UNIVERSIDAD PRIVADA TELESUP

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

TESIS

SISTEMA DE DETECCIÓN DE INCENDIOS Y LA RELACIÓN CON LA OPTIMIZACIÓN DE LA DATA CENTER EN LAS MUNICIPALIDADES DE LIMA METROPOLITANA, 2020.

PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE ELECTRÓNICA Y TELECOMUNICACIONES

AUTORES:
Bach. RUTTI CANCHANYA, JHONATAN
Bach. AREVALO CAMPOS, FERNANDO JOSE

LIMA – PERÚ

2022

ASESOR DE TESIS

_____

Mg. RAÚL GUALBERTO QUISPE TAYA

JURADO EXAMINADOR

_____

Dr. JUAN ANTENOR CACEDA CORILLOCLLA
Presidente

_____

Mg. DANIEL VICTOR SURCO SALINAS
Secretario

_____

Mg. JAIME GABINO JAUREGUI DEL ÁGUILA
Vocal

DEDICATORIA

A nuestros padres, que retaron a la vida por nosotros.

A nuestros hijos, que hicieron de nuestras vidas, un reto.

AGRADECIMIENTO

A la Universidad Privada Telesup por habernos dado la oportunidad de realizar el presente informe.

RESUMEN

La investigación titulada: “Sistema de detección de incendios y la relación con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020”, tuvo como objetivo establecer la relación entre el sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020. En cuanto a la metodología, se ha considerado un enfoque cuantitativo, diseño no experimental de corte transversal y de alcance correlacional. Se aplicó la técnica de encuesta y el instrumento de un cuestionario de 20 preguntas tipo Likert, la muestra estuvo constituida por 43 Gerencias de Tecnologías de Información de las Municipalidades distritales de Lima Metropolitana.

Los resultados obtenidos fueron analizados en el nivel descriptivo y en el nivel inferencial según los objetivos y las hipótesis formuladas, efectivamente el diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020; donde, los resultados demuestran que el 48,8% respondieron que la mayoría de veces si tienen conocimiento de dicho sistema de detección de incendios implementadas en las áreas o departamentos de las gerencias tecnológicas; asimismo, el 60,5 % indicaron que siempre tienen conocimiento para la optimización de la data center en la toma de decisiones al disponer de información las Gerencias de Tecnologías de Información de las municipalidades distritales de Lima Metropolitana.

Palabras clave: Diseño del sistema de detección de incendios y la data center.

ABSTRACT

The research, entitled: Fire detection system and the relationship with data center optimization in the municipalities of Metropolitan Lima, 2020, aimed to establish the relationship between the fire detection system and the optimization of the data center in the municipalities of Metropolitan Lima, 2020. Regarding the methodology, a quantitative approach has been considered, a nonexperimental design of cross-sectional and correlational scope. We applied the survey technique and the instrument of a questionnaire of 20 Likert type questions, the sample was constituted by 43 Information Technology Managers of the district municipalities of Metropolitan Lima.

The results obtained were analyzed at the descriptive level and at the inferential level according to the objectives and assumptions formulated, effectively the design of the fire detection system is significantly related to the optimization of the data center in the municipalities of Metropolitan Lima, 2020; where, the results show that 48.8% responded that most of the time if they have knowledge of such fire detection system implemented in the areas or departments of technological management; 60.5% also indicated that they always have knowledge for the optimization of the data center in decision-making when they have information from the Information Technology Managers of the district municipalities of Metropolitan Lima.

Keywords: Design of fire detection system and data center.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La presente tesis de investigación tuvo por objetivo establecer la relación entre el sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020. En este contexto, las organizaciones que tienen la gerencia de las áreas de tecnologías de información (TI), en la actualidad toman importancia para diseñar un sistema de detección y extinción de incendios dentro de la institución, otorgándole la probabilidad de tener en sus organizaciones un sistema para gestionar y afrontar cualquier tipo de eventualidad de incendio o iniciar un incendio dentro de la infraestructura de los servidores llamado data center, los cuales deben cumplir para su implementación estándares y fases de manera específica sobre cómo implementar el diseño en base a las regulaciones NFPA 72 (Código nacional de alarma y señalización contra incendios) donde se establecen la protección de vidas humanas en la organización.

Por otra parte, promover proyectos en diseño del sistema de detección y extinción de incendio, en las áreas de TI, en la actualidad es la solución integral para las organizaciones que viene implementando frente a los posibles incendios que se requiere, por la latencia permanente en nuestro medio, por ende, la investigación y el conocimiento de las normas permitirán prevenir en la gestión del riesgo para poner a salvo y tener como misión la protección de vidas humanas, al incorporar la herramienta de apoyo a las municipalidades de Lima Metropolitana al momento de implementar este sistema como parte de la infraestructura basado en la normatividad técnica que beneficiara en las instalaciones del área de tecnología.

De igual manera, es importante tener presente que, en las actividades frecuentes de cualquier organización, se puede presentar situaciones que afectan repentinamente riesgos y amenazas de situaciones como Naturales (vendavales, inundaciones, sismos, incendios forestales, tormentas eléctricas), Tecnológicas (incendios, explosiones, derrames de combustible, fallas eléctricas, fallas estructurales, etc.) y Sociales (atentados, vandalismo, terrorismo, amenazas de diversa índole), lo cual requiere disponer de planes de contingencias, lo cual se convierte en un plan de emergencias que se cimenta en las tareas de prevención y

preparación, a partir del diagnóstico de la situación desde el punto de vista administrativo, funcional y operativo para proteger el activo de la información y de nuestros sistemas de información y de seguridad que siempre habrá nuevos ataques a los que seremos vulnerables.

La investigación ha sido desarrollada en siete capítulos. En el primer capítulo, se plantea la descripción de la realidad problemática, formulación de los problemas, los objetivos y las hipótesis de la investigación y la justificación.

En el segundo capítulo, se desarrollaron los antecedentes de la investigación, las bases teóricas, y las definiciones de términos básicos.

En el tercer capítulo, se muestra la metodología, es decir el diseño metodológico, población y muestra, técnicas de recolección de datos y procesamiento de los datos.

En el cuarto capítulo, se detallaron la presentación, análisis e interpretación de resultados obtenidos en la investigación a través de las encuestas; así como también, la contrastación de la hipótesis.

En el quinto capítulo, se detalló la discusión de los resultados obtenidos en la investigación a través de las encuestas; se presenta las conclusiones y las recomendaciones donde se plantea los logros alcanzados en el proceso de la investigación y los planteamientos para abordar la solución de los problemas identificados. Asimismo, se presentan las fuentes de información, que son el sustento de la presente investigación, y los anexos conformados por la matriz de consistencia, el cuestionario de la encuesta y la base de datos utilizada en el presente estudio de investigación.

En el sexto capítulo, se muestra la conclusión obtenida en el trabajo de investigación mostrando relación de las 2 variables.

En el séptimo capítulo, se mencionó las recomendaciones para obtener mejoras.

I. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

Las actividades en el mundo a través de las organizaciones públicas y privadas generan grandes volúmenes de información que sirven para la toma de decisiones, gracias al uso y conocimiento de las tecnologías de información y comunicación se puede promover cambios, en base a la interconexión física de redes e inalámbrica entre las instituciones, los cuales requieren que sus equipos y las arquitecturas tecnológicas que disponen en los diferentes procesos organizacionales, sean diseñados e implementados en espacios y áreas que brinden la seguridad efectiva, a fin de garantizar la vida útil del equipamiento electrónico, protección en la detección y extinción de incendios para la optimización del Data Center (Servidor principal del centro de datos) que debe estar en todo momento funcionando y operativo para brindar los servicios que ofrece la institución con la ciudadanía.

> Desde este contexto, en la actualidad la mayoría de las organizaciones a nivel mundial y latinoamericana, están dando prioridad con la implementación y diseño de infraestructura de un Data Center, teniendo presente previo el diseño de un sistema de detección de incendios, planes de contingencia, seguridad de la información, cableado estructurado de redes, con la finalidad de integrar múltiples servicios, principalmente garantizar la seguridad de la información a través de la aplicación de normas y estándares, para proteger los servidores de bases de datos, de archivos y web que contienen información crítica e histórica de los procesos de la organización. Por lo tanto, el gerente de Tecnología de Información debe ver que el crecimiento de la información a manejar trae consigo el crecimiento de la infraestructura requerida para almacenar, mantener y administrar dicho volumen de datos, lo cual representa diversos retos para la administración de la Data Center en diferentes organizaciones (Córdova, 2012, p. 1).

Es importante destacar, el problema se origina en las direcciones, áreas, departamentos de las Gerencias de Tecnologías de Información de las 43 municipalidades distritales de Lima Metropolitana, debido que al avance de los años

estas Instituciones Públicas incrementó sus aplicaciones y equipos de arquitecturas tecnológicas dando espacio a la necesidad de disponer con un sitio adecuado para los servidores centrales, con el fin de promover la integración, seguridad, control y seguimiento de los diferentes sistemas de información de manera apropiada en las municipalidades. En efecto, los diseños actuales del espacio o área (físico) para los servidores centrales no sigue las normas (*American National Standards Institute/Telecommunications Industry Association*) ANSI/TIA 942 para las instalaciones físicas de un Data Center; no se dispone de un sistema de detección y extinción de incendios, planes de contingencia actualizados (plan informático, plan contra incendios y plan de seguridad de la información) para hacer frente a los problemas y eventos que ponen en riesgo y peligro los volúmenes de la información de los diversos procesos y servicios que ofrecen a la ciudadanía, asimismo, en muchos casos no se cuenta con un manual de procedimientos informáticos actualizado para responder a las amenazas latentes.

