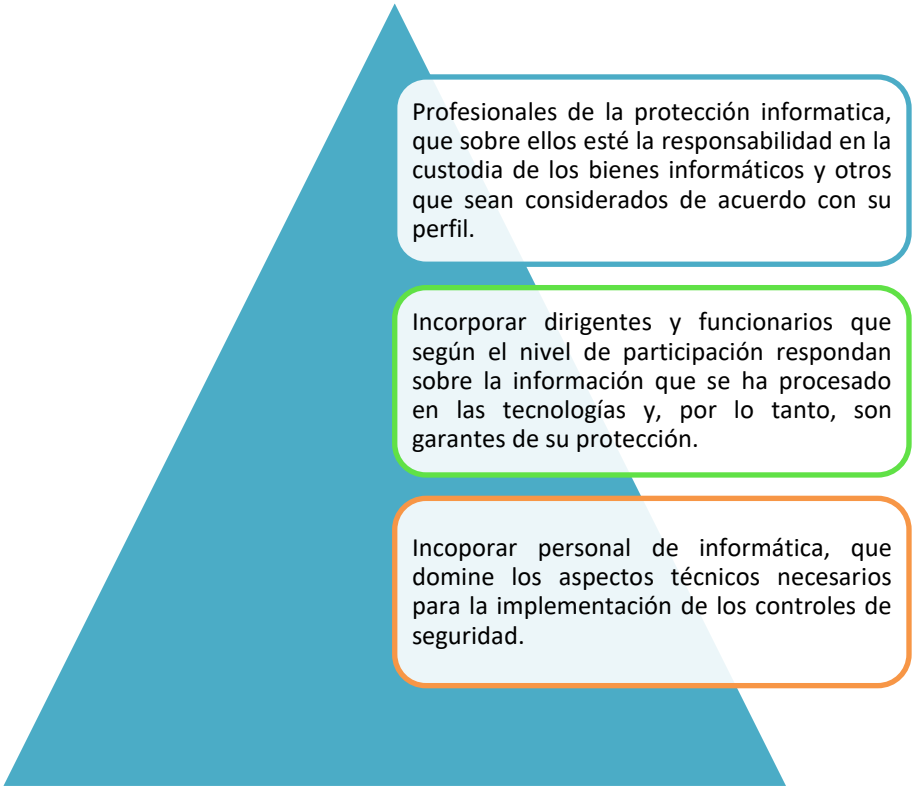
Tabla X. **Conjunto de actividades y compromisos adquiridos por la dirección en la gestión de seguridad del usuario**

	Tipo de actividad o compromiso
•	Asegurar que todos los objetivos de seguridad informática se planteen debidamente identificados, además que cumplan con los requisitos establecidos por la organización, estos deberán estar debidamente integrados en los procesos principales.
•	Se deberá formular, revisar y aprobar el conjunto de políticas de seguridad informática.
•	Continuamente se deberá revisar la efectividad de la implementación de las políticas de seguridad.
•	Se deberá proveer la orientación clara y todo el apoyo visible hacia las iniciativas de seguridad.
•	Los recursos necesarios que complementen el rol de la seguridad, deberán ser proporcionados.
•	Se deberá aprobar y designar la asignación de los roles específicos y responsabilidades en seguridad informática en la organización.
•	Enfatizar en el aseguramiento sobre la implementación de los controles de seguridad informática, que sea coordinado por toda la organización.

Fuente: elaboración propia.

Además, el proceso de diseño e implementación del futuro proyecto de seguridad informática no deberá ser realizado por una sola persona, tampoco se atribuirán roles o autorizaciones para un determinado grupo de personas con una misma especialidad, por lo que se espera que el resultado final sea producido por un equipo multidisciplinario en el que participen los altos mandos, los técnicos disponibles, los académicos profesionales y el ingeniero responsable del proyecto total. Así de manera integral puedan garantizar el cumplimiento de los objetivos planteados.

Figura 18. **Formulación del equipo que participará con el compromiso impulsado por la empresa**



Fuente: Oficina de seguridad de redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 11.

2.1.3. Recopilar información de seguridad

Durante el proceso de preparación el equipo de trabajo responsable de la seguridad informática deberá unificar la información que facilite el diseño e implementación del sistema de gestión de seguridad informática, para lo cual se deberán emplear documentos normativos y metodológicos diseñados sobre el tema por implementarse.

Además, incorporar el desarrollo de la documentación de aplicaciones y sistemas en explotación de la organización, documentación de incidentes ocurridos dentro de la empresa y en áreas de riesgo que fueron vulneradas, también se deberá formalizar el uso de las tendencias de seguridad nacionales e internacionales, así como el uso de otros instrumentos y herramientas que permitan faciliten su realización.

2.2. Determinación de las necesidades de protección

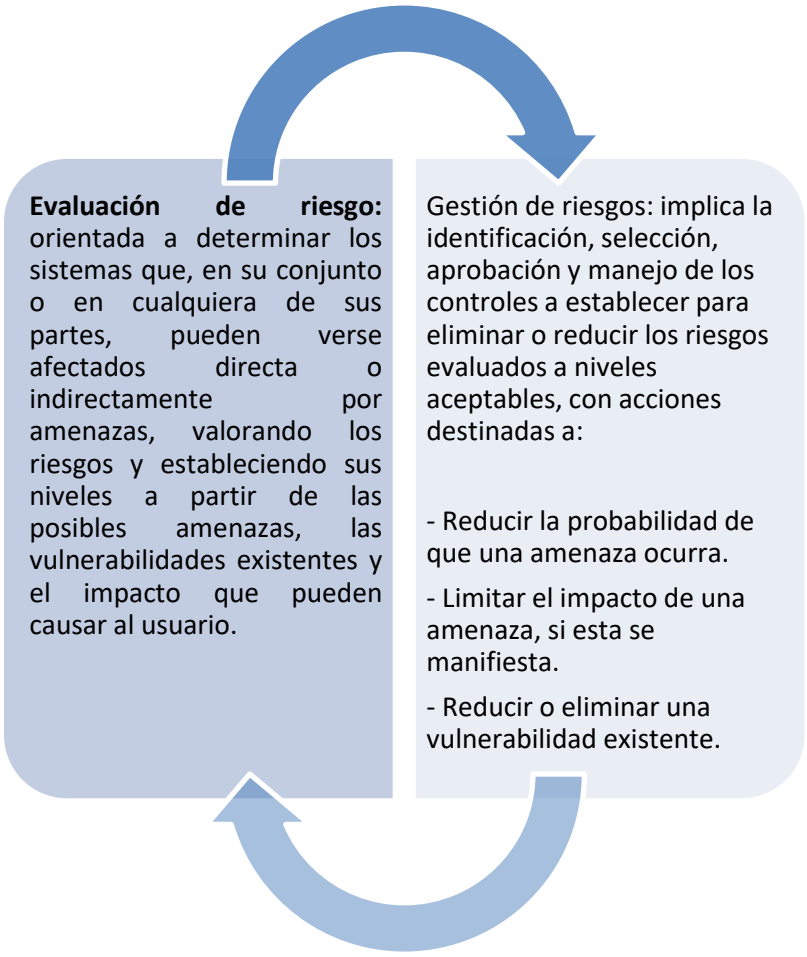
Para la protección y resguardo del sistema informático, se deberán establecer mediante la realización de análisis de riesgos, este proceso está dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos, lo cual implicará la identificación de los bienes por proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que podrían causar.

- Fases por incorporar en el análisis de riesgos

    - Realizar una detallada caracterización del sistema informático objeto de protección.
    - La creación de un inventario de bienes informáticos por proteger.

- Evaluación de los bienes informáticos por proteger en orden de su importancia para la organización.
- Identificación y evaluación de amenazas y vulnerabilidades.
- Estimación de la relación importancia-riesgo asociada a cada bien informático.

Figura 19. **Aspectos fundamentales que diferencian el proceso de análisis de riesgos**



Fuente: elaboración propia.

Además, la gestión de riesgos implica la clasificación de las alternativas para manejar los riesgos que se puedan estar sometiendo sobre un bien informático dentro de los procesos en una entidad. Esto implica desarrollar una estructura bien definida, con controles adecuados y su conducción mediante acciones factibles y efectivas.

Tabla XI. **Técnicas de manejo del riesgo según sean las necesidades de protección**

Técnica	Descripción
Evitar	Impedir el riesgo con cambios significativos por mejoramiento, rediseño o eliminación, en los procesos, siendo el resultado de adecuados controles y acciones realizadas.
Reducir	Cuando el riesgo no puede evitarse por dificultades de tipo operacional, la alternativa poder ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla y se consigue optimizando los procedimientos y con la implementación de controles.
Retener	Cuando se reduce el impacto de los riesgos pueden aparecer riesgos residuales. Dentro de las estrategias de gestión de riesgos de la entidad se debe plantear como manejarlos en un nivel mínimo.
Transferir	Es buscar un respaldo contractual para compartir el riesgo con otras entidades, esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferir a otro, o para minimizarlo.

Fuente: Oficina de seguridad de redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 13.

2.3. Caracterización del sistema informático

En un sistema de informático que requiera diseño e implementación, será imprescindible el conocimiento pleno del objeto sobre el cual se requiere diseñar

o implanta. Para eso, deberá ser apropiado precisar los elementos que permitan identificar las especificaciones de este.

La caracterización del sistema informático incluye la determinación de los bienes informáticos que requieren ser protegidos, su valoración y clasificación según su importancia.

Se precisarán los datos que permitan determinar cómo fluye la información entre los diferentes elementos de la entidad, así como entre la entidad y otras instituciones considerando el carácter de la información y su nivel de clasificación de acuerdo con lo establecido en el país.

Durante la caracterización del sistema informático es necesario establecer además las características de las edificaciones y locales donde están instalados los equipos, tipo de construcción y estructura, lugares o puntos de acceso, visibilidad desde el exterior, la ubicación de las tecnologías de la información, tipos de tecnologías, software instalado, nivel de clasificación de la información que se procesa, documentación de software, preparación y conocimiento del personal que opera los equipos, así como cualquier otro aspecto que haga más precisa su descripción.

Tabla XII. **Agrupación de categorías que facilitan la identificación de bienes informáticos por proteger**

Bien	Descripción
Hardware	Redes de diferente tipo, servidores y estaciones de trabajo, computadoras personales (se incluyen las portátiles), soportes magnéticos y ópticos, medios informáticos removibles, líneas de comunicaciones, módems, ruteadores, concentradores.
Software	Programas fuentes, programas ejecutables, programas de diagnóstico, programas utilitarios, sistemas operativos, programas de comunicaciones.
Datos	Durante la ejecución, almacenados en discos, información de respaldo, bases datos, trazas de auditoría, en tránsito por los medios de comunicaciones.
Personas	Usuarios, operadores, programadores, personal de mantenimiento.
Documentación	De los programas empleados, de los sistemas, del hardware, de procedimientos de administración.

Fuente: Oficina de seguridad de redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 14.

Luego de identificar los bienes informáticos que necesitan ser protegidos, se determinará su importancia dentro del sistema informático y se clasificarán según su prioridad. La valoración de estos bienes informáticos posibilitará mediante su categorización, el lograr determinar en qué medida es más importante uno del otro, para establecer un grado de importancia.

Además, se deberá realizar considerando los aspectos tales como: la función que realizan, su costo requerido, la repercusión que ocasionaría la pérdida y posibilidad de recuperación de estos; así como la preservación de la confidencialidad, la integridad y disponibilidad.

Subjetivamente el lograr estimar la repercusión que ocasionaría la pérdida de un bien informático deberá contener el tiempo que la entidad podría continuar trabajando sin el mismo, lo que puede ser vital para su funcionamiento. Ese tiempo podría oscilar entre pocas horas, hasta días y semanas.