De eso se desprende que, las municipalidades distritales de Lima Metropolitana en la actualidad las Gerencias de Tecnologías de Información disponen de un cuarto de servidores que carecen de la aplicación de las normas y estándares de infraestructura, lo cual convierte que la seguridad que ofrece esta área no es la más óptima y adecuada debido a que existen accesorios, climatización, cámaras limitadas para el monitoreo del personal y equipos informáticos, por ende, es de urgencia la necesidad de un sistema de detección y extinción de incendios para el accionamiento manual y automático, el sistema de control de acceso para los cuartos posee funciones muy básicas de operación, las puertas de ingreso al cuarto de servidores centrales (data center) no están construidas de un material resistente para la protección del activo crítico del equipamiento y la información de la organización.

De igual manera, con relación al personal del área no dispone de un plan de contingencia actualizado, para actuar frente a desastres y emergencias que pudieran suscitarse, además existe limitación con los sistemas de climatización para mantener los equipos en óptimo funcionamiento para la prolongación de la vida útil del equipamiento en el data center que garantice la seguridad de la información.

Por estas razones, las municipalidades distritales de Lima Metropolitana deben priorizar a fortalecer la gestión de las actividades públicas, teniendo en cuenta que, las Tecnologías de Información garantizan el cumplimiento de los objetivos institucionales, a fin de garantizar la seguridad de la información institucional para brindar mejores servicios de calidad a los ciudadanos, que son la razón de ser para su calidad de vida y bienestar general.

En resumen, se evidencia claramente que estas limitaciones tienen como consecuencia que las municipalidades distritales de Lima Metropolitana, adquieran una pésima imagen frente a los ciudadanos en los diferentes servicios en la administración pública y a los propios colaboradores al no disponer de los medios adecuados para realizar sus propias actividades en la institución como parte de la gestión pública por resultados.

1.2. Formulación del problema

1.2.1. Problema general.

PG. ¿Qué relación existe entre el diseño del sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020?

1.2.2. Problemas específicos.

PE 1. ¿Qué relación existe entre la central de detección y extinción de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020?

PE 2. ¿Qué relación existe entre los planes de contingencia y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020?

1.3. Justificación del estudio

La investigación se justifica porque se procedió a determinar si el diseño del sistema de detección de incendios se relaciona con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

1.3.1. Justificación práctica.

Desde el punto de vista práctico, se justifica porque el diseño y la implementación producirá beneficios en cuanto a la protección, detección y extinción de incendios, administración y funcionamiento del Data Center, con la finalidad de optimizar su rendimiento basado en la seguridad de la información, garantizando la simplificación en la protección de los datos, la disponibilidad inmediata de la información, la escalabilidad a futuro para brindar mejores servicios de calidad a la ciudadanía.

1.3.2. Justificación metodológica.

Desde el punto de vista metodológico, se justifica porque se utilizó la investigación de campo a través de las entrevistas, encuestas y observaciones porque permitió la recolección de datos de los sujetos objetos de estudios en la investigación, de igual manera, se hizo uso del tipo de investigación aplicada porque permitió manejar el problema tecnológico, obteniendo la información de fuentes de información importantes para el estudio.

1.3.3. Justificación teórica.

Desde el punto de vista teórico, se justifica porque se puso mucho énfasis en las especificaciones técnicas de las normas y estándares que sirven de guía para el diseño de un sistema de detección y extinción de incendios y de la data center, el plan de contingencias informático, plan contra incendios porque se determina acciones que permiten hacer frente a eventualidades que se originan en los sistemas de información y comunicación, asimismo, indicar que la actualización del manual de procedimientos informáticos es de importancia porque compone las políticas, funciones y procedimientos que facilitan el cumplimiento de las tareas de manera organizada la gestión y administración del data center en las municipalidades de Lima Metropolitana.

1.4. Objetivos de la investigación

1.4.1. Objetivo general.

OG. Establecer la relación entre el sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

1.4.2. Objetivos específicos.

OE 1. Establecer la relación entre la central de detección y extinción de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

OE 2. Establecer la relación entre los planes de contingencia y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

II. MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes nacionales.

Yrupailla Delgado, J. A. (2021), *Planificación de un Data Center para la gestión de los servidores en el Operador Logístico JMA***.** (Tesis de Pregrado). Escuela Profesional de Ingeniería de Sistemas. Universidad César Vallejo. Lima. Perú.

Tuvo como objetivo determinar de qué manera, la planificación de un Data center influye en la gestión de servidores en el operador logístico JMA, la investigación fue aplicada, de diseño pre experimental de enfoque cuantitativo. Los resultados de la investigación se emplearon el pre test y post test para las hipótesis planteadas las cuales fueron nivel de disponibilidad de los sistemas en el pretest fue de 88.54%, mientras que en el postest se obtuvo un valor de 95.00%., índice de backup de base de datos en el prestest de 57.5%, mientras que en el postest se obtuvo un valor de 86% y el nivel de desempeño del api rest en el pretest fue 43.67%, obteniéndose luego el valor de 116 % en el postest para la muestra.

Se llegó a la conclusión de la velocidad tanto para la disponibilidad y desempeño de los servidores en porcentaje, involucró un crecimiento en la producción de entregas de pedido del día a día en el operador Logístico JMA.

Montaño Guerrero, R. A. y Bustíos Arteaga, J. L. J. (2020), *Diseño de un data center con arquitectura convergente para optimizar los procesos informáticos de la municipalidad distrital de José Leonardo Ortiz*. (Tesis de Pregrado). Escuela Profesional de Ingeniería Electrónica. Universidad Nacional Pedro Ruiz Gallo. Lambayeque. Perú.

Tuvo como objetivo principal diseñar un Data Center con arquitectura convergente, que permita integrar los servicios de voz, datos y video sobre una misma infraestructura de cableado estructurado, que solucione la problemática de la Municipalidad Distrital de José Leonardo Ortiz. Fue de tipo tecnológica de modo unidisciplinario. Con una población de 368 puntos de red, distribuidos en las diferentes áreas de la municipalidad.

En las conclusiones se definió el nivel de Clase 2 para el diseño del data center, según normativa BICSI 002, ya que cumple con los parámetros de nivel operativo 3, impacto del tiempo de inactividad menor, disponibilidad de la red, redundancia de los componentes eléctricos de UPS y la continuidad de los procesos informáticos. Se diseñó un Data Center con arquitectura convergente, logrando optimizar los recursos de infraestructura de cableado, al unificar en una sola red 298 estaciones de trabajo, 60 teléfonos VoIP y 10 Cámaras IP.

Larico, G. R. (2020). *Sistemas hiperconvergentes para mejorar la gestión tecnológica en centros de datos de la Universidad Nacional Amazónica de Madre De Dios* (Tesis de Doctorado). Escuela Universitaria de Posgrado. Universidad Nacional Federico Villareal. Lima. Perú.

Tuvo como objetivo determinar si el empleo de los sistemas hiperconvergentes mejora la gestión tecnológica en centros de datos de la Universidad Nacional Amazónica de Madre de Dios. La metodología es de tipo de investigación aplicada, enfoque cuantitativo, nivel explicativo, con una muestra de 15 trabajadores que laboran en la Oficina de Tecnología de Información de la Universidad Nacional Amazónica de Madre de Dios, se aplicó como técnica la encuesta y de instrumento el cuestionario que permitió recoger y analizar una serie de datos de la muestra.

Llegó a la conclusión que, el empleo de los sistemas hiperconvergentes, el diseño y la implementación de la nueva arquitectura permitió solución en la mejora de la Gestión tecnológica encontrando como resultado de la variable independiente en la variable dependiente el valor de significancia (valor critico observado) 0,003<0,05, por lo tanto, rechazamos la hipótesis nula y aceptamos la hipótesis alternativa, es decir la implementación de los sistemas hiperconvergentes mejora significativamente la gestión de servidores de centros de datos de la Universidad Nacional Amazónica de Madre de Dios.

Castillo, G. J. (2018). *Modelo de optimización de recursos de un data center que brinda infraestructura como servicio (IAAS) de manera controlable y auditable a pymes de la provincia del santa* (Tesis de Maestría). Escuela de Posgrado. Universidad Nacional del Santa. Chimbote. Perú.

El objetivo de investigación fue elaborar un modelo de optimización de un data center que brinda Infraestructura como Servicio (IaaS) de manera controlable y auditable a Pymes de la provincia del Santa. En el aspecto metodológico utilizó el enfoque cuantitativo, tipo aplicada, diseño no experimental, método deductivo, aplicando una muestra de 129 Pymes, la técnica empleada fue la entrevista y la observación, los instrumentos son cuestionarios y listas aplicados a los gerentes y/o personal TI de pymes de la provincia, así como observar sus políticas de control, seguridad y costes aproximados, las cuales quedan registradas mediante un acta de reunión.

La investigación concluyo que, actualmente la infraestructura TI – servidores de las PYMES analizadas, ninguna cumple con normas y buenas prácticas por la información recopilada, por ende, que ninguna satisface a los requerimientos de la gerencia de dichas empresas. Dentro de lo que cabe, la empresa Corporación MW cuenta con un mejor hardware, así como una mejor administración de su servidor y seguridad de la información; en tal sentido, la prioridad de la norma ANSI 942 se complementa con las buenas prácticas BICSI 002, pues una se centra netamente en la ejecución y la otra, aunque toca ese tema de forma superficial, también abarca gestión y control de la data center. La norma ISO 27001, y su correcta implementación con la ISO 27002 permitirá garantizar que el servicio de Infraestructura como Servicio cuente con un buen sistema de gestión de seguridad de la información.