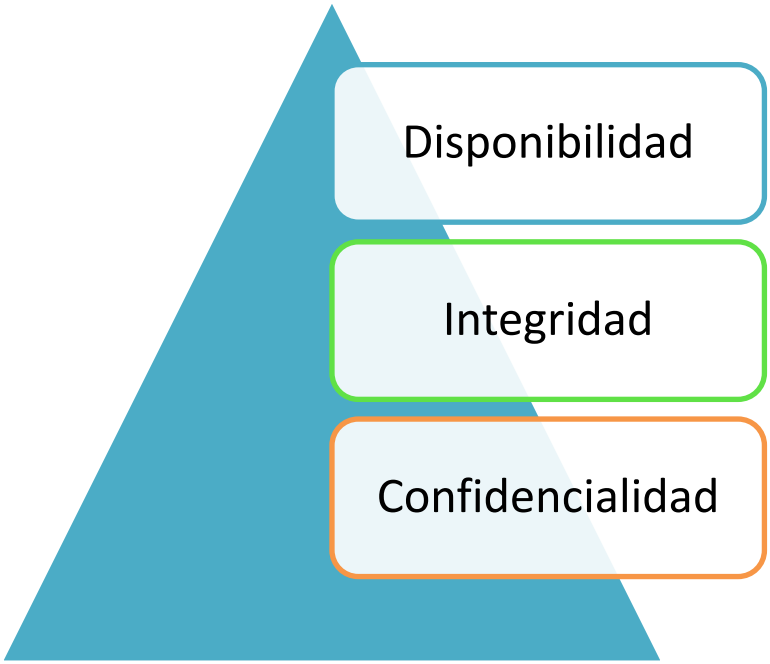
Se considera, además, que un bien informático puede permanecer por un período de hasta dos o tres semanas dañado, esto dependerá del ciclo de uso. Por lo tanto, la importancia de cada bien informático se puede realizar de forma descriptiva empleando protocolo de valoración o asignación de estatus por necesidad (valor alto, valor medio, valor bajo), otro protocolo de valoración que puede ser empleado es por asignación de forma numérica, asignando valores desde cero hasta diez (0 si tiene poca importancia y 10 sí es máxima). El resultado inmediato y a corto plazo de la caracterización del sistema informático deberá ser la confirmación de una lista que contenga la relación de los bienes informáticos identificados y clasificados según su relevancia de participación en el sistema empleado por el usuario, que deberá ser proporcional a su importancia.

2.4. Identificación de las amenazas sobre el sistema informático

Luego de identificar los bienes informáticos prioritarios que desean ser protegidos, se valoran según sus funciones dentro de la red interna y su importancia, será necesario identificar las posibles amenazas y estimar el posible daño (impacto) que puede producir su materialización.

Se deben establecer los protocolos de identificación para cada bien informático por proteger, se valorarán los objetivos fundamentales de seguridad, los cuales se mostrarán en una pirámide de jerarquías, además se debe determinar cada amenaza sobre la base de cómo podría llegar a afectar a estas características de la información.

Figura 20. **Pirámide de seguridad informática por jerarquía y precedencia**



Fuente: elaboración propia.

La relevancia e influencia de cada una de las características presenta para los bienes informáticos, varía de una entidad a otra, en dependencia de la naturaleza de los procesos informáticos que se llevan a cabo en función de su objeto social.

Figura 21. **Amenazas comunes sobre el sistema informático**

Fuente: elaboración propia.

Empleando el análisis de riesgos es clave y vital para desempeñar las funciones de un examen a cada una de las amenazas sobre los bienes informáticos y su clasificación por niveles jerárquicos, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir.

2.5. Estimación del riesgo sobre los bienes informáticos

Se validará la estimación de riesgo sobre cada bien informático involucrado o de objeto de análisis, considerando las probabilidades de materialización de las posibles amenazas que actúan sobre el mismo. Esto se realiza de forma

descriptiva, también aplica de forma numérica asignando valores entre cero y uno (0 sí la probabilidad que se materialice la amenaza es nula y 1 sí es máxima).

Cualquier tipo de amenaza por leve o agresiva puede incidir sobre varios bienes informáticos con la misma probabilidad y, sin embargo, sus consecuencias no serán iguales, acá ocurre la premisa de probabilidad selectiva, dependiendo en por casos aislados y separados la importancia del bien afectado. La interrelación entre la probabilidad de materialización de las amenazas que actúan sobre un bien informático y la importancia estimada determinan el nivel del riesgo.

La segmentación y preparación de las evaluaciones sobre los riesgos, crea la posibilidad de conocer cuáles pueden ser los bienes informáticos vulnerables, o cuáles serán las áreas expuestas o vulnerables que pueden ser sometidas a una mayor probabilidad de riesgo. Esto proyectará emplear selección adecuada de controles de seguridad que deben ser establecidos en cada uno de los casos, garantizándose de esta manera la correcta proporcionalidad por medio de la adecuada relación entre costos y beneficios.

Será necesario establecer de forma puntual cuales pueden ser los riesgos a que está expuesto el sistema en cada una de sus partes y componentes, a partir de lo cual se podrán determinar con racionalidad los controles de seguridad que deben ser implementados.

2.6. Selección de los controles de seguridad informático

Luego de establecer los procedimientos que lógicamente conforman la evaluación, creación de los supuestos y controles a futuro sobre las áreas

vulnerables que se encuentran en riesgo identificado, se adoptará una decisión sobre su tratamiento o corta fuego.

Tabla XIII. **Posible decisión adoptada a futuro sobre el posible riesgo a identificar**

Decisión	**Acción de mitigación o resultado esperado**
Aplicar controles apropiados	Para lograr reducir los riesgos de bajo nivel.
Aceptar riesgos	Se adoptan de manera consciente y objetiva, siempre que satisfagan las políticas y criterios de la organización para la aceptación de riesgos.
Evitar riesgos	Rechazando las acciones que propicien los riesgos.
Transferir los riesgos	A instituciones de respaldo o resguardo, donde se obtenga un programa de o plan de seguro informático.

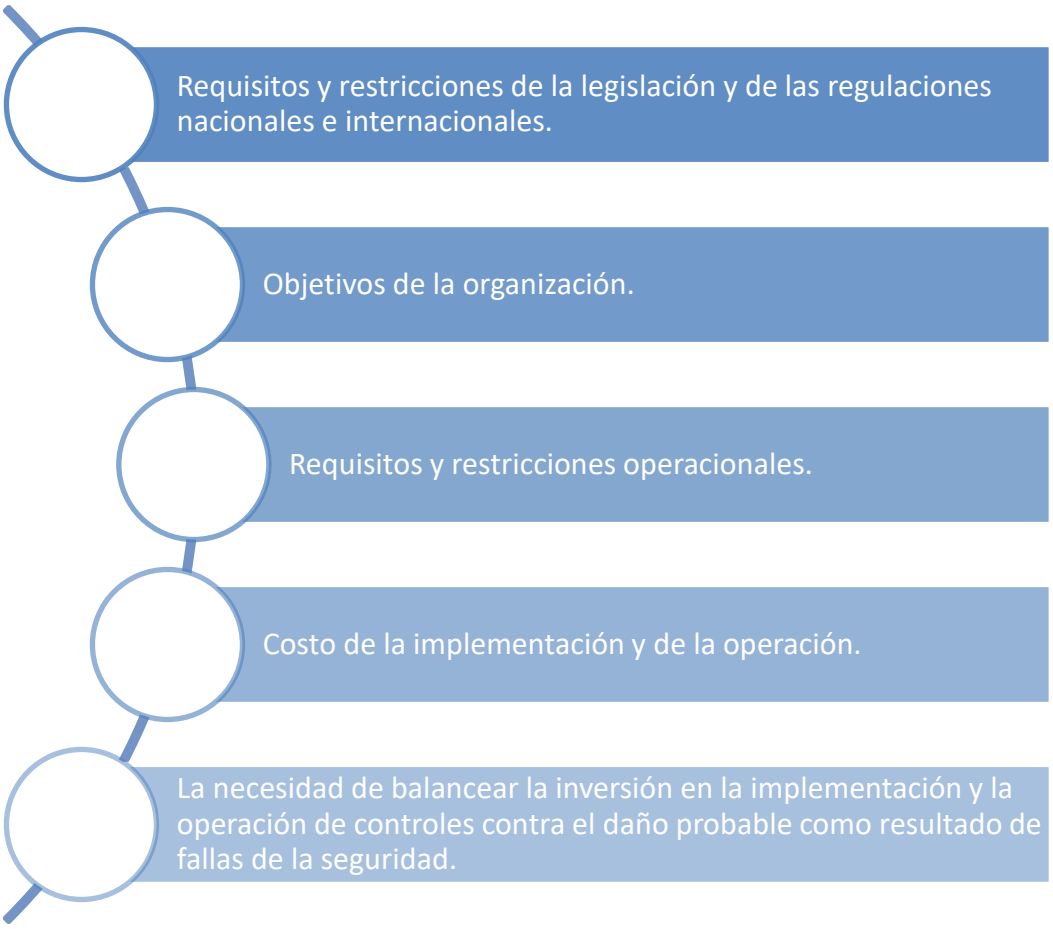
Fuente: Oficina de seguridad paras las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 19.

Además, existen riesgos donde se puede aplicar controles apropiados, estos deberán ser seleccionados e implantarse para lograr los requisitos identificados mediante la evaluación de riesgos. Los controles deberán asegurar que puedan ser reducidos a un nivel aceptable y permisible.

Cuando se establezcan controles de seguridad, deberán ser seleccionados para apoyar la reducción de riesgos a nivel aceptable que puedan respaldar adecuadamente las necesidades específicas de la organización. Junto con la selección de los controles de seguridad que dependerán de una decisión organizacional basada en criterios para la aceptación del riesgo, se incluyen las opciones de tratamiento y el debido acercamiento a su gestión general en donde

será aplicada a la organización. También será apegada al marco legal que rija en Guatemala sobre leyes informáticas y sus derivadas.

Figura 22. **Tipos de controles fundamentales predominantes en la toma de decisiones**



Fuente: elaboración propia.

Los objetivos de control y los controles se basan en la incorporación de los resultados y conclusiones de la evaluación de riesgos, en los procesos de tratamiento del riesgo; en los requisitos legales o reglamentarios, en las

obligaciones contractuales y en las necesidades orgánicas de la entidad en materia de seguridad informática.

Además, cada uno de los controles de seguridad informática deberá ser considerado en la etapa específica de requisito, conforme a la arquitectura del diseño en el sistema y su posible aplicación. El faltar a este ordenamiento podría dar lugar a costos adicionales y a soluciones menos eficaces, también puede podría reducir el porcentaje de eficiencia esperado en el nivel de seguridad adecuado. Por lo tanto, esos controles deberán ser establecidos, implementados, supervisados y mejorados cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad en la organización.

2.6.1. Políticas de seguridad informática

Consistirá en lograr proporcionar la orientación y guía técnica hacia la dirección de la seguridad informática institucional o del usuario de las OIT, de acuerdo con los requisitos de la organización y con las leyes y regulaciones vigentes.

Por lo cual, la dirección establecerá políticas de seguridad en correspondencia con los objetivos de la empresa para demostrar el apoyo y compromiso a la seguridad informática, publicando y manteniendo las políticas en toda la organización, las cuales se podrán comunicar hacia todos los usuarios de forma apropiada, accesible y comprensible.