Córdova, J., Fernández, I., Salgado, N., y Soberón, R. (2017). *Dirección del proyecto: sistema de detección, alarma y extinción de incendios de planta Atocongo* (Tesis Pregrado). Universidad Peruana de Ciencias Aplicadas. Lima. Perú.

El objetivo principal fue la aplicación de los estándares globales del PMI® en la Dirección del Proyecto llamado “Sistema de Detección, Alarma y Extinción de Incendios en Planta Atocongo” de la Empresa UNACEM. La metodología empleada es descriptiva bajo el enfoque cuantitativo, basado en la elaboración del Plan para la Dirección del Proyecto: Sistema de detección, alarma y extinción de incendios de planta Atocongo desarrollado en 24 meses y con un presupuesto estimado en USD 4,800,000.00.

La investigación concluyo que, a la finalización del proyecto, la Planta Atocongo de UNACEM cumplirá con la normativa nacional vigente al inicio del proyecto y desarrollará las operaciones asegurando la integridad de todos los trabajadores y de los activos de la organización; asimismo, asegurará la continuidad sostenible de las actividades operativas y comerciales, teniendo como resultado de la evaluación financiera del proyecto se obtuvieron los siguientes valores: TIR = 6.24%, VAN (8%) = USD 517,372.0, PAYBACK = 7 años.

2.1.2. Antecedentes internacionales.

Espinoza Ortega, M. G. (2021), *Estudio y diseño de un data center aplicando la norma ANSI/TIA 942 para ISP AZOTEL S.A*. (Tesis de Maestría) Universidad Católica de Santiago de Guayaquil. Ecuador.

Tuvo como objetivo realizar un Estudio y Diseño para un Data Center basado en la Norma ANSI/TIA-942. Fue una investigación de campo-documental.

En las conclusiones se puede mencionar que el diseño propuesto del data center de Clase II cumple totalmente con las recomendaciones del estándar ANSI / TIA 942 hechas para cada subsistema: para el subsistema de telecomunicaciones que está especificado en: cables, racks, gabinetes y pathways; en el subsistemas eléctricos que constituya en la redundancia, topología UPS y sistemas de aterramiento; en el subsistema mecánico determinando el área de cobertura adecuado del sistema de aire acondicionado, cumpliendo con todas estas recomendaciones de diseño se puede brindar disponibilidad y confiabilidad en los servicios brindados por Azotel S.A.

Ruiz, J. E. y Uribe, M. C. (2019). *Sistema de detección de incendios* (Tesis de Pregrado). Área de Posgrados de la Universidad Piloto de Colombia. Bogotá.

El objetivo de investigación fue crear el sistema de detección de incendios óptimo para la subestación del Papayo que permita cumplir con la normatividad vigente y con los requerimientos técnicos y financieros exigidos por Enertolima S.A. La metodológica que se escogió fue una investigación cuantitativa de tipo descriptivo, apoyada en el método de observación y el aprendizaje de datos históricos, partiendo el estudio con una revisión bibliográfica histórica sobre los

daños ocasionados y causas origen de un incendio en las subestaciones, como fuente de información se aplicó la norma NFPA 72 código de sistemas de alarma y detección de incendios.

La investigación concluyo que, se logró establecer el proceso de adjudicación, e implementación del sistema de detección de incendios en una subestación de distribución eléctrica perteneciente a la empresa Enertolima, cumpliendo la normatividad vigente con respecto a dichos sistemas además de las exigencias solicitadas en la definición de especificaciones técnicas determinadas por la compañía. Asimismo, se lograron materializar los puntos de referencia del diseño, suministro, montaje, y puesta en servicio de un sistema de detección de incendios, mediante la selección y la compra de los equipos en cumplimiento de las exigencias técnicas para la mejor solución del sistema de detección de incendios en las subestaciones eléctricas que permitirá beneficios de la implementación del sistema, y su aplicabilidad en las demás instalaciones de la compañía.

Cárdenas, S. E. (2017). *Análisis de arquitecturas modernas de Data Center* (Tesis de Pregrado). Universidad Técnica Federico Santa María. Valparaíso. Chile.

El objetivo de investigación fue crear un marco conceptual, mediante un modelo capas que permita establecer las estructuras que componen una data center, con el fin de servir como ayuda para su comprensión y evaluación de las arquitecturas modernas, lo cual busca analizar las últimas tecnologías para diseñar data centers eficientes, de bajo costo, y fácil administración. La metodológica utilizada fue de análisis – teórico, que requirió hacer una revisión de literatura actual como estado del arte sobre las tecnologías actuales con relación en términos de eficiencia, escalabilidad y confiabilidad.

La investigación concluyo que, existen diferentes tipos de estándares que permiten una correcta implementación y funcionamiento de una data center, dentro de las que se encuentran las normas mínimas que debe cumplir una data center para que pueda funcionar (temperaturas, humedad, seguridad, protección contra incendios) como las definidas por ASHRAE, en el caso de Chile: CONAMA para evaluar impacto ambiental. También se presentan diversos estándares que definen estructuras modulares para diseñar data centers de gran escala, como el popular

estándar TIA-942, el cual define los patrones de diseño de redundancia para catalogar a una data center en Tiers. Asimismo, el consumo energético en las datas centers llega al 4% del consumo a nivel mundial, por lo que generan un impacto ambiental considerable. La eficiencia energética en las datas centers no solo reduce la huella de carbono, si no que reduce considerablemente los costos generados por energía mal aprovechada, perdiendo millones de dólares al año por concepto de mal manejo energético. Finalmente, las nubes públicas proveen agilidad, escalabilidad, y alta disponibilidad para desplegar recursos IT de forma rápida. Dependiendo del caso, podría ser más económico el uso de las nubes públicas incluso a largo plazo, si se manejan de forma correcta los recursos IT y se mantiene control sobre los recursos desplegados.

Idrovo, C. (2017). *Rediseño integral del sistema de protección contra incendios en un edificio multipropósito* (Tesis de Maestría). Universidad del Alzuay, Cuenca. Ecuador.

El objetivo de investigación fue rediseñar un sistema integral de protección contra incendios en un edificio multipropósito. La metodológica utilizada es un estudio de tipo descriptivo, empleando la observación y análisis del diseño y características constructivas de la edificación, por lo cual se determina el nivel de riesgo para diseñar el sistema integral de protección contra incendios. El universo de estudio está constituido por todas las áreas del edificio: Locales comerciales, departamentos, pasillos, parqueaderos, terraza, área comunal, se aplicó técnicas e instrumentos de medición de áreas de la edificación, tanto constructiva como de su contenido y de las medidas de protección adoptadas, se aplicó el formulario como método (hoja de cálculo), donde se registraron los datos encontrados, para determinar el factor de seguridad contra incendios y con esto el nivel de riesgo. Posteriormente se realiza investigación documental con base en las normas en materia de prevención de incendios.

La investigación concluyo que, aplicando el Método Gretener y la evaluación sistemática, se logró identificar y evaluar el riesgo de incendio de la edificación. Además, las alternativas de prevención planteadas en base al cumplimiento de la normativa legal aumentan el nivel de seguridad de la instalación lo que se comprueba aplicando nuevamente el Método Gretener donde se obtiene un nivel

de seguridad Aceptable. Por ende, el plan de respuesta a emergencias contribuye con el rediseño del sistema para asegurar la prevención y protección de los ocupantes y minimizar las pérdidas.

Molano Pinzón, J. A. y Rodríguez Leguizamón, L. F. (2017), *Diseño del sistema contra incendios de extinción y detección para la facultad tecnológica de la universidad distrital Francisco José de Caldas, conforme a la norma NFPA y la NSR-10*. (Tesis de Pregrado). Universidad Distrital Francisco José Caldas. Bogotá. Colombia.

Tuvo como objetivo Diseñar el sistema de extinción y detección de incendios para la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas, conforme a la norma NFPA y la NSR-10. El proyecto exige identificar y separar las zonas que tienen más riesgo en caso de propagación de incendio de las que no requieren de una protección por su bajo grado de inflamabilidad, ya que se contempla que no todo el plantel cuente con una red del sistema contra incendio, sino solo aquellas áreas que por su grado de peligrosidad o número de residentes así lo exijan.

Se llegó a las conclusiones que las técnicas de cálculo por software computarizado permitieron agilizar el proceso de diseño y optimizar los tamaños de la red contra incendio, de manera que esto permitió mediante iteración la minimización de los diámetros de las tuberías y accesorios del sistema. Se evidenció a lo largo de este proyecto que el sistema contra incendio es una necesidad de la Facultad Tecnológica. El trabajo llevado a cabo busca contribuir al cambio de esa condición, pretendiendo así que sea instalada una red que sea efectiva y funcional a la hora de apagar incendios, que salvaguarde la vida de los habitantes del plantel y la integridad de las cosas.

2.2. Bases teóricas de las variables

2.2.1. Variable sistema de detección de incendios.

2.2.1.1. Definición.

“Son unos medios muy eficaces para proteger a las personas, las instalaciones, los equipos, los bienes y los materiales de los peligros derivados de un incendio, si son instalados, mantenidos y utilizados adecuadamente” (Llenas, 2016, 2016, p. 5).

En este contexto, el sistema de detección de incendios se ha desarrollado a lo largo de su vida y en la actualidad se han fortalecido con el avance de las tecnologías y en la praxis su empleo es un elemento indispensable a la hora de detectar un incendio, de consideración relevante en su periodo inicial, lo que evidencia los momentos más críticos. Es decir, en el momento que se origina un incendio puede ser neutralizado sencillamente, en cambio, una detección lenta del incendio retrasaría las intervenciones de emergencia presentada, lo cual puede causar grandes pérdidas e incrementar exponencialmente el problema, lo cual dificultará la extinción oportunamente.

Asimismo, cabe señalar que el sistema de detección de incendios debe ser empleado e implementado con la normativa técnica que permite su correcto y apropiado diseño, donde viene definida en la familia de las normas UNE EN 54. Sistemas de detección y alarma de incendios, y en la norma UNE 23007-14. Sistemas de detección y alarma de incendios. Los cuales pueden ser implementadas de acuerdo al Parte 14: Planificación, diseño, instalación, puesta en servicio, uso y mantenimiento, teniendo en cuenta la Norma UNE 23007-14 (2014).

Por otra parte, según Esplugas (2016) señala que “la función principal de un sistema de detección de incendios es la de detectar un incendio en el momento más temprano posible y emitir las señales de alarma y de localización adecuadas para que puedan adoptarse las medidas apropiadas” (p. 7).

Por lo tanto, dicha función de un sistema de alarma consiste en emitir señales acústicas y/o visuales a los habitantes de un edificio y/o trabajadores de la data center, etc., en el que pudiera existir el riesgo de incendio. Es decir, tanto las funciones de detección y de alarma pueden estar integradas en un solo sistema, lo cual hace que la detección de un incendio puede ser ejecutada por las personas, por instalaciones automáticas de detección, o sistemas mixtos, de acuerdo con la implementación del servicio solicitado por las empresas.

En definitiva, todas las empresas deben conocer y considerar para el diseño del sistema de detección y extinción de incendio, cumplir con las normas NFPA 72: “*National Fire Alarm Code* - Código nacional de alarma y señalización contra incendios” y NFPA 2100: “*Standard on clean agent fire extinguishing systems* -

Sistemas de extinción de incendios con agentes limpios".

Norma NFPA 72 (Código nacional de alarma y señalización contra incendios)

Proporciona las disposiciones de seguridad más recientes para satisfacer las demandas cambiantes de detección de incendios, señalización y comunicaciones de emergencia de la sociedad. Además del enfoque principal en los sistemas de alarma contra incendios, el código incluye requisitos para los sistemas de notificación masiva utilizados para emergencias climáticas; eventos terroristas; emergencias biológicas, químicas y nucleares; y otras amenazas.

Norma NFPA 2100 (Sistemas de extinción de incendios con agentes limpios)

Los sistemas de extinción de incendios con agentes limpios se rigen por la norma NFPA 2001. A partir del 2012, el Consejo de Normas de la NFPA la norma contiene algunos cambios importantes que incluyen aumentos a la concentración mínima de diseño de los gases del agente limpio.

2.2.1.2. Dimensiones de la variable sistema de detección de incendios.

2.2.1.2.1. Dimensión central de detección y extinción de incendios.

> Se define como un sistema electrónico encargado de la protección a instalaciones que tengan un grado de vulnerabilidad para que se presente un incendio, es un conjunto de dispositivos guiados mediante un controlador que permiten dar una señal de alerta sobre algún evento que se pueda generar en el lugar protegido, acompañado de un sistema de extinción que se accionara en el momento que se presente un incendio (Neira, 2008, p. 14).

Dentro de este contexto, se puede evidenciar que el autor señala que, todo diseño de un sistema de detección y extinción de incendio para una instalación, específicamente para un Data Center (Centro de Datos), debe tener como prioridad promover la capacidad de respuesta para hacer frente a una emergencia de incendio que pueda llegarse a generar dentro de las instalaciones, que contenga equipamiento de arquitectura de tecnología de información de alta performance, por ende, la solución integral al tema de incendio conllevaría a la instalación de dispositivos electrónicos eficaces, los principios de seguridad contra incendios son:

- Reducir las posibilidades de inicio de un incendio
- Prevenir la propagación del fuego y el humo
- Asegurar la evacuación de los ocupantes
- Facilitar la intervención de los bomberos

Asimismo, Neira (2008) señala que, al disponer de un sistema de detección y extinción de incendio en una instalación, cuya selección para el diseño viene condicionada por:

- Las pérdidas humanas o materiales en juego.
- La posibilidad de vigilancia constante y total por personas.
- La rapidez requerida.
- La fiabilidad requerida.
- Su coherencia con el resto del plan de emergencia o contingencia.

2.2.1.3. Características de un sistema de detección y extinción de incendio.

Para Neira (2008) establece que:

> Se entiende por detección de incendios el hecho de descubrir y avisar que hay un incendio en un determinado lugar. Aunado a esto, las características últimas que deben valorar cualquier sistema de detección en su conjunto son la rapidez y la fiabilidad en la detección. De la rapidez dependerá la demora en la puesta en marcha del plan de emergencia y por tanto sus posibilidades de éxito; la fiabilidad es imprescindible para evitar que las falsas alarmas quiten credibilidad y confianza al sistema, lo que desembocaría en una pérdida de rapidez en la puesta en marcha del plan de emergencia (p. 14).

En tal sentido, la prioridad de la rapidez y la fiabilidad conlleva viabilizar el diseño de un sistema de detección y extinción de incendio, por ende, las empresas deben implementar una “Central automática de detención de incendios”, que es la encargada de recibir, procesar y ejecutar las señales recibidas desde los dispositivos de detectores, alarmas, central de control, pulsadores, etc., para ejecutar según la programación específica del recinto, la activación de pre-alarmas, alarmas y disparo de extinción (Edapi, 2018).

De eso se desprende que, la Central automática de detención de incendios deberá funcionar de manera provechosa, no sólo en las condiciones de un incendio, sino también cuando esté sometido a condiciones susceptibles de producirse en la práctica evitando falsas alarmas desde la programación automática. Es decir, las posibles acciones como resultado de la alarma es ordenar la evacuación de las personas antes de que las vías de evacuación puedan ser inundadas por el humo, así como acortar los daños al poder iniciar la extinción con los medios de extinción disponibles en el lugar del incendio.

De este modo, aplicar estrategias promueven desarrollar en cuanto a detección, alarma y comunicación, son necesarias para procurar una buena capacidad de respuesta ante una emergencia de incendio del personal que habitará las instalaciones, con la idea de facilitar las funciones de este sistema ante un evento de esta magnitud, por medio de los sistemas de Detección, Monitoreo, alarmas de evacuación y el sistema encargado de la extinción coordinados desde una central de control de operaciones o central automática de detención de incendios.

2.2.1.4. Componentes del sistema central automática de detención de incendios.

Una instalación automática de detección de incendios está formada por:

- Unos detectores de incendios distribuidos de forma regular por el recinto o recintos a vigilar.
- Un equipo de control y señalización.
- Unos elementos auxiliares: dispositivos de alarma por zonas y general, dispositivos de control y accionamiento de sistemas automáticos de protección contra incendios, incluyendo los sistemas de cierre de puertas de sectorización, apertura de exutorios de humo automáticos, transmisión de la alarma al exterior, paro de sistemas de aire acondicionado y ventilación, etc.
- Pulsadores de alarma.
- Líneas de interconexión entre los elementos anteriores y fuente de alimentación.

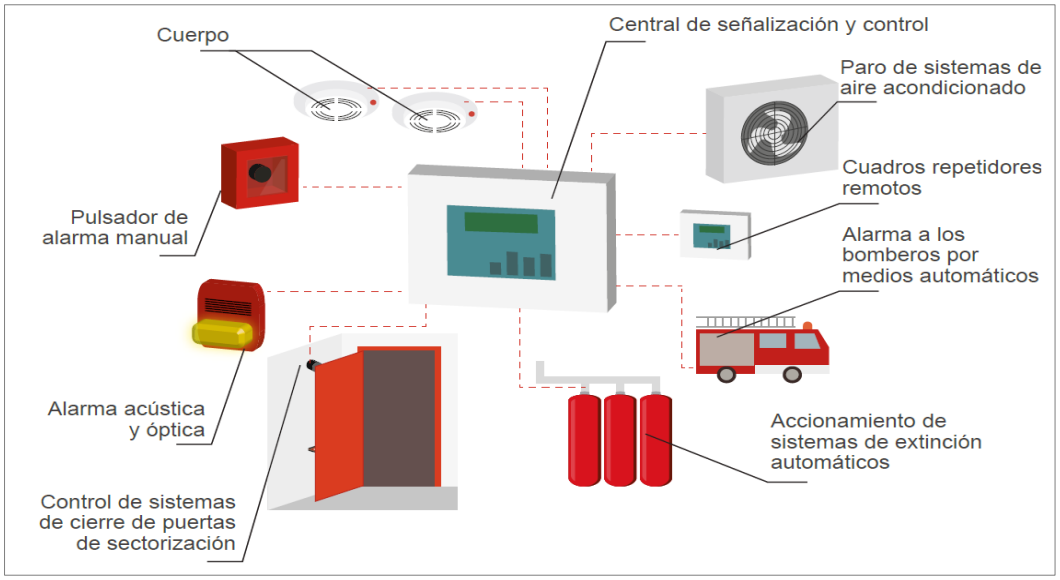


Figura 1. Componentes de un sistema de detección automática de incendios
Nota: Tomado de Esplugas (2016, p. 7). Guía para el diseño, uso y mantenimiento de los sistemas de detección automática de incendios.

2.2.1.4.1. El detector de incendios.

Es el elemento característico de la instalación es el detector de incendios. Según la Norma UNE EN 54-1 (UNE 23007, 2011) es el "componente de un sistema de detección de incendio que contiene, al menos, un sensor que controla de manera continua o a intervalos regulares, un fenómeno físico y/o químico asociado a un incendio y que emite una señal al equipo de control y señalización".