La formulación de las políticas de seguridad ronda sobre una estructura analítica subjetiva basada en la concepción del qué, qué deberá ser protegido, qué puede presentar mayor importancia, qué puede ser o no prioritario, qué puede estar permitido y qué no puede estar permitido, qué tipo de tratamiento se

le puede desarrollar a los problemas de seguridad. Las políticas de seguridad en sí misma no dicen “cómo” las cosas son protegidas, esto se desarrollará en función de las medidas y procedimientos de seguridad.

Por eso, se indica que las políticas de seguridad conforman la estrategia general. Las medidas y procedimientos que establecen en detalle las etapas requeridas para proteger el sistema informático. No pueden existir medidas y procedimientos que no respondan a una política, al igual que no pueden concebirse una política que no esté complementada con las medidas y procedimientos que le correspondan.

Tabla XIV. **Componentes fundantes de las políticas de seguridad**

	Base de acción según futuras necesidades
•	El tratamiento que requiere la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría.
•	Emplear convenientemente y segura las tecnologías instaladas en cada uno de los servicios que se puedan disponer.
•	La definición de los privilegios y derechos de acceso a los bienes informáticos para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación, mediante la especificación de las facultades y obligaciones de los usuarios, especialistas y dirigentes.
•	Los aspectos relacionados con la conexión a redes de alcance global y la utilización de sus servicios.
•	El establecimiento de los principios que garanticen el efectivo control de acceso a las tecnologías (se incluye el acceso remoto).
•	Las normas generales relacionadas con la información de respaldo y su conservación.

Continuación de la tabla XIV.

•	Los principios por tomar en cuenta sobre los requerimientos de seguridad informática que deban ser considerados en la adquisición de nuevas tecnologías.
•	Los aspectos relacionados con la adquisición por cualquier vía de software y documentos de fuentes externas a la entidad y la conducta por seguir.
•	La definición de las responsabilidades de los usuarios, especialistas y dirigentes, sus derechos y obligaciones respecto de la seguridad informática.
•	La definición de los principios relacionados con el monitoreo del correo electrónico, la gestión de las trazas de auditoría y el acceso a los ficheros de usuarios.
•	Las normas por tomar en cuenta con relación al mantenimiento, reparación y traslado de las tecnologías y del personal técnico (interno y externo) que requiera acceso a las mismas por esos motivos.
•	Los principios generales para el tratamiento de incidentes y violaciones de seguridad, que se considera incidente de seguridad y a quién debe reportarse.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 23.

Las políticas de seguridad informática serán revisadas por programación de intervalos programados, se esperan surgimientos de cambios significativos para asegurar su actualización, adecuación y efectividad.

2.6.2. Medidas y procedimientos de seguridad informática

Las diferentes medidas y procedimientos de seguridad se implementarán en correspondencia con las políticas definidas, las cuales conforman el cuerpo del sistema de seguridad diseñado y representan la línea de defensa básica de protección de los bienes informáticos, por lo cual, será importante emplear una

objetiva selección, de forma tal que cubran las amenazas identificadas durante el proceso de evaluación de riesgos, implementándolas de forma rentable ante la organización.

Las medidas de seguridad informática se clasifican de acuerdo con el origen de la causa o factor de riesgo se dividen en: administrativas, de seguridad física, técnica o lógica, de seguridad de operaciones, legales y educativas. A su vez, por su forma de actuar, las medidas pueden ser: preventivas, de detección y de recuperación.

Tabla XV. **Tabla de medidas de seguridad informática**

Creación de medida	**Descripción y alcance**
Administrativa	No son apreciadas frecuentemente en toda su importancia, a pesar de que la práctica ha demostrado que un elevado por ciento de los problemas de seguridad se puede evitar con medidas de esta naturaleza. Serán establecidas por la dirección de cada entidad mediante las regulaciones comprendidas dentro de las facultades y, por tanto, son de obligatorio cumplimiento por todo el personal hacia el cual estarán dirigidas.
Seguridad física	Constituyen la primera barrera de protección en el sistema de seguridad informáticas e introducen el retardo que incrementa el tiempo de materialización del acto doloso o accidental. Se aplican a los locales donde se encuentran las tecnologías de información y directamente a estas mismas tecnologías se incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

Continuación de la tabla XV.

Técnica o lógica	Son las de mayor requerimiento dentro del sistema de seguridad informática, pueden ser implementadas por software, a nivel de sistemas operativos y de aplicaciones o por hardware. El uso combinado de técnicas de software y hardware incrementa la calidad y efectividad en la implementación de ese tipo de medidas. Algunos tipos de medidas técnicas son empleadas para identificar y autentificar usuarios, protección criptográfica, protección contra virus y otros programas dañinos, registro de auditorías entre otros.
Seguridad de operaciones	Estarán dirigidas a lograr la eficiente gestión de la seguridad mediante la ejecución de procedimientos definidos y deben garantizar el cumplimiento de las regulaciones establecidas por cada entidad y por las instancias superiores a la misma.
Legal	Representan ser el mecanismo de disuasión que contribuye a prevenir incidentes de seguridad y sancionar adecuadamente a los violadores de las políticas establecidas por la entidad. Estas son establecidas mediante disposiciones jurídicas y administrativas, en los cuales se plasman: deberes, derechos, funciones, atribuciones y obligaciones, así como se tipifican las violaciones y tipos de responsabilidad administrativas, civiles, penales u otras.
Educativa	Están dirigidas a inculcar la forma mental de actuar, mediante la cual el individuo esté consciente de la existencia del sistema de gestión de seguridad informáticas. Donde puedan ser sustentados dos elementos fundamentales: • La existencia de un sistema de gestión de seguridad informática. • La participación consciente del hombre en el éxito de los objetivos de seguridad planteados.

Continuación de la tabla XV.

Recuperación	Están dirigidas a garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos ante cualquier eventualidad que pueda ocurrir, que afecte o ponga en peligro el normal desarrollo de estos. Se establecen a partir de la identificación de los posibles incidentes o fallos que puedan causar la interrupción o afectación de los procesos informáticos y garantizan las acciones de respuesta por realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios para ello.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 27.

Con la implementación de las políticas de seguridad informática, requiere generalmente de la realización de un conjunto de acciones que permitan garantizar el cumplimiento. La descripción de esta secuencia de acciones constituye el procedimiento de seguridad. Los procedimientos, al igual que las medidas, se clasifican en procedimientos de prevención, de detección y de recuperación.

Tabla XVI. **Procedimientos propuestos para la seguridad informática**

Procedimiento	Descripción
Prevención	Su objetivo es asegurar las acciones que se requieren para evitar que una amenaza se pueda materializar, y los de detección se dirigen a identificar cualquier tipo de indicio que revele la posible materialización de una amenaza, la amenaza en desarrollo o de una posible vulnerabilidad en los sistemas.
Recuperación	No es la prevención, ni la detección de posibles amenazas, su función es lograr establecer las acciones que se deben ejecutar cuando una amenaza ya se ha materializado, afectando parcial o totalmente los bienes informáticos.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 27.

2.7. Propuesta del plan de seguridad informática

Las actividades referentes al plan de seguridad informática serán coordinadas por los consejos de dirección de los órganos, organismos y entidades, proponiendo incluir personal de diferentes partes de la organización con funciones y roles específicos.

Tabla XVII. **Atributos y acciones que fortalecen la propuesta del plan de seguridad informática**

	Ítem
•	Verificar que las actividades referentes a la seguridad sean ejecutadas de acuerdo con las políticas establecidas.
•	Identificar cómo manejar los incumplimientos.
•	Aprobar metodologías y procedimientos para la seguridad informática.
•	Identificar cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas.
•	Evaluar la adecuación y coordinación de la implementación de los controles de seguridad informática.
•	Promover en forma efectiva la educación, la formación y la concienciación en seguridad informática a través de la organización.
•	Evaluar la información resultante del tratamiento y análisis de los incidentes de seguridad informática y las acciones recomendadas en respuesta a los mismos.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 30.

El objetivo del plan de seguridad informática será lograr establecer los requisitos de seguridad del sistema y en él se especifican los controles previstos en cada área o lugar para cumplirlos. También describe las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema y debe reflejar las contribuciones de los distintos actores con responsabilidades sobre el sistema de gestión de seguridad informática.

Tabla XVIII. **Consideraciones generales para la elaboración del plan de seguridad informática**

	Descripción de la consideración
•	El plan de seguridad se considera como el documento de trabajo preventivo, será accesible a todo el personal que demande utilización por lo que la información incluida deberá ser clara y concisa. No se incluirá información limitada o clasificada, la cual, de ser necesario, formará parte del documento independiente que será categorizado conforme a las leyes vigentes del país sobre la seguridad de bienes e información particular.
•	Se deberá ajustar en todo momento al sistema de seguridad diseñado e implementado, evitando formalismos y definiciones conceptuales, utilizando una herramienta de trabajo para la gestión de la seguridad.
•	Su redacción será simple, clara y libre de ambigüedades para que sea de comprensión para todo los involucrados en su cumplimiento.
•	Tendrá carácter impositivo por lo que se podrán evitar diferentes términos que no impliquen obligatoriedad.
•	Contendrá tablas, gráficos y otros complementos que contribuyan a su mejor interpretación.
•	Se deberá actualizar permanentemente sobre la base de los cambios que se produzcan en las condiciones consideradas durante su elaboración.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 43.

3. ESTRUCTURA Y CONTENIDO DEL PLAN DE SEGURIDAD INFORMÁTICA

3.1. Alcance del plan de seguridad informática

El proceso de gestión de la seguridad informática comprende la implementación de controles definidos en el Plan Director de Seguridad de la Información sobre los componentes de la infraestructura tecnológica institucional y otras necesidades que permitan mantener la operación normal y segura de los servicios informáticos institucionales y finaliza con el monitoreo, que permite establecer la correcta y eficiente operación de los controles implementados.

La redacción sobre la propuesta está basada directamente sobre dispositivos destinados a empresas industriales o comerciales, como sensores en aeropuertos o redes de hoteles, ciudades inteligentes, industria que emplea la automatización, ya que en este tipo de IoT normalmente las empresas y clientes tienen los recursos o incentivos para especificar y gestionar las características de seguridad y privacidad de los productos que compran.

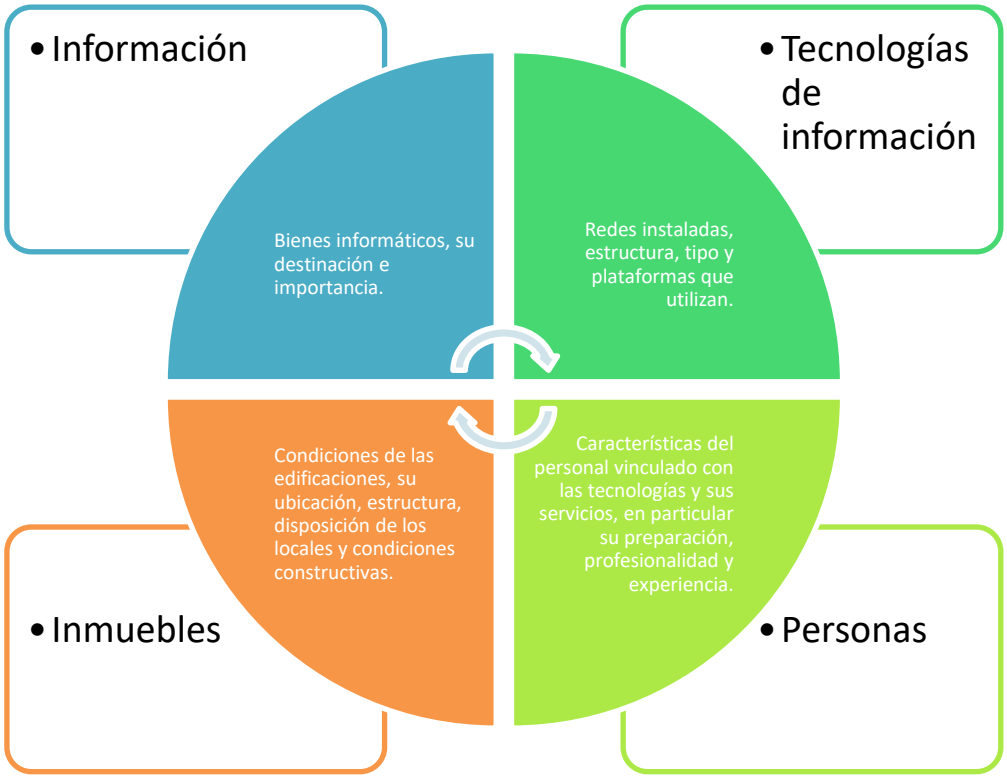
Además, muchos de esos dispositivos emplean conexiones inalámbricas comerciales que no ofrecen acceso completo desde y hacia la internet. Por lo tanto, se espera que el radio de acción del plan este estructurado de acuerdo con el sistema informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el sistema de seguridad.

La importancia de dejar definido claramente el alcance del plan (y de ahí su inclusión al comienzo de este) estriba en que permite tener *a priori* una idea precisa de la extensión y los límites en que tiene vigencia.

3.2. Caracterización del sistema informático

Se deberá describir de forma detallada el sistema informático de la entidad, precisando los elementos que permitan identificar sus particularidades y las de sus principales componentes.

Tabla XIX. **Componentes principales que conforman la caracterización del sistema informático**



Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 45.

Cuando se trata de describir el sistema informático, se podrán emplear esquemas, tablas, gráficos y otros medios auxiliares necesarios con la idea de facilitar la comprensión del lector. Los medios auxiliares podrán ser insertados, dentro de una sección especializada o al final del plan de seguridad.

Se considera que la caracterización del sistema informático permitirá facilitar de forma determinada las necesidades de protección y evitar todo tipo de pérdidas de tiempo e imprecisiones. Su descripción en detalle posibilitará al lector obtener el conocimiento exacto y afinado del plan de seguridad informática, a futuro propone ser de utilidad cuando se produzcan cambio al personal operativo y administrativo.

3.3. Políticas de seguridad informático

Se procede a definir cada uno de los aspectos que podrán conformar la estrategia por seguir por la empresa o corporación sobre la base de sus características, en conformidad con la política vigente en el país en esta materia y el sistema de seguridad diseñado.

También deberán ser incluidas las normas generales que debe cumplir el personal que participa en el sistema informático y se podrán derivar los resultados obtenidos en el análisis de riesgos y del conjunto de definiciones por las instancias superiores en las leyes, resoluciones, reglamentos y otros documentos legales vigentes en la república de Guatemala, acerca de la seguridad informática y sus derivados.

Dentro de estas políticas de seguridad informática se podrán incluir los siguientes aspectos relevantes.

Tabla XX. **Batería de consideraciones importantes para crear políticas de seguridad informática efectiva**

	Ítem selectiva
•	¿Qué tipo de estrategia será adoptada para la gestión de seguridad informática?
•	¿Quién será autorizado para utilizar los bienes informáticos?
•	¿Quién estará a cargo del uso correcto de los recursos?
•	¿Quién estará autorizado para garantizar el acceso y aprobar el uso de los bienes informáticos?
•	¿Quién debe tener los privilegios de administración de los sistemas?
•	¿Cuáles son los derechos y responsabilidades de los usuarios?
•	¿Cuáles son los derechos y responsabilidades de los administradores de sistemas frente a los de los usuarios?
•	¿Qué se deberá hacer con la información clasificada y limitada?
•	¿Qué se deberá hacer ante la ocurrencia de un incidente de seguridad?

Fuente: elaboración propia.

Tabla XXI. **Políticas de seguridad informática básicas en los proyectos futuros**

	Acciones de seguridad propuestas
•	Las propuestas de iniciativas por mejorar el sistema de seguridad informática se aprobarán por el consejo de dirección.
•	El acceso a las tecnologías de la entidad será expresamente aprobado en cada caso y el personal tiene que estar previamente preparado en los aspectos relativos a la seguridad informática.
•	Todos los bienes informáticos serán identificados y controlados físicamente hasta nivel de componentes.

Fuente: elaboración propia.

3.4. Responsabilidades

Cada proyecto que emplea la guía descrita deberá establecer el orden lógico y ordenado del organigrama institucional, donde se describa la estructura organizacional, especificando las atribuciones, funciones y obligaciones de las distintas categorías de personal. Estas deberán incluir los cargos administrativos superiores (jefe de la entidad, jefes de departamentos, áreas y grupos de trabajo o estructuras equivalentes).

Además, en cargos o rangos medios de control de información y asignación de recursos deberán incluirse los jefes, especialistas de informática, administradores de redes, sistemas y aplicaciones, en nivel menor de la escala jerárquica podrán incorporarse los especialistas de seguridad informática y de protección al usuario, en la parte inferior ya se pueden asignar los roles y atributos para los usuarios del sistema y de las tecnologías de información.

Se deberá reconocer que al especificar las atribuciones, funciones y obligaciones del personal en función de sus cargos se tendrá en cuenta lo establecido dentro del propio reglamento de seguridad para las tecnologías de la información, si la empresa o el usuario responsable no cuenta con esta herramienta deberá de desarrollarlo y ejecutar la práctica.

3.5. Medidas y procedimientos de seguridad informáticos

Conforme la estructura y el giro comercial de la empresa o el usuario que implementará el plan de seguridad informática se deberá describir cómo se implementarán en las áreas por proteger, se deberán incorporar cada una de las políticas que han sido definidas para la entidad, en correspondencia con las

necesidades de protección en cada una de ellas, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios.

Se deberán describir por separado cada uno de los controles de seguridad implementados en correspondencia con su naturaleza, combinando el empleo de los medios humanos y de los medios técnicos con las acciones que deben ser realizadas.

Las medidas y procedimientos deberán ser redactadas de forma clara y lógica, evitando que sean confundidas con una declaración de intención o línea de deseos, por lo cual, su descripción se deberá especificar en los controles implementados. El plan de seguridad industrial se fortalecerá sobre la base de los recursos disponibles y en dependencia de los niveles de seguridad alcanzados, también participarán los aspectos que puedan ser cubiertos por el programa de desarrollo de la seguridad informática, que incluya las acciones por realizar por etapas para lograr niveles superiores.

3.5.1. Clasificación y control de los bienes informáticos

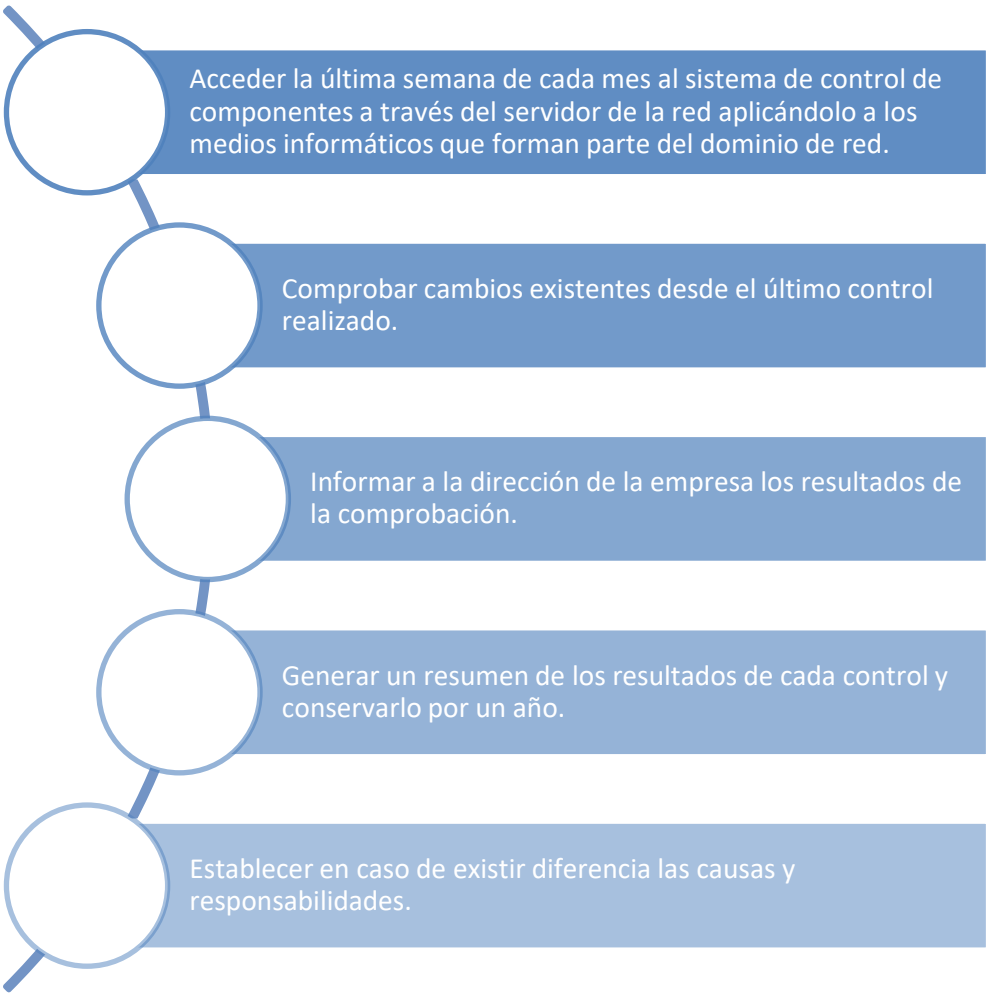
Este conjunto de medidas proyecta identificar los bienes informáticos de acuerdo con su relevancia e importancia, además de controlar y supervisar que sean empleados en funciones propias del trabajo y garantizar su protección.

Tabla XXII. **Medidas de clasificación y control de bienes informáticos**

Tipo de procedimiento
• Precisar los métodos de supervisión y control que se emplearán, el personal responsable de ejecutarlos y los medios empleados para ello.
• Establecer los mecanismos que se requieren para identificar y controlar los bienes informáticos y la conformación de un inventario de estos permanentemente actualizado.
• Precisar la persona encargada de cada bien informático y responsable por su protección.
• Garantizar la autorización y el control sobre el movimiento de los bienes informáticos.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 50.

Figura 23. **Acciones básicas para el control de medios informáticos**



Fuente: elaboración propia.

3.5.2. Sobre el personal disponible

El conjunto de medidas asociadas al personal en conjunto con los procedimientos tiene como objetivo, garantizar el total cumplimiento de las funciones y responsabilidades de seguridad generales y específicas de las personas vinculadas con las tecnologías de la información y sus servicios, así

como la documentación, también deberán asegurar la calidad y confidencialidad de la itinerancia de los datos.

Tabla XXIII. **Conjunto de aseguramientos sobre el personal disponible**

	Conjunto de acciones y actividades programadas
•	La selección adecuada del personal previsto para ocupar cargos en las actividades informáticas o con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas.
•	La obligación de la entidad en cuanto a la preparación del personal y la responsabilidad del trabajador hacia la seguridad informática, así como la inclusión de estos aspectos en los términos y condiciones del contrato de empleo.
•	La forma en que será autorizada por la dirección de la entidad la utilización de las tecnologías y sus servicios por parte de los usuarios que lo necesiten.
•	La obligación de los jefes a cada nivel en cuanto a garantizar la seguridad informática en su área de responsabilidad.
•	Las acciones por realizar en caso de empleo no autorizado de las tecnologías y sus servicios por parte de los usuarios.
•	La responsabilidad de los jefes a cada nivel en cuanto a la preparación de su personal y del conocimiento de sus deberes y derechos, incluyendo la inclusión en el contrato de trabajo de la constancia del compromiso de cada trabajador.
•	Las formas y medios mediante los cuales los usuarios deben informar acerca de cualquier incidente de seguridad, debilidad o amenaza.