En efecto se dispone de los siguientes tipos de detectores, en función de las diferentes magnitudes físicas y/o químicas que son capaces de detectar:

- Los detectores térmicos son sensibles a la elevación de la temperatura (Termostáticos, termovelocimétricos y Combinados).
- Los detectores de humo son sensibles a las partículas derivadas de la combustión y/o pirólisis suspendidos en la atmósfera (aerosoles) y son de dos tipos (Iónicos y ópticos).
- Los detectores de gases son sensibles a los productos gaseosos de la combustión y/o descomposición térmica.
- Los detectores de llamas son sensibles a la radiación emitida por las llamas de un fuego.
- Finalmente, los detectores multisensores son sensibles a más de un fenómeno del fuego, por ejemplo, calor y humo.

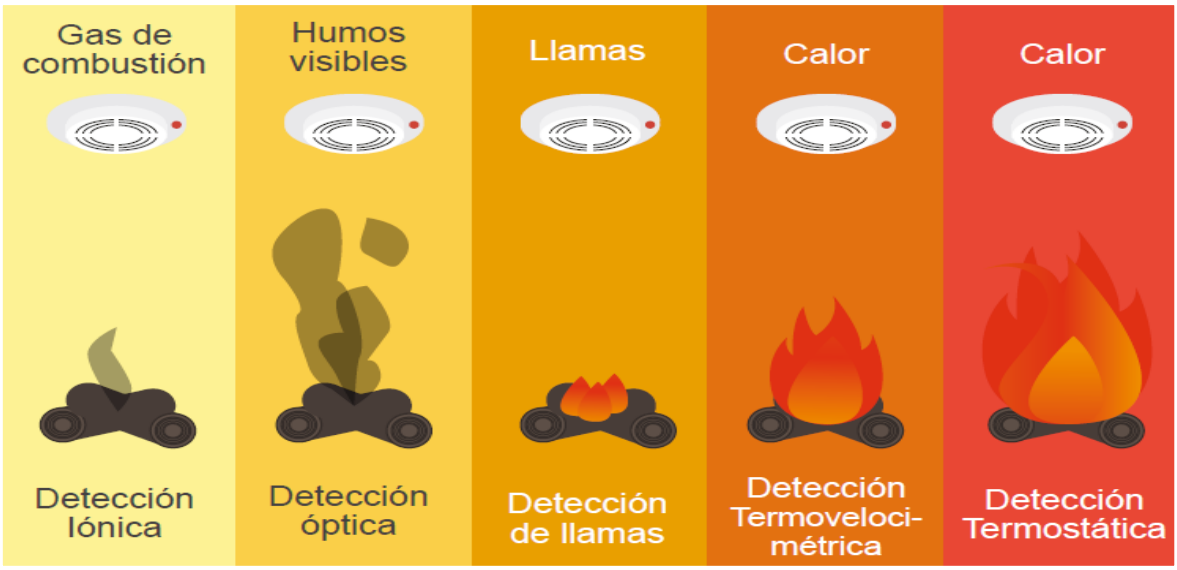


Figura 2. Tipo de detección en función de la evolución del fuego
Nota: Recuperado de Esplugas (2016, p. 11).

En tal razón, Esplugas (2016), señala que los detectores de incendios están diseñados usualmente para detectar una o más de las tres características del fuego: el humo, el calor y la radiación (llama). Cada tipo de detector corresponde a los distintos tipos de fuego con una sensibilidad diferente. Existen también detectores multisensores que combinan la detección simultánea de varias magnitudes, por ejemplo, temperatura, humo y gases de combustión como el CO (monóxido de carbono).

2.2.1.4.2. Equipo de control y señalización.

Es la parte de la instalación que alimenta a los detectores y otros componentes del sistema de detección y que realiza las siguientes funciones:

- Recibir la señal enviada por los detectores y pulsadores, determinando si corresponden a una condición de alarma de incendio, indicando la alarma por medio de señales audibles y visuales, y localizando el lugar en que se encuentra el detector o pulsador activado.
- En forma optativa puede registrar (grabar) total o parcialmente esta información.
- Transmitir la señal de alarma de incendio:

- A dispositivos de alarma de incendio audibles o visuales,
- A un servicio de bomberos, mediante un dispositivo de transmisión,
- A un sistema o equipo automático de lucha contra incendio.

- Supervisar continuamente la instalación e indicar los defectos mediante señales ópticas y acústicas de avería (Por ejemplo, en caso de rotura de línea o fallos de alimentación).

Aunado a esto, existe algunos tipos de centrales que llevan incorporados los dispositivos de alarma, por ejemplo: una sirena o un indicador óptico, mientras que otras no los incluyen.

En definitiva, Paltán (2013) establece que el sistema de detección de incendio debe cumplir con las normas NFPA 72*: "National Fire Alarm Code* - Código nacional de alarma y señalización contra incendios*"* (p. 124). Es decir, el Diseño del Sistema de Detección estará enfocado bajo la "Central automática de detención de incendios", que estará basado en un sistema de control y alarmas, capaz de emitir reportes remotos y de control a un panel centralizado, ubicado en el área de equipos de acuerdo a los parámetros de la superficie construida en m2, donde los detectores deben ser instalados en zonas de riesgo alto. Deberá constar de los siguientes componentes mínimos:

- **Panel de Control.** Deberá contar con un display digital, con circuitos de notificación, relays de contacto seco, etc. Mediante el display digital debe presentar las principales alarmas del mismo, así como el conteo regresivo para descarga de gas, voltaje de baterías y corriente de carga, etc.
- **Detectores de humo.** El sistema debe utilizar detectores fotoeléctricos y de ionización para pre-alarma y disparo en el área. Deberá existir detectores de humo distribuidos con sensores para detección en ambiente principal, sensores para detección en piso falso y sensores para detección en techo falso.
- **Sirenas con luz estroboscópica.** Se deberá contar con elementos de notificación de alarma como son sirenas con luz estroboscópica al interior del Data Center y una luz estroboscópica al exterior del Data Center.
- **Actuación Manual de Descarga.** El sistema podrá ser accionado mediante la estación manual de descarga ubicada a la salida del Data Center.

En resumen, los detectores serán del tipo adecuado a la forma de desarrollo

del posible incendio, teniendo en cuenta que no hay ningún tipo de detector que sea el más apropiado para todas las aplicaciones y la alternativa final dependerá de las circunstancias propias de cada evento que suceda, es decir, con frecuencia será útil usar una mezcla de diversos tipos de detectores, que serán seleccionados de acuerdo con la eficacia según la altura del local, entre otros factores que condicionan para la detección del incendio y tener presente el tiempo de respuesta.

2.2.1.4.3. Extinción de incendios.

> "Los métodos de extinción de incendios varían de acuerdo al sistema y el elemento encargado de sofocar las llamas. Encontramos entonces de diversos tipos, cada cual se adecua al tipo de vivienda o edificio en el cual son utilizados" (Neira, 2008, p. 39).

Según Paltán (2013) señala que el sistema de extinción de incendio debe cumplir con las normas NFPA 2100: *"Standard on clean agent fire extinguishing systems* - Sistemas de extinción de incendios con agentes limpios*".* Según la norma, el sistema debe usar agente limpio que cumpla: no corrosivo, no conductivo eléctricamente, incoloro y principalmente debe ser seguro para las personas, ya que no tiene restricciones en el tiempo de exposición posterior a una descarga. Daño potencial a la capa de Ozono (ODP) = 0, Potencial de calentamiento global=1 (p. 125). La cual debe constar de los siguientes componentes mínimos:

- **Agente extintor.** El sistema debe usar agente extintor FM-200. Debe ser un agente limpio, compuesto inodoro, incoloro, no conductor eléctrico y altamente estable. Su acción extintora se debe basar en un efecto fisicoquímico sobre el proceso de combustión a escala molecular, sin afectar el oxígeno disponible en el área. Esta acción debe permitir a las personas ver y respirar en una atmósfera. El nivel de concentración del agente para la supresión de incendios debe ser aprobado por la agencia *Enviromental Protection Agency* (EPA), para ser usado en áreas normalmente ocupadas, adicionalmente el agente extintor debe ser diseñado para extinguir fuegos de las siguientes clases: Clase A (madera, papel, plástico), Clase B (líquidos inflamables), Clase C (equipos eléctricos energizados)
- **Cilindro.** El agente deberá ser almacenado en cilindros de acero con

capacidad adecuada de acuerdo a la cantidad de agente para cada riesgo, presurizado con Nitrógeno seco. El cilindro deberá estar provisto de los siguientes componentes: válvula de operación automática alto flujo, manómetro para indicación visual de la presión, válvula de seguridad, tapa de seguridad para la boca de la válvula, soporte estructural, indicador de nivel para evitar el pesaje durante el mantenimiento periódico.

- **Boquillas de descarga.** Estas boquillas tendrán que estar diseñadas y fabricadas para producir una adecuada difusión del agente dentro del Data Center. Deberán constar de once boquillas de descarga distribuidos de la siguiente manera: 7 Boquillas en ambiente principal, 2 Boquillas en piso falso, 2 Boquillas en techo falso.

2.2.1.4.4. Cables y canalización.

El grupo de detectores requieren mínimo del cable que corresponderá a un cordón con un par calibre #18 AWG retardante de flama tipo FPL *(Fire Power Limited)* o FPLR. Encerrado en tubería Conduit EMT de acero galvanizado de 1/2" para la instalación de la canalización del sistema de detección y descarga. Para los cruces y derivaciones del Conduit, así como para base de montaje de detectores, sirenas y pulsadores, se utilizarán cajas de acero galvanizado octogonal o cuadrada con tapas. Tubería EMT de acero galvanizado para sistema de rociadores. El diseño del sistema de detección y extinción de incendios se presenta en la figura 3.