.

Fuente: elaboración propia.

3.5.3. Seguridad física y ambiental

Este conjunto de acciones y actividades programadas tiene la función de evitar accesos físicos no autorizados, daños e interferencia contra las instalaciones, las tecnologías y la información de la organización. Se podrá aplicar en locales donde se disponga de tecnologías de información y

directamente de estas mismas tecnologías a los soportes de información, se deberán incorporar los medios físicos, medios técnicos de detección, alarma y el personal que forma parte de las fuerzas especializadas.

La protección que se debe incorporar al equipamiento es altamente necesaria para mitigar y reducir el riesgo de accesos no autorizados a la información y para protegerlo contra pérdidas o daños. Se podrán requerir controles especiales para proteger contra amenazas físicas y para preservar los equipos, tales como la garantía del suministro eléctrico y la infraestructura adecuada del cableado.

Tabla XXIV. **Conjunto de variables tangibles e intangibles a las cuales esta dirigidas las medidas de seguridad física**

	Descripción
•	Protección de las tecnologías contra la sustracción o alteración, incluyendo sus componentes y la información que contiene.
•	Impedir su empleo para cometer acciones malintencionadas o delictivas.
•	Disminuir el impacto producido por fuego, inundación, explosión, perturbación del orden y otras formas de desastre natural o artificial.
•	Protección contra fallas de alimentación u otras anomalías eléctricas.
•	Protección de los cables que transporten datos o apoyen los servicios contra la intercepción o el daño.
•	Garantizar que el equipamiento reciba un mantenimiento adecuado en correspondencia con las especificaciones de las tecnologías.
•	Preservación de la información del equipamiento que cause baja o se destine a otras funciones.

Fuente: elaboración propia.

Al referir las medidas y procedimientos que se establecen para lograr la seguridad física y ambiental adecuada a las necesidades de las tecnologías de la información, no será necesario describir las condiciones constructivas de los inmuebles, ya que eso se deberá realizar durante la caracterización del sistema informático.

Tabla XXV. **Clasificación y medidas básicas para áreas de control**

Área de influencia	**Categoría**	**Medidas específicas**
Dirección, cuadros, seguridad y defensa	Limitada	Acceso físico limitado: cierres seguros en puertas y ventanas, alarma contra intruso.
Economía	Limitada	Acceso físico limitado: control de soportes removibles, alarma contra intrusos, separación de funciones, protección de las copias de programas y datos.
Servidores de la red	Restringida	Acceso solo a administradores: cierre magnético en la puerta de acceso y alarma contra intrusos, redundancia de HW, SW, climatización y datos.
Investigación y desarrollo	Restringida	Acceso físico limitado: cierres seguros en puertas y ventanas, alarma contra intrusos, redundancia de datos.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 54.

3.5.4. Respaldo de la información

Se deberá disponer de procedimientos de respaldo que permitan asegurar la información sensible y esencial, además proteger el software para que pueda recuperarse tras algún siniestro o desastre.

Tabla XXVI. **Conjunto de elementos básicos que permitirán disponer del respaldo hacia la información**

	Acción por definir
•	Definir el nivel necesario de información de respaldo.
•	Realizar copias seguras y completas de la información, establecer los procedimientos de restauración.
•	Determinar el grado (completo / parcial) y la frecuencia de los respaldos en correspondencia con los requisitos de la entidad, los requisitos de seguridad de la información implicada, y la importancia de la información que permita la operación continúa de la organización.
•	Precisar las copias que deben ser almacenadas en un área apartada del lugar habitual de procesamiento de la información que se preserva, a una suficiente distancia para la salvaguarda de cualquier daño producto de un desastre en el sitio principal.
•	Establecer un nivel apropiado de protección ambiental y físico de la información de respaldo consistente con las normas aplicadas al sitio principal. Los controles aplicados a los soportes en el sitio principal se extenderán para cubrir el sitio de respaldo.
•	Probar regularmente los soportes de respaldo para verificar que puede confiarse en ellos para el uso cuando sean necesarios.
•	Comprobar de forma regular los procedimientos de restauración para lograr asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos de recuperación.
•	Proteger los respaldos por medio del cifrado en los casos que sea requerido.

Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 64.

Cuando se analizan los sistemas críticos, las disposiciones de respaldo cubrirán la información y los datos para recuperar el sistema completo en un posible evento o siniestro de ruptura de datos. Las respuestas de respaldo, cuando sea posible, se podrán automatizar, esto permitirá facilitar el respaldo y los procesos de restauración. Las futuras soluciones en formato de automatización deberán ser puestas a prueba suficientemente antes de la ejecución en la práctica y en intervalos regulares.

3.6. Lista nominal de usuarios con acceso a los servicios de red

Se deberá habilitar un listado oficial de los usuarios debidamente autorizados por cada servicio, especificando diferentes campos obligatorios, además los servicios para los que tiene autorizado el acceso dentro de la empresa.

Tabla XXVII. **Matriz de variables que deberán asignarse para cada usuario autorizado**

	Variables de interés	
•	Nombre completo.	Formará parte de la base de datos interna de la empresa.
•	Apellido (de casada si amerita).	
•	Número de documento de identificación personal.	Además, se puede incluir el número de antigüedad del personal.
•	Cargo que ocupa dentro de la empresa.	Descripción y nombre de la plaza ocupada.
•	Servicios autorizados.	Conjunto de atributos asignados.
•	Permisos especiales asignados.	Áreas digitales a las cuales podría tener acceso.

Fuente: elaboración propia.

4. ¿QUÉ ES INTERNET DE LAS COSAS?

4.1. Protocolos eficientes de comunicación

El internet de las cosas (IoT) ha tomado mucha fuerza, convirtiéndose en una de las tecnologías más impactantes en los últimos años. Ofrece gran variedad de posibilidades dentro de la industria tecnológica por su capacidad de conectar objetos a la red de redes y poder acceder a estos en cualquier lugar, siempre que se cuente con conexión a internet.

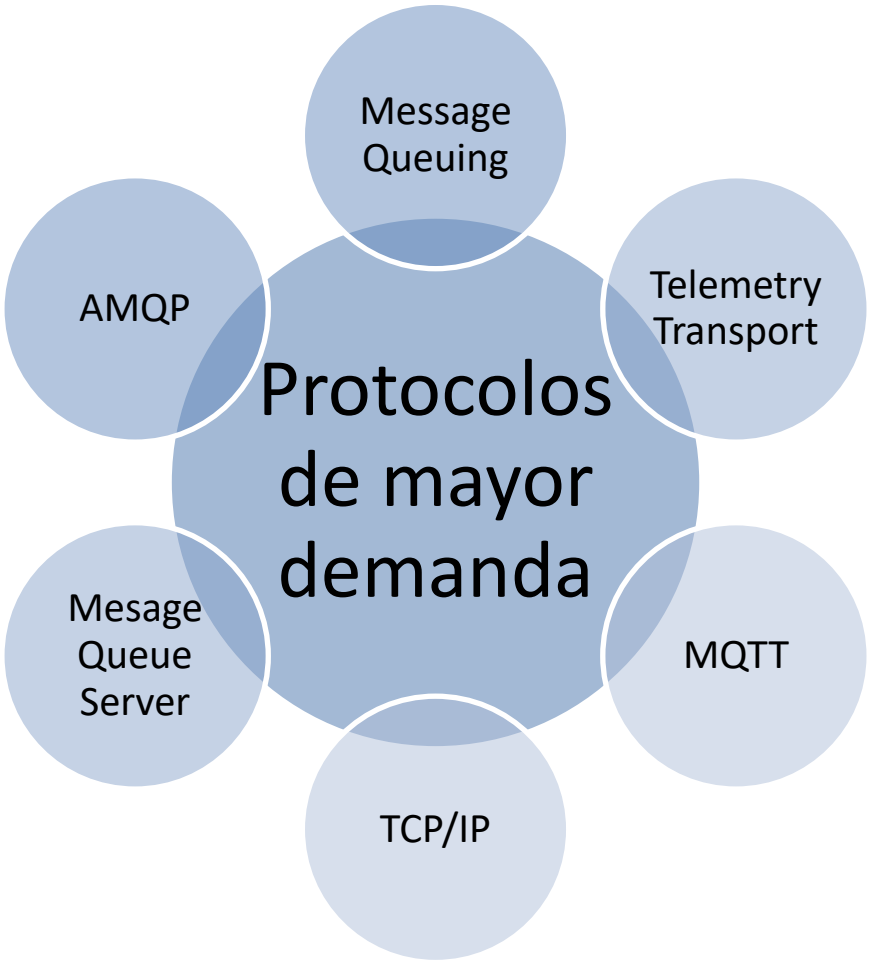
A pesar de los grandes beneficios que ofrece la tecnología IoT, tiene debilidades, esto debido a que los fabricantes de dispositivos IoT centraron sus esfuerzos en desarrollar componentes para que objetos comunes se pudieran conectar a internet sin haber tenido en cuenta en su momento la seguridad. Lo anterior, llevó a que objetos conectados a internet queden expuestos, permitiendo que se usarán como medio para que los ciberdelincuentes realicen ataques informáticos, ocasionando que se afecten muchos sectores empresariales.

Algunas de las plataformas de software y hardware de dispositivos IoT no cuentan con las medidas de seguridad apropiadas, esto es porque muchos de sus fabricantes dejan de brindarle soporte o simplemente no cuentan con módulos de seguridad para protección de la información que circulan a través de estos dispositivos.

Para las conexiones inalámbricas, existen diferentes opciones. Por lo cual el método de transferencia deberá ser seleccionado en función de la distancia de

transferencia necesaria, se conoce que la demanda real esta actuada por conexiones inalámbricas de corto alcance, medio alcance y largo alcance. El rango físico suele ser desde pocos metros hasta 100 metros, otro factor relevante es emplear bajo consumo de energía.

Figura 24. **Protocolos de mayor demanda para las IoT**



Fuente: GALLARDO MONTES, Francisco. *Seguridad en internet de las cosas*. p. 17.

4.2. Modelos aplicados al internet de las cosas

Parte integral en los modelos arquitectónicos de IoT es el Big Data y el conjunto de aplicaciones analíticas. En la actualidad existen demandas sobre diferentes proveedores que ofrecen aplicaciones para gestionar y administrar cantidades volumétricas de datos. Las plataformas deben determinar la gestión y el análisis de los datos. Las plataformas existen proveedoras de servicios digitales permiten gestionar los análisis de datos en tiempo real, así permite interconectar tecnologías entre sí.

Los datos generados por el conjunto de dispositivos IoT es de alta demanda, para ese conjunto de estadísticas no se descartan los datos generados por un sensor o una cámara de vigilancia, se hacen parte de esa muestra los dispositivos de Hardware IoT. La cantidad de datos puede ser insuficiente hasta que sea analizada y adaptada de tal manera que las personas puedan interpretarla. En la peor experiencia técnica, los datos generados del sensor son solo un texto básico de Ascii sin ningún formato.

El propósito y uso de la aplicación Big Data es apoyar los diferentes análisis a comprender sobre los datos recolectados, lo más importante, es la relevancia de los datos almacenados y analizados. El papel clave con que se emplean las herramientas Big Data es también la capacidad de almacenar los datos y mantenerlos seguros.

4.2.1. Modelo TCP

Con el desarrollo exponencial de los canales de comunicación e itinerancia de datos se permite robustecer el modelo TCP (*Transmition Control Protocol*) estableciendo en el medio social y digital como la plataforma estandarizada que

permite establecer la comunicación de red a través de la cual los diferentes programas de aplicación logran intercambiar datos. Esto se logra por medio de otro protocolo suplementario (Internet Protocol IP), por el cual se muestra la ruta lógica de cómo las computadoras realizan el intercambio de datos de forma bidireccional o unidireccional.

Por medio del protocolo TCP también se plantea de forma ordenada la secuencia empleada para lograr intercambiar datos a través del IoT, proporcionando los sistemas de comunicación de extremo a extremo que permiten identificar cómo se deben dividir los paquetes de datos, el sentido de envío, enrutamiento y el punto de anclaje de destino final, una ventaja del TCP es que demanda muy poca administración central, su diseño robusto permite que sus redes sean fiables y seguras. Además, otra capacidad sustancial que permite recuperarse automáticamente de la falta de cualquier dispositivo en la red.

Figura 25. **Fortalezas del TCP**

Fuente: elaboración propia.

4.2.2. Modelo IP

La plataforma original propuso un modelo sostenible y funcional con expansión según la demanda de los usuarios, su plataforma de expansión se vio aprovechada por medio de la globalización, la lucha intrínseca de sus pioneros se sustentó en la robusta arquitectura de sus servicios modelos y propuestos.

El modelo IP o protocolo de internet, emplea direcciones series de cuatro octetos con formato de punto decimal (como por ejemplo 75.4.160.25). Este protocolo lleva los datos a otras máquinas de la red.

Además, el modelo IP permite intercambio de datos fiable dentro de una red, definiendo los pasos a seguir desde que se envían los datos (en paquetes) hasta que son recibidos. Para lograrlo emplea un sistema de capas con jerarquías (se construye una capa a continuación de la anterior) que se comunican únicamente con su capa superior (a la que envía resultados) y su capa inferior (a la que solicita servicios).

Tabla XXVIII. **Capas del modelo IP**

Clasificación	Contenido o formulación
Nivel de enlace o acceso a la red	Primera capa dentro del modelo IP, logra ofrecer la posibilidad del acceso físico a la red el cual puede ser en anillo, ethernet o similares. A través de este modelo se especifican el modo en que los datos deberán enrutarse independientemente del tipo de red empleado.
Nivel de red o internet	Dentro de este nivel se proporciona el paquete de datos, también se reconocen como datagramas, su función es administrar las direcciones IP. Los denominados datagramas son conjunto de paquetes de datos que constituyen el mínimo de información requerido en una red. Acá también es donde se engloban los protocolos IP, ARP, ICMP, IGMP y RARP.
Nivel de transporte	Permiten conocer el estado de la transmisión, así como los datos de enrutamiento y utilizan los puertos para asociar un tipo de aplicación con un tipo de dato.
Nivel de aplicación	Se reconoce como la parte superior del protocolo IP, esta capa suministra las aplicaciones de red tipo TELNET, FTP O SMTP, estas se comunican con las capas inferiores o también conocidas como anteriores de tipo TCP o UDP.

Fuente: ROBLEDANO. Ángel. *Qué es TCP/IP*. https://openwebinars.net/blog/que-es-tcpip/. Consulta: junio de 2020.

4.2.3. Capa física

Parte esencial del IoT es donde se logra especificar los parámetros mecánicos, eléctricos de las conexiones físicas. Las unidades de información que se consideraron fueron nombradas como bits dentro del canal de comunicación, cuando el emisor envía un 0 al receptor deberá llegar un 0.

La capa de enlace es la que define la conexión segura entre dos dispositivos, de forma que no se pierdan los datos cuando se presentan múltiples dispositivos compartiendo el mismo medio, esto es conocido como un consenso entre qué medio puede hacer uso del medio física en cada momento. Se logra realizar descomponiendo los mensajes que son recibidos del nivel superior en bloques de información, a las cuales añade la cabecera (DH) e información redundante para control de errores.

Esta cabecera agregada (DH) contiene información de direcciones sobre el origen y el destino, la ruta que deberá seguir el paquete de datos, también es la responsable de transmitir sin error de comunicación los paquetes de datos de cada enlace que conectará directamente dos puntos físicos adyacentes de la red y desconectar el enlace de datos sin pérdidas de información.

Figura 26. **Elementos complementarios de la capa física**

Parámetros mecánicos	**Parámetros eléctricos**	**Elementos de comunicación**
Grosor de los cables	Temporizador de señales	Pares trenzados de cable
Tipo de conectores	Niveles de tensión	Cable coaxial
		Radio
		Infrarrojos
		Fibra óptica

Fuente: GONZÁLEZ, Jesús. *IoT: dispositivos, tecnologías de transporte y aplicaciones*. p. 16.

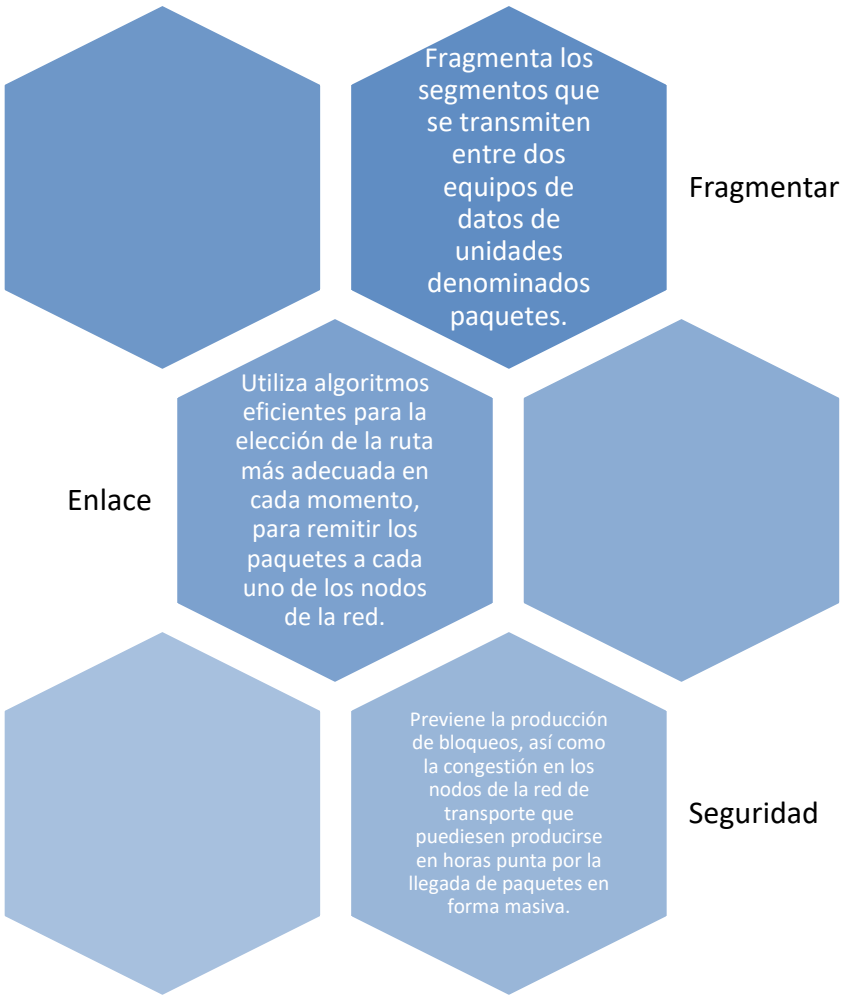
4.2.4. Capa de red

Luego de sustentar y establecer la capa física con su perfecta conectividad, se procederá a establecer y configurar el protocolo de comunicación de la red, con un método único que permita diferencia los dispositivos que operan en su

propio rango. Por medio de este enlace se establecerá la dirección de red la cual presenta una función principal de identificar a cada dispositivo conectado al mismo enrutador, muy similar a la selección, control y reconocimiento del ID.

La IP, especialmente IPv6 están diseñadas para el IoT de hoy en día con el uso de ordenadores personales, portátiles y servidores conectados por cable. Pero las restricciones cada vez más exigentes sobre los dispositivos de los sistemas de IoT, hacen que las características de los protocolos actuales no se logren adecuar a las necesidades específicas de estos propios dispositivos, porque es necesario impulsar el desarrollo de nuevos modelos o adaptación hacia los ya existentes.

Figura 27. **Funciones de la capa de red**



Fuente: GONZÁLEZ. Jesús. *IoT: dispositivos, tecnologías de transporte y aplicaciones*. p. 21.

4.3. Tecnología robusta para comunicaciones inalámbricas

Las tecnologías LPWA (*Low Power Wide Area Network*) fueron diseñadas para disponer de áreas extensas de cobertura y excelencia propagación de la señal, difícil de conseguir en entornos de interior. Para permitir a los dispositivos conectarse a las estaciones base a distancias comprendidas entre unos pocos

metros y decenas de km, para eso es necesario obtener ganancia de 20dB por encima de los sistemas de telefonía móvil.

Para obtener ese objetivo se deberá emplear un espectro por debajo de la banda de 1 GHz y modulaciones especiales. La mayoría de las tecnologías LPWA emplean la banda por debajo de 1 GHz (sub-1GHz) ya que permite mejorar la comunicación y además de proporcionar seguridad con bajos consumos de energía. Todo esto comparado con la banda de 2,4 GHz, donde las señales de baja frecuencia sufren menor atenuación y efectos multipath, además de presentarse menos congestionadas.

Las tecnologías LPWA empleadas actualmente, fueron diseñadas para conseguir alcances de 150 ±10 dB que permiten alcanzar distancias entre puntos que van desde pocos hasta decenas de kilómetros en entornos urbanos y áreas rurales. El nivel físico se compromete con la velocidad de los datos disminuyendo la velocidad de modulación, para lograr mayor energía en cada bit transmitido. De esa forma los receptores podrán decodificar señales correctamente, aunque se encuentren atenuados.

4.3.1. Tipos de redes

En el ámbito digital, donde las demandas del consumidor hacia la IoT presentan redes de área personal, su capacidad inalámbrica dispone de conexión estable y segura, cubre rangos aproximadamente de 10 metros de radio. Empleando un dispositivo PAN con tecnología inalámbrica, comúnmente llamados Smartphone el cual se conecta a través del protocolo Bluetooth con una gama de accesorios. Estos dispositivos Pan son de baja impedancia de transmisión, otra característica muy versátil es lograr que operen en condiciones ideales solamente empleando baterías de baja potencia.

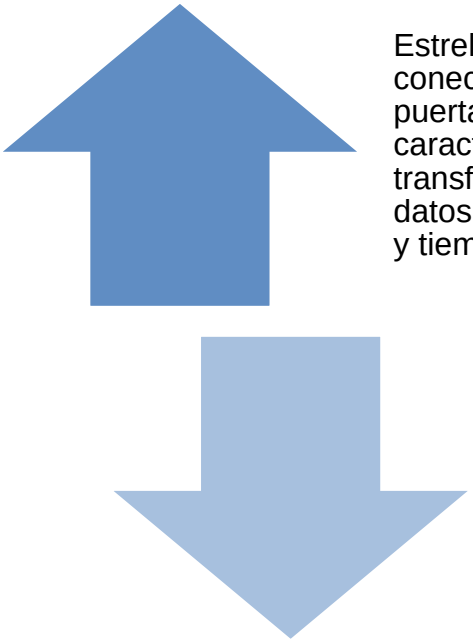
Con un mapeo de cables y selección inalámbrica se forma la red de área local, se puede trabajar con la combinación de las dos variantes. Acá predomina LAN (*Local Area Network*) su arquitectura cumplirá los lineamientos y requerimientos a detalle del usuario o la empresa contractual, su rango efectivo está por debajo de los 100 metros de radio, en la sociedad común este tipo de red es llamada wifi

Otro conjunto de redes en áreas locales o comúnmente localizados en vecindarios, poseen alta capacidad de comunicación inalámbrica donde su radio efectivo para itinerancia de datos está en 25 kilómetros aproximadamente. Emplean altos niveles de potencia, su transferencia de bloques de datos es baja para la alta demanda.