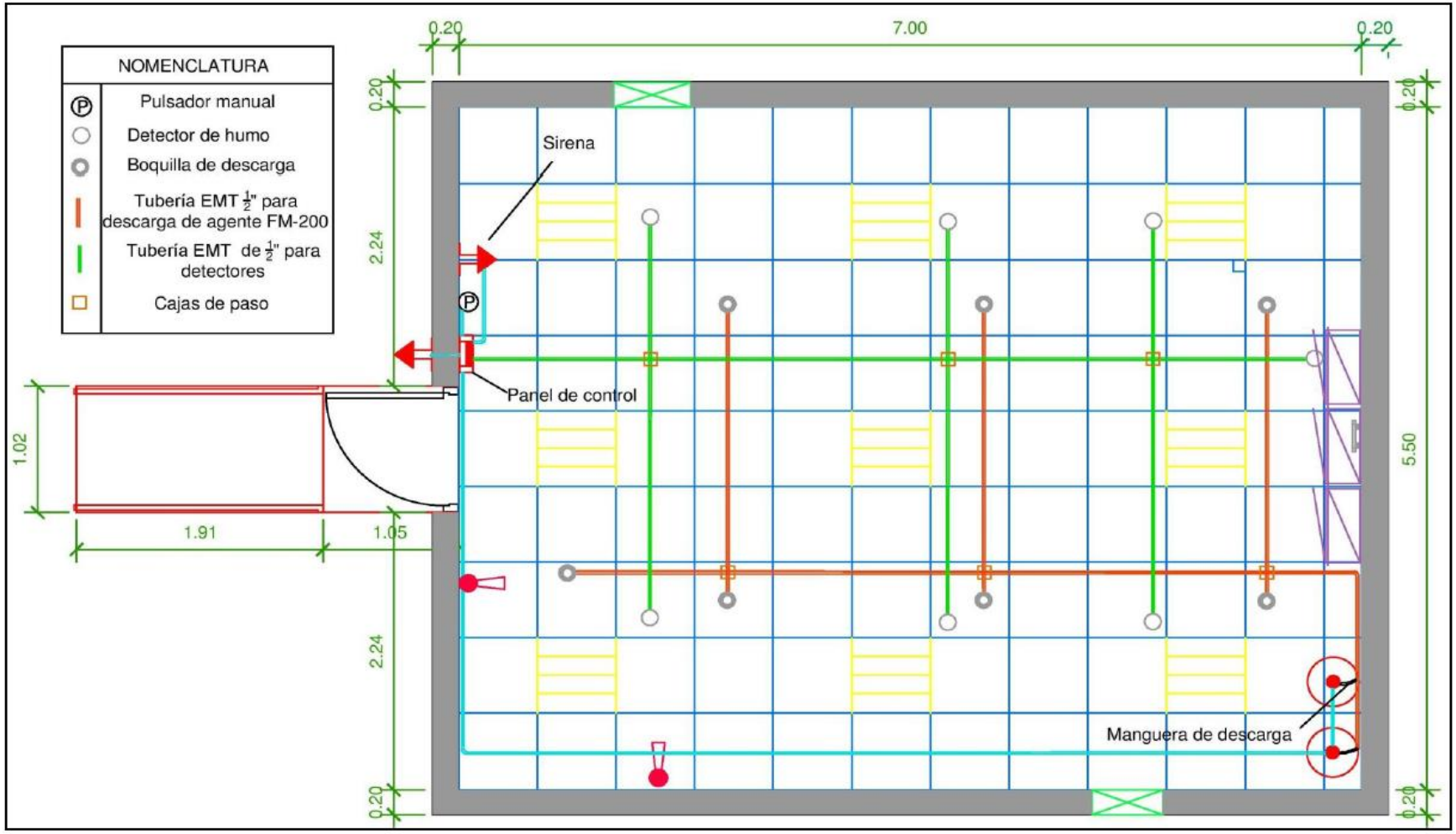


Figura 3. Propuesta de diseño del sistema de detección y extinción de incendios para el Data Center

2.2.1.4.5. Dimensión planes de contingencia.

> Es el instrumento principal que define las políticas, los sistemas de organización y los procedimientos generales aplicables para enfrentar de manera oportuna, eficiente y eficaz las situaciones de calamidad, desastre o emergencia, en sus distintas fases. Con el fin de mitigar o reducir los efectos negativos o lesivos de las situaciones que se presenten en la Organización (Positiva Compañía de Seguros de Colombia, 2015, p. 8).

> Para, Gutiérrez y Valencia (2006) establecen que el "Plan de contingencia" es una herramienta valiosa que permite implementar medidas de tipo preventivo que aminoren o eviten la ocurrencia de accidentes, tanto del personal vinculado directamente a las labores en las instalaciones que disponen equipamientos tecnológicos, como del área de influencia que sean vulnerables ante cualquier tipo de amenaza que provenga tanto del interior y del exterior (p. 143)

Según la Ley N° 28551 (2005), los planes de contingencia son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, victimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de producción industrial, potencialmente dañinos.

Dentro de este marco, en la administración pública según INDECI señala que los Planes de Contingencias, son procedimientos específicos prestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento particular para el cual se tienen escenarios prestablecidos. Donde las actividades señaladas en estos deben ser incorporadas al Plan Operativo Institucional (POI), los cuales se formulan a nivel nacional, regional y local, teniendo en cuenta la formulación y aprobación de Planes de Contingencia en base a un Lineamiento, que es de aplicación y cumplimiento en las entidades del Estado (Decreto Supremo Nº 048-2011-PCM, Reglamento de la Ley 29664).

Para tal efecto, el plan de contingencia según la Ley 29664 constituye un instrumento técnico de planeamiento especifico y gestión obligatoria, cuyo propósito es proteger la vida humana y el patrimonio.

En tal sentido, las empresas o entidades públicas del Estado realizan el diagnóstico para implementar los “Planes de contingencias”, teniendo en cuenta el Escenario definido, es decir, inicia con la descripción del evento particular, considerando su ocurrencia o inminencia, identificando su magnitud, duración, ubicación espacial y consignado en forma precisa su secuencia y características de manifestación. Para cada uno de los escenarios, detallar el impacto directo en: Personas, Líneas vitales y servicios básicos, Infraestructura productiva, vivienda y ambiente. Por lo tanto, teniendo como base, la implementación de los planes de contingencia en un escenario de manejo de cantidad de información y de equipamiento informático, se considera elaborar lo siguiente:

2.2.1.4.6. Plan de contingencia informático.

> Es el documento donde se establece las acciones que permiten afrontar eventualidades que se produzcan en los sistemas de información y comunicación, determinándose el manual de procedimientos informáticos porque compone las políticas, funciones y procedimientos que facilitan el cumplimiento de las tareas de manera organizada, frente a cualquier eventualidad de riesgo dentro de la instalación (Paltán, 2013, p. 4).
>
> Para el Ministerio del Ambiente (2020) señala que el Plan de contingencia informático, es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización (p. 5).

Es decir, dicho plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

- Antes, como un plan de prevención para mitigar los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

2.2.1.4.7. Plan contra incendios.

"Es el documento que se refiere a la gestión de la Brigada contra Incendios específicamente instruida para el control de incendios y emergencias asociadas a los riesgos y amenazas en las instalaciones" (Soto & Mora, 2017, p. 82).

Tabla 1.

Funcionamiento del Plan contra incendios

<table>
<tr><td colspan="3">COORDINACIÓN:
El plan contra incendios se encuentra a cargo del jefe de Tecnologías de Información en el Data Center y del jefe de Seguridad del Concejo de la Municipalidad Distrital</td></tr>
<tr><td>FUNCIONES EN EL DESARROLLO NORMAL DE LA ACTIVIDAD</td><td colspan="2">FUNCIONES EN CASO DE EMERGENCIA</td></tr>
<tr><td>Mantenimiento preventivo de extintores portátiles.</td><td>ANTES</td><td>Mantenimiento a equipos de atención de emergencias por fuego.
Ubicación estratégica del extintor, generando su fácil acceso. Capacitación anual de todos los empleados de la Municipalidad distrital sobre el manejo correcto del extintor.</td></tr>
<tr><td>Mantenimiento preventivo a instalaciones eléctricas.</td><td>DURANTE</td><td>Facilitar la evacuación de las personas en caso de conato de incendio.
Utilizar el extintor más cercano de acuerdo al tipo de fuego generado, siempre y cuando no se exponga la integridad personal de los Brigadistas.
Activación del sistema de emergencias a través del número único de emergencias 116.</td></tr>
<tr><td>Inspecciones mensuales a extintores y realización de los correctivos necesarios a los mismos.</td><td>DESPUÉS</td><td>Inventario de recursos utilizados en la emergencia para ser completados. Reacondicionamiento del lugar dependiendo los daños generados por la emergencia.
Informe del evento.</td></tr>
<tr><td>SEGUIMIENTO Y CONTROL</td><td colspan="2">CAPACITACIÓN</td></tr>
<tr><td>Registros de mantenimientos preventivos a extintores, realizado por personal especializado en el tema.</td><td colspan="2">Los Brigadistas reciben entrenamiento en manejo de extintores y técnicas de evacuación por fuego.</td></tr>
<tr><td>RECURSOS</td><td colspan="2">Extintores manuales distribuidos en todas las áreas de las Municipalidades de acuerdo al tipo de riesgo Sistema de alarma general Planos de evacuación de las diferentes áreas.</td></tr>
</table>

En este contexto, las entidades del Estado deben actualizar los Planes de Contingencia en su ámbito de responsabilidad según el Reglamento de la Ley 29664, en el marco del Lineamiento de aplicación y cumplimiento de las entidades de los tres niveles de gobierno integrantes del SINAGERD, teniendo en cuenta los contenidos de:

a) Escenario definido
b) Procedimiento de Coordinación
c) Procedimiento de Alarma
d) Procedimiento de Movilización
e) Procedimiento de Respuesta
f) Recursos financieros, logísticos y humanos
g) Mecanismos de evaluación.