4.3.2. Topologías de redes

Cuando se expresa la idea del protocolo o arquitectura de la red, se entenderá sobre la propia jerarquía donde se envían los mensajes a un servidor central empleando *gateways*. Su tasa de transmisión puede oscilar de 300 bps hasta 50 Kbps empleando agregación de canales.

Figura 28. **Topología de red estrella y malla**



Estrella: todos los nodos se encuentran conectados a uno central, suele ser la puerta de entrada a Internet. Su característica principal es permitir la transferencia de grandes bloques de datos, velocidad de interconexión rápida y tiempos de respuesta muy cortos.

Malla: cada nodo se encuentra conectado entre sí. Dado que el proceso de comunicación es un gran número de pequeños saltos, la velocidad de comunicación dentro y fuera de la red de malla local es relativamente lenta. Requiere mayor complejidad para ser diseñada.

Fuente: elaboración propia.

4.3.3. Estándares de interoperabilidad

Existen diferentes retos dentro del uso de comunicación, los dispositivos, sensores, redes y el conjunto de aplicaciones para IoT se reconoce como la capacidad de entender y conectarse entre sí. En el medio digital, tanto en Latinoamérica como en otros continentes predominan las alianzas estratégicas para desarrollar en mesas técnicas los modelos eficientes que brinden el respaldo protocolario entre la comunicación de un usuario hacia un banco de datos.

Avances recientes se presentan por el Instituto de Ingenieros Eléctricos y Electrónicos, mejorando los estándares en 802.x 802.3 especializado en Ethernet, estos protocolos son empleados en redes de computadoras cableadas,

también se mejoran la conectividad LAN 802.11 inalámbrica, PAN que mejora el estándar de especificación en 802.15.4 empleado en ZigBee y 6LoWPAN.

4.3.4. Protocolos inalámbricos

Para las conexiones inalámbricas existen múltiples opciones. Donde el método de transferencia utilizado deberá seleccionarse en función de la distancia de transferencia necesaria, ya que se disponen de diferentes categorías, se pueden emplear conexiones inalámbricas de corto alcance, medio alcance y largo alcance. Ejemplos de corto alcance Bluetooth, Z-Wave y ZigBee. La razón de emplear método de bajo alcance es que estos dispositivos de IoT se emplean como dispositivos de red de área personal y solo necesitan velocidad de transferencia de datos de corto alcance y baja latencia.

Con métodos de transferencia inalámbrica de rango medio, el bajo consumo de energía también es una característica importante. La tasa de datos también podría ser baja. Los de mayor demanda o comúnmente empleados son HaLow, 802.11ah (IEEE 801.11ah 2018) y LTE Advanced.

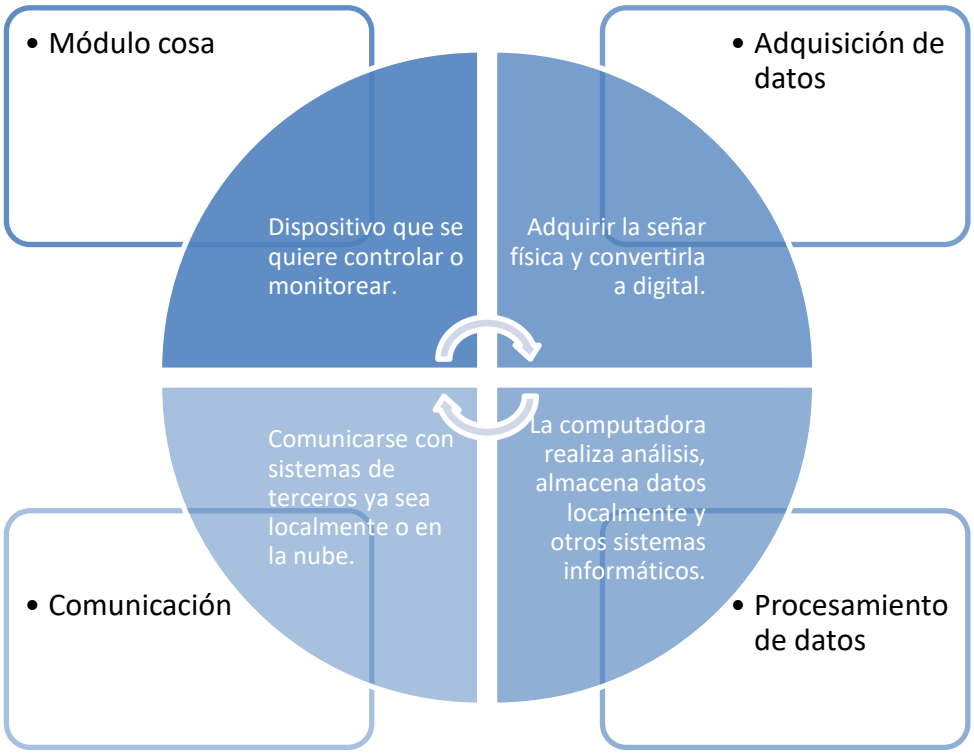
El método más común de transporte hoy en día es la red móvil 4G, proporciona un modelo eficaz para transmitir datos a alta velocidad y la cantidad de datos también puede ser muy elevado. Los protocolos mayormente empleados con dispositivos IoT son Message, Queuing, Telemetry Transport, MQTT, que funciona sobre el protocolo TCP/IP. El beneficio con MQTT es ser muy ligero y por lo tanto adecuado para aplicaciones IoT.

Otro protocolo que presenta demanda continua es el protocolo Avanzado de Message Queue Server, AMQP, este se basa en estándar abierto y su objetivo principal es transmitir mensajes comerciales entre aplicaciones.

4.4. Hardware en un sistema de internet de las cosas

Es aquel conformado por dispositivos para un panel de control remoto, dispositivos para control, servidores, un dispositivo de enrutamiento o puente y sensores. Estos dispositivos administran tareas y funciones clave, como la activación del sistema, las especificaciones de acción, la seguridad, la comunicación y la detección para cumplir con objetivos y acciones específicas.

Figura 29. **Diferentes módulos que complementan sistema de IoT**



Fuente: elaboración propia.

4.5. Formato de datos

El lenguaje o arquitectura desarrollada que se emplea para obtener las plataformas digitales varía según su campo de aplicación y alcance esperado, por lo cual es un conjunto finito de modelos presentes.

Tabla XXIX. **Formatos de datos**

	Tipo	Descripción
WEB	HyperText Markup Language HTML	Consiste en una serie de códigos cortos escritos por el autor del sitio en un archivo de texto: estas son las etiquetas. Luego, el texto se guarda como un archivo html y se visualiza a través de un navegador, como Internet Explorer o Netscape Navigator. Este navegador lee el archivo y traduce el texto a una forma visible, con la esperanza de representar la página como el autor había querido. Escribir un HTML implica usar etiquetas correctamente para crear la visión. Se puede utilizar cualquier editor para redactarlo, desde un editor de texto rudimentario hasta un editor gráfico potente para crear páginas HTML.
	Extensible Markup Language XML	Se utiliza para describir datos. El estándar XML es una forma flexible de crear formatos de información y compartir electrónicamente datos estructurados a través de la Internet pública, así como a través de redes corporativas. El código XML, una recomendación formal del World Wide Web Consortium (W3C), es similar al lenguaje de marcado de hipertexto (HTML). Tanto XML como HTML contienen símbolos de marcado para describir el contenido de la página o el archivo. El código HTML describe el contenido de la página web (principalmente texto e imágenes gráficas) solo en términos de cómo se debe mostrar e interactuar. El componente básico de un documento XML es un elemento definido por etiquetas, que tiene un comienzo y una etiqueta final. Todos los elementos en un documento XML están contenidos en un elemento más externo conocido como el elemento raíz. XML también puede soportar elementos anidados, o elementos dentro de elementos. Esta capacidad permite que XML soporte estructuras jerárquicas. Los nombres de los elementos describen el contenido del elemento y la estructura describe la relación entre los elementos.

Continuación de la tabla XXIX.

	JavaScript Object Notation JSON	Es un formato ligero de intercambio de datos. Es fácil de leer y escribir para los humanos; las máquinas, es fácil de analizar y generar. Se basa en un subconjunto del lenguaje de programación de JavaScript. JSON es un formato de texto que es completamente independiente del lenguaje, pero utiliza convenciones que son familiares para los programadores de la familia C de lenguajes, incluida la C, C ++, C #, Java, JavaScript, Perl, Python y muchos otros. Estas propiedades hacen de JSON un lenguaje ideal para el intercambio de datos.
Formatos en IoT	JSON	La mayoría de los protocolos de IoT utilizan TCP / IP como mecanismo de transporte. Es un protocolo basado en flujo que no incluye ninguna información de trama cuando se utiliza para enviar mensajes a través del cable. Los protocolos IoT agregan información de trama sobre TCP / IP cuando se transmiten datos, lo que facilita el envío de paquetes a través del cable. Por ejemplo, el protocolo WebSocket agrega un encabezado de tamaño a los datos, y una pila WebSocket proporciona una API basada en paquetes para el diseñador de la aplicación que usa la pila. Los protocolos de publicación / suscripción, como MQTT y SMQ, también proporcionan una API basada en paquetes. Como los protocolos de IoT proporcionan una API basada en paquetes, cualquier codificador / decodificador JSON se puede usar para serializar y deserializar los datos estructurados enviados a través del cable. Sin embargo, en algunos casos, un protocolo IoT es una exageración que puede agregar memoria innecesaria y sobrecarga de procesamiento. Un diseñador de productos de IoT puede elegir utilizar directamente TCP / IP como la capa de transporte para enviar datos estructurados a través del cable. No se puede utilizar un codificador / decodificador JSON estándar cuando se utiliza una capa de transporte no basada en tramas.

Continuación de la tabla XXIX.

	Concise Binary Representation	La representación concisa de objetos binarios es un formato de serialización de datos binarios basado libremente en JSON. Al igual que JSON, permite la transmisión de objetos de datos que contienen pares nombre-valor, pero de una manera más concisa. Esto aumenta el procesamiento y las velocidades de transferencia a costa de la legibilidad humana. Otros usos, es la capa de serialización de datos recomendada para el conjunto de protocolos CoAP Internet of Things y el formato de datos en el que se basan los mensajes COSE.
	Tensor Flow	La versión 1.0.0 se lanzó el 11 de febrero de 2017. Mientras que la implementación de referencia se ejecuta en dispositivos individuales, TensorFlow puede ejecutarse en múltiples CPU y GPU (con las extensiones opcionales CUDA y SYCL para computación de propósito general en unidades de procesamiento de gráficos). TensorFlow está disponible en Linux, macOS, Windows y plataformas de computación móviles de 64 bits, incluyendo Android e iOS. Su arquitectura flexible permite el fácil despliegue de cómputo en una variedad de plataformas (CPU, GPU, TPU), y desde computadoras de escritorio hasta clústeres de servidores a dispositivos móviles y de vanguardia. Los cálculos de TensorFlow se expresan como gráficos de flujo de datos con estado. El nombre TensorFlow deriva de las operaciones que realizan dichas redes neuronales en matrices de datos multidimensionales, que se denominan tensores. Durante la Conferencia de Google I / O en junio de 2016, Jeff Dean declaró que 1,500 repositorios en GitHub mencionaron TensorFlow, de los cuales solo 5 eran de Google.

Fuente: elaboración propia.

4.6. Herramientas empleadas de mayor demanda en internet de las cosas

Su principio se sustenta en el Tensor Flow, los cálculos que pueden ser expresados como gráficos también involucran modelos predictivos de construcción, producción y experimentación, todo relacionado con la investigación, la mejora continua sobre la base arquitectónica en el desarrollo del IoT.

Tabla XXX. **Herramientas principales para trabajar las IoT**

Herramienta	Descripción
Construcción fácil.	TensorFlow ofrece múltiples niveles de abstracción. Permite crear y entrenar modelos utilizando la API de alto nivel de Keras, que facilita el inicio de TensorFlow y el aprendizaje automático.
Producción de ML.	Ya sea en servidores, dispositivos perimetrales o en la web, TensorFlow permite capacitar e implementar un modelo fácilmente, sin importar qué idioma o plataforma se use. Se usa TensorFlow Extended (TFX) si se necesita un ducto ML de producción total. Para ejecutar inferencia en dispositivos móviles y de borde, se emplea TensorFlow Lite. Se puede entrenar y despliegan modelos en entornos de JavaScript utilizando TensorFlow.js.
Experimentación para la investigación.	Permite crear y entrenar modelos de última generación sin sacrificar la velocidad ni el rendimiento. Brinda la flexibilidad y el control con funciones como la API funcional de Keras y la API de subclasificación de modelos para la creación de topologías complejas. Para una creación de prototipos fácil y una depuración rápida, se usa la ejecución. TensorFlow también es compatible con un ecosistema de potentes bibliotecas y modelos complementarios para experimentar, incluidos los Tensors Ragged, TensorFlow Probability, Tensor2Tensor y BERT.

Fuente: elaboración propia.

CONCLUSIONES

1. Tensor Flow establece resguardar los bienes informáticos del usuario, además de la relación existente del intercambio de datos entre hardware y software, empleando modelos seguros y sistemas de protección, verificación y control.

2. Por medio de puntos de red que permitan controlar los dispositivos mediante una consola central, permitirá disminuir los riesgos de amenaza ante la vulneración en la itinerancia de los paquetes de datos transmitidos.

3. Se pueden emplear dispositivos de gama media-baja, pero con la poca fiabilidad de que sean eficientes, la relevancia e importancia de la información, servicio o datos que se desea asegurar propondrá el costo de inversión.

4. El conjunto de reglas básicas propuestas para formular la arquitectura interna de los usuarios dentro de la red o base de datos permitirá que alguna amenaza externa sea detectada inmediatamente, además de que los usuarios debidamente registrados estarán condicionados sobre la toma de decisiones en cada una de las etapas desarrolladas de la guía del plan de seguridad informática.

5. La seguridad informática podría verse comprometida si no se incorporan las acciones propuestas, además de las estructuras básicas para trabajar por medio de Arduino o un medio parecido.

6. El conjunto de información incorporada sobre el desarrollo de lenguaje informático, medios y canales de comunicación, trasladar de 0 a 1, son parte complementaria del IoT.

RECOMENDACIONES

1. Comprometer al futuro profesional de IoT que pueda emplear la presente guía de alternativas con el uso de las herramientas desarrolladas para proteger los bienes informáticos del proyecto deseado.

2. Adquirir dispositivos electrónicos aptos para el desarrollo de una red de infraestructura robusta por la demanda constante en transferencia de datos, los cuales posean protocolos internos de seguridad por el fabricante para garantizar la confidencialidad de los datos de los usuarios.

3. Emplear modelos seguros de obtención de datos para los usuarios, podrá mediar el umbral de acceso a los puntos de red, sin el control maestro y restricción de atributos para cierto personal no de confianza o no necesario, podría permitir vulnerabilidades al sistema.

4. Impulsar los ajustes aportados y que puedan ser incorporados al plan de seguridad informática, los equipos son demandados hasta su nivel máximo en las temporadas de lluvia y frío en nuestro país, exigiendo el doble de su capacidad de trabajo, esto se refleja con los paros innecesarios y fallas repentinas.

5. Monitorear conjunto de atributos y las bases de diseño empleadas para loT ya que estas variables comprometen la seguridad informática, además de comprar equipos robustos que representan al usuario

garantía en la certeza de impenetrabilidad, harán un modelo eficiente y sustentable.

BIBLIOGRAFÍA

1. CASSIMALLY, Hakim. *Designed Internet of Things*. Inglaterra: John Willey and Sons, 2014. 338 p.

2. CNEE. *Normas técnicas de diseño y operación de las instalaciones de distribución*. Guatemala: MEM, 1999. 52 p.

3. CONDUMEX. *Manual técnico de instalaciones eléctricas en baja tensión*. 5a ed. México: Servicios Condumex, S.A., 2009. 289 p.

4. DORF, Richard. *Circuitos eléctricos*. 8ª ed. México: Alfaomega, 2011. 908 p.

5. GARCÍA, Néstor. *Potencia en circuitos monofásicos*. [en línea]. <https://es.slideshare.net/NUVILDE/potencia-elctrica-monofsica>. [Consulta: junio de 2020].

6. GALLARDO MONTES, Francisco. *Seguridad en internet de las cosas*. España: Universitat Oberta de Catalunya, 2019. 66 p.

7. GONZÁLEZ. Jesús. *IoT: dispositivos, tecnologías de transporte y aplicaciones.* España: Universidad de Cataluña, 2017. 73 p.

8. HARRINGTON, James. *Metodología para la elaboración del plan de seguridad informática*. Ecuador: Ejército Ecuatoriano, 1996. 118 p.

9. LÓPEZ, Ricardo. *Sistema de gestión de la seguridad informática*. [en línea]. <https://core.ac.uk/download/pdf/326424017.pdf>. [Consulta: junio de 2020].

10. MALLEY, Jhon. *Análisis de circuitos eléctricos*. New York: McGraw-Hill, 2011. 432 p.

11. MORALES, Andrés. *Mecanismos de seguridad en el Internet de las cosas*. Colombia: Universidad Distrital Francisco José de Caldas, 2019. 110 p.

12. Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. Cuba: Redacción Canal Caribe, 2017. 68 p.

13. ROBLEDANO. Ángel. *Qué es TCP/IP*. [en línea]. <https://openwebinars.net/blog/que-es-tcpip/>. [Consulta: junio de 2020].

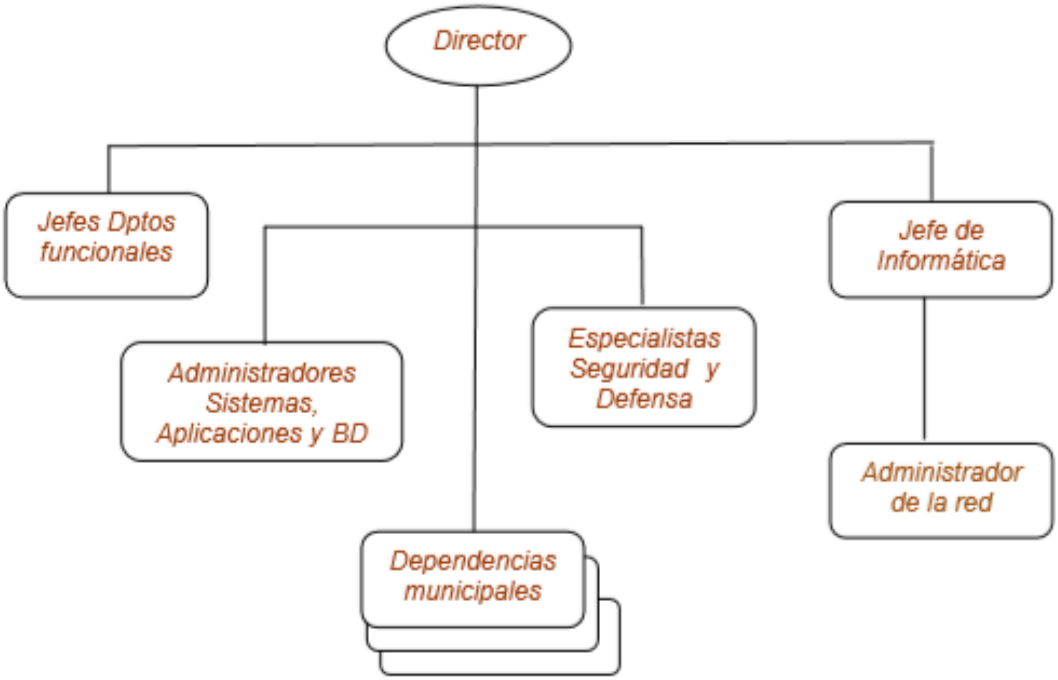
14. ROMERO, Martha. *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*. España: Área de innovación y Desarrollo, S.L., 2018. 124 p.

15. Superintendencia de Bancos. *Gestión de seguridad informática*. [en línea]. <https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2018/04/13.3.3_manual.pdf>. [Consulta: junio de 2020].

16. UCHA, Florencia. *Definiciones*. [en línea]. <https://www.definicionabc.com/tecnologia/carga-electrica.php>. [Consulta: junio de 2020].

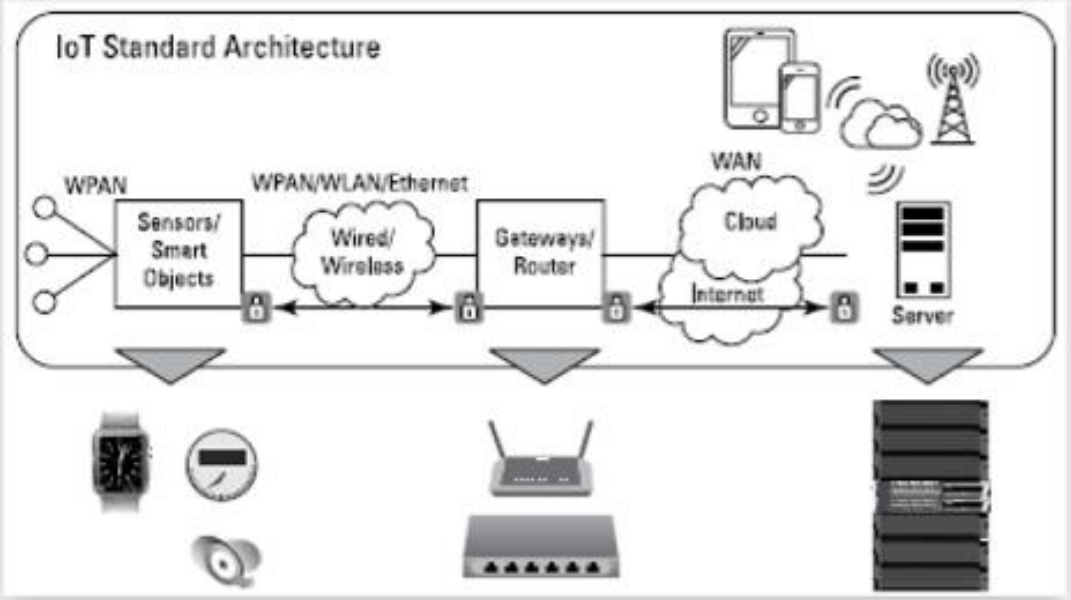
ANEXOS

Anexo 1. **Estructura de gestión de la seguridad informática de la empresa X**



Fuente: Oficina de seguridad para las redes informáticas. *Metodología para la gestión de la seguridad informática*. p. 49.

Anexo 2. **Arquitectura estándar IoT**



Fuente: GALLARDO MONTES, Francisco. *Seguridad en internet de las cosas*. p. 15.