En definitiva, es importante establecer la gestión para la creación de un plan de contingencias que permitirá minimizar los riesgos y amenazas a las entidades públicas, específicamente al contar con Data Center que requiere de la prevención mediante un plan de contingencia informático y plan contra incendios. Por lo tanto, en relación a lo establecido en el marco de la Ley N° 28551 (2005), en su artículo 10: que es de responsabilidad de las autoridades, obligados a capacitar a sus funcionarios y empleados en realizar los simulacros necesarios para la correcta aplicación de los procedimientos contenidos en los Planes de Contingencia y de prevención y atención de desastres. Es decir, la adecuación de la norma debe ser de prioridad contra los riesgos y eventos que se producen en las instalaciones en mención.

2.2.2. Variable data center.

2.2.2.1. Definición.

“El centro de datos (Data Center) es una instalación donde se concentran todos los recursos necesarios para el procesamiento de información de una organización o empresa” (Escobar, 2015, p. 10).

De igual manera, López (2012) señala que un Data Center es un espacio utilizado para contener sistemas de cómputo y sus componentes asociados como:

servidores, sistemas de almacenamiento, infraestructura de redes y telecomunicaciones.

En efecto, el estándar TIA 942 (2005) concebido como una guía para los diseñadores e instaladores de centro de datos, provee los lineamientos tomando en cuenta cuatro subsistemas, telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico.

De las evidencias anteriores, es muy importante tener en cuenta que, al diseñar un centro de datos, permitirá garantizar la integridad y funcionalidad de los sistemas mediante una distribución física, lógica de manera organizada, al ser la información un aspecto crucial en la mayoría de las operaciones de una empresa u organización se debe priorizar una Infraestructura robusta y confiable para albergar los equipos de tecnología, considerando en todo momento la disponibilidad y seguridad de los equipos informáticos o de comunicaciones implicados para la prestación de servicios en las entidades del estado para brindar un mejor servicio de calidad al ciudadano.

Asimismo, en espacio de las actividades cada área dentro del Centro de Datos debe tener los requerimientos específicos correspondiente a su propio sistema, cada sistema del Centro de Datos trabaja de manera interdependiente y la implementación de los mismos es obligatorio para un Centro de Datos como el diseñado en todo proyecto cuando se va a implementar. Según Escobar (2015) señala que dentro del Data Center debemos como mínimo contar los elementos siguientes:

a) **Infraestructura Física.** Se debe disponer de espacio suficiente para alojar los racks de los clientes y por ende a los equipos, se debe conocer cuál es el peso de los mismos para asegurar que el piso pueda resistir y el área que ocuparán dichos equipos / racks.

b) **Sistema eléctrico.** Se necesita un sistema autónomo que provea el suministro de energía eléctrica dentro del Centro de Datos y de igual manera provea energía a la Infraestructura que lo sostiene, esta energía debe ser provista de forma redundante y debe ser confiable para el buen funcionamiento de los equipos. Si el centro de datos está distribuido en

diferentes sitios los voltajes de operación pueden variar de un lugar a otro. Aquí también se enmarcan los sistemas de respaldo eléctrico.

c) **Sistema de Climatización.** Si no está aclimatado correctamente el cuarto que contiene los equipos, estos no podrán funcionar por mucho tiempo debido al sobrecalentamiento que se produciría por falta de circulación de aire que mantenga la temperatura óptima su trabajo. Se necesita tener un sistema de climatización que maneje los parámetros fundamentales de temperatura y humedad.

d) **Comunicaciones.** Sin un ancho de banda y comunicaciones adecuadas el Centro de Datos pierde el valor. El tipo y calidad del ancho de banda depende de los dispositivos tantos activos como pasivos que se encuentren en el Centro de Datos, Un buen sistema de comunicaciones es la ruta principal para la conectividad entre los equipos y sus interconexiones.

e) **Seguridad.** El sistema de seguridad brinda al Centro de Datos la certeza que su información permanece segura y confiable, por ende, se debe tener un sistema de video-seguridad y control de accesos acorde a la criticidad de cada área De acuerdo al sistema de seguridad diseñado se crearán los controles necesarios y otorgarán los permisos al personal.

En definitiva, la disponibilidad mínima de cada sistema dentro del Data Center debe tener un cumplimiento del 99.995%, acorde a lo que establece como disponibilidad para un Data Center Tier IV. Es decir, en particular, TIER denominación del nivel de fiabilidad de un centro de datos, indicando por uno de los cuatro niveles de fiabilidad llamados TIER, en función de su redundancia, a mayor número de TIER, mayor disponibilidad y por tanto mayores costes de construcción.

2.2.2.2. Clasificación de la Data Center.

2.2.2.2.1. Por el tipo de servicio.

1) **Data center de internet:** Construido por empresas para proveer a sus clientes tanto servicios de internet como servicios de datos (housing y hosting) quien abarca gran parte del mercado de las telecomunicaciones.

2) **Data center corporativo.** Son construidos para proveer servicio de datos a una sola empresa, quien permite la interconexión entre los diferentes servidores internos de una organización hacia la WLAN e internet.

2.2.2.2.2. Por los niveles de redundancia.

Está determinada por el *Uptime Insti*tute (2015) y depende de la disponibilidad y redundancia que posee una data center, se definen por 4 niveles de TIER:

1) **TIER I.** Infraestructura básica.

Usados en empresas pequeñas, no posee redundancia en ningún de sus componentes por lo que es susceptible a interrupciones de los servicios en el caso de existir alguna falla en sus elementos.

2) **TIER II.** Infraestructura con dispositivos redundantes.

Posee elementos redundantes, usualmente en aspectos eléctricos y de refrigeración, que lo hace menos susceptible a interrupciones en comparación al nivel I, tiene una sola ruta de distribución eléctrica, el piso y el uso de UPS es un requerimiento para su alimentación.

3) **TIER III.** Infraestructura concurrente mantenible.

Además de contar con redundancia en sus componentes, posee dos rutas de alimentación eléctrica y de enfriamiento de las cuales una está activa, todos los equipos de telecomunicaciones deben tener fuentes de alimentación redundantes esto permite realizar mantenimiento sin interrupciones de los servicios. Se establece el control de acceso mediante uso de lector de tarjeta o la identificación biométrica con el tiempo estimado de fallas de 105 minutos al año.

4) **TIER IV.** Infraestructura tolerante a fallos.

Data center con sistemas independientes con múltiples componentes redundantes y rutas de distribución que están activas siempre. Tiene resguardo contra desastres naturales como sismos, huracanes o inundaciones. Funcionamiento de alarmas de incendios, extinción de incendios o las características de apagado de emergencia puede causar una interrupción de

aproximadamente 52.56 minutos anuales.

En tal razón, Benalcázar (2017, p. 84), señala que el desarrollo y despliegue de software debe diseñarse en base a los nuevos contextos tecnológicos con infraestructura diseñada para las necesidades corporativas. Para lograr un alineamiento entre el desarrollo y despliegue de aplicaciones es necesario detallar los componentes del Data Center. Los componentes de Data Center se pueden clasificar en:

a) Componentes Mecánicos y Eléctricos:

Son los componentes de hardware que ayudan a mantener el ambiente del Data Center en condiciones propicias para dar continuidad al servicio que se provee. Estos elementos son: UPS, Tableros Eléctricos o PDU, Aire Acondicionado, Sistema contra Incendios, Seguridades Físicas, Tarjetas de Control, Control de Pasillos Caliente y Frío.

b) Componentes Computacionales:

Son aquellos que poseen capacidades técnicas y de seguridad que permiten asegurar disponibilidad de operación, entre éstos tenemos: Servidores Tipo Torre, Servidores Tipo Blade, Equipos de Comunicaciones y Firewall, Storage Externo, Firewall físico, Equipos Virtualizados, Servidores Web, Servidores SOA, Servidores de Autenticación, Servidores de Control de Perfiles de Usuario, Dispositivos de Almacenamiento (Sistemas basados en cinta, Unidades de Disco Duro, Unidades de estado sólido, Unidades de Disco Duro Híbrido).

c) Componentes de Software:

Son aquellos programas que sirven para gestionar los recursos del Data Center. Sirven para controlar la eficiencia y administrar los recursos que se proporcionan al usuario como servicios, mismos que son transparentes ya que solo ven el insumo final que es el sistema informático que utiliza. En esta categoría se ubica todo tipo de software que va a residir en forma directa en los servidores del Data Center o software que es utilizado en computadores personales que utilicen los servicios de cualquier componente del Data Center, un ejemplo es el software que utilizan los desarrolladores en forma local, pero utiliza la base de datos que

reside en los servidores del Data Center. Un ambiente seguro en Data Center consta de elementos como UPS, PDU, detectores de incendio, puertas de seguridad.

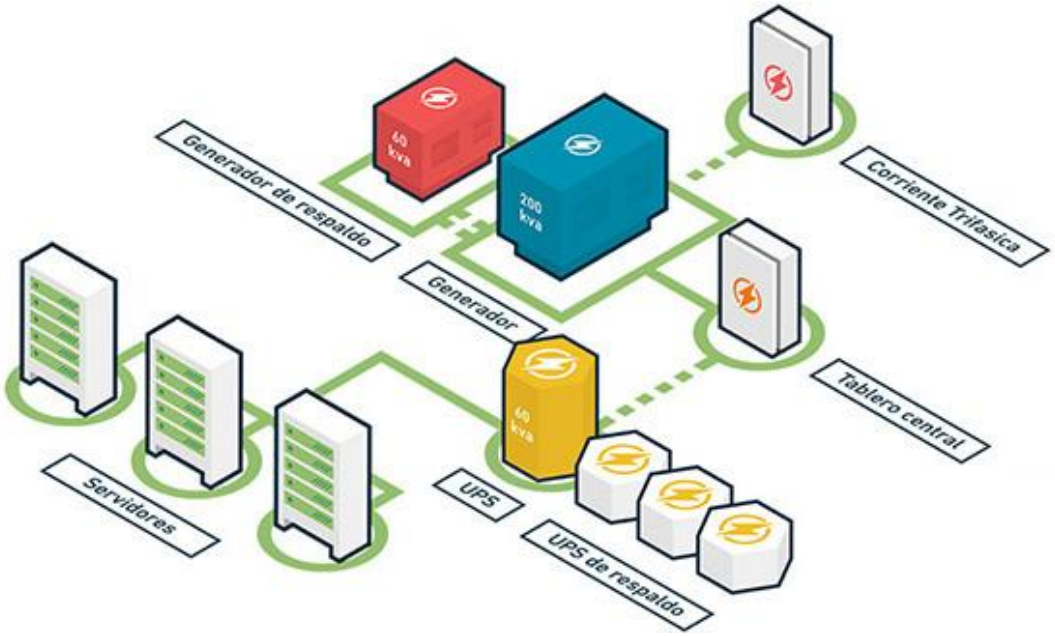


Figura 4. Componentes de un Data Center
Nota: Tomado de Tecnologías emergentes para Data Center

Los componentes de un Data Center con sus tecnologías pueden configurar sus sistemas de forma tan detallada que puedan satisfacer las necesidades particulares ambientales y de seguridad con una estrategia de supervisión que puede incluir múltiples puntos de recopilación de datos (Robinson, 2016) (Pracht & Architektur, 2011).

2.2.2.3. La Seguridad del Data Center.

El diseño del Data Center también debe emplear prácticas de seguridad y protección. Por ejemplo, la seguridad se refleja a menudo en el diseño de las puertas y pasillos de acceso, que debe adaptarse al movimiento de los equipos informáticos grande, difícil de manejar, así como los empleados de permiso para acceder y reparar la infraestructura. La extinción de incendios es otra área llave de seguridad, y el uso extensivo de equipos eléctricos y electrónicos, de alta energía sensible opone rociadores comunes. En cambio, los centros de datos suelen utilizar sistemas de supresión de fuego químico con el medio ambiente, que se muere de hambre con eficacia un fuego de oxígeno, mientras que la mitigación de los daños colaterales a los equipos.

Finalmente, desde el centro de datos también es un activo negocio principal, las medidas integrales de seguridad, como tarjeta de acceso y video vigilancia, ayudar a detectar y prevenir la malversación de los empleados, contratistas he intrusos (Alcocer, 2010).

2.2.2.4. Dimensiones de la variable data center.

2.2.2.4.1. Dimensión seguridad de la información y redes.

Se define como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada, es decir, significa que debemos proteger nuestros datos y nuestros recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos (ISO/IEC 27000, 2016).

> Por otro lado, (Vega, 2021) señala que seguridad de la información significa proteger nuestros activos, es decir, protegerlos de atacantes que invaden nuestras redes, desastres naturales, condiciones ambientales adversas, cortes de energía, robo o vandalismo u otros estados indeseables, por lo tanto, intentaremos protegernos contra las formas más probables de ataque, en la mejor medida que podamos, dado nuestro contexto (p. 9).

Para Gonzales y Vanegas (2006, p. 2), para mantener segura la información que viaja a través de la red esta debe cumplir con tres requisitos:

1) **Confidencialidad:** se debe garantizar que la información sea accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación.

   La confidencialidad es un concepto similar, pero no igual, a la privacidad. La confidencialidad es un componente necesario de la privacidad y se refiere a nuestra capacidad de proteger nuestros datos de aquellos que no están autorizados para verlos. La confidencialidad es un concepto que puede implementarse en muchos niveles de un proceso (Vega, 2021, p. 12).

   La confidencialidad puede verse comprometida por la pérdida de una

computadora portátil que contiene datos confidenciales, una persona que mira por encima del hombro mientras escribimos una contraseña, envío de archivos adjuntos de correo electrónico a la persona equivocada, un atacante que penetra en nuestros sistemas o infraestructura por medio de aplicaciones MITM (Man in The Middle) (Tchernykh et al., 2019).

2) **Integridad:** requiere que los recursos sean modificados por quienes están autorizados y que los métodos y los procesamientos de la información sean salvaguardados en su totalidad y con exactitud.

La integridad se refiere a la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o indeseable. Esto podría significar el cambio o la eliminación no autorizada de nuestros datos o partes de nuestros datos, o podría significar un cambio o eliminación autorizado, pero no deseable. Para mantener la integridad, no solo necesitamos tener los medios para evitar cambios no autorizados en nuestros datos, sino también la capacidad de revertir los cambios autorizados que deben deshacerse (Vega, 2021, p. 13). Es decir, la integridad es particularmente importante cuando discutimos los datos que proporcionan la base para otras decisiones.

3) **Disponibilidad:** se requiere que la información esté disponible en el momento exacto para quienes están autorizados a acceder a ella.

La disponibilidad se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos. La pérdida de disponibilidad puede referirse a una amplia variedad de interrupciones en cualquier parte de la cadena de comunicaciones que nos permite acceder a nuestros datos. Tales problemas pueden ser el resultado de pérdida de energía, problemas del sistema operativo o de la aplicación, ataques a la red de datos, compromiso de un sistema u otros problemas que impidan a los usuarios acceder a su información. Tales problemas son comúnmente causados por los ya conocidos y avanzados ataques de denegación de servicio (DoS) (Wang et al., 2017, citado en Vega, 2021, p. 13).

Aunado a esto, los tres los conceptos principales en seguridad de la información son precisamente la confidencialidad, integridad y disponibilidad, comúnmente conocida como la tríada de la seguridad de la información. La tríada

de la CIA, que ha sido utilizada por más de 20 años, brinda un modelo mediante el cual podemos pensar y discutir conceptos de seguridad, y tiende a centrarse mucho en la seguridad de los datos (Parada et al., 2018 citado en Vega, 2021, p. 12).

2.2.2.5. Riesgos y medidas de seguridad.

Un riesgo es la probabilidad de que ocurra un evento en contra de la seguridad de la red o uno de sus activos causando daños o pérdidas, un análisis de riesgos permitirá a la organización especificar cuáles riesgos son más probables de ocurrencias, cuáles serán más destructivos y cuáles serán los más urgentes de minimizar. Las medidas de seguridad son las acciones que toma una organización para disminuir los riesgos de seguridad (Gonzales & Vanegas, 2006, p. 7). Las medidas de seguridad se dividen en:

- Preventivas: son las medidas que tienden a disminuir el riesgo de que una amenaza ocurra antes de producirse. ·
- Perceptivas: estas medidas consisten en realizar acciones que revelen riesgos no detectados.
- Correctivas: son las medidas que se toman cuando ha ocurrido una amenaza.

2.2.2.6. Políticas de seguridad.

Las políticas de seguridad son los lineamientos y formas de comunicación con los usuarios, que establecen un canal de actuación en relación a los recursos y servicios de la red. Esto no significa que las políticas sean una descripción técnica de mecanismos y tecnologías de seguridad específicas y tampoco términos legales que impliquen sanciones. Las políticas son una descripción de lo que se desea proteger y la razón por la cual debe hacerse. Estos lineamientos deben abordar aspectos como la evaluación de los riesgos, protección perimétrica, control de acceso, y normas de uso de Internet y correo electrónico, protección contra virus y copias de seguridad entre otros (Gonzales & Vanegas, 2006, p. 15)

2.2.2.7. Seguridad en servicios de red.

> Un servicio de seguridad es un servicio que garantiza que los sistemas de información o las transferencias de datos puedan tener la seguridad adecuada. Los servicios de seguridad se implementan mediante mecanismos de seguridad y de acuerdo a las políticas de seguridad. (Soriano, 2014, p. 31).

2.2.2.8. TLS.

Transport Layer Security (TLS) es un protocolo estándar de Internet que proporciona seguridad de las comunicaciones a través de Internet. El objetivo principal de este protocolo es proporcionar confidencialidad e integridad de datos entre dos entidades que se comunican. Un uso importante de TLS es proteger el tráfico de la *World Wide Web* permitiendo transacciones seguras de comercio electrónico. (Soriano, 2014, p. 64). Es decir, el TLS se utiliza ampliamente en aplicaciones tales como la navegación web, correo electrónico, fax por Internet, mensajería instantánea y voz sobre IP (VoIP).

2.2.2.9. Seguridad perimetral (Firewalls).

> Un firewall o cortafuegos es un dispositivo que se utiliza para proteger la red interna de una organización. Esta protección se lleva a cabo mediante la separación de la red interna del mundo exterior, o Internet. Todos los mensajes que entran o salen de la red interna a través del firewall son examinados para verificar si cumplen las normas de seguridad especificadas en las reglas del firewall. (Soriano, 2014, p. 69).

Por ende, antes de instalar un firewall, es preciso definir un conjunto de normas o reglas que constituyen la política de seguridad. Sin este documento no se puede asegurar la red con un firewall.

En consecuencia, un firewall puede hacer dos cosas. Puede bloquear o permitir una comunicación. Por lo general, se permiten todas las comunicaciones de la red interna a la red externa (Internet), pero si la política de seguridad establece una regla impidiendo el paso de un tipo de mensajes, el firewall lo bloqueará. Por ejemplo, a veces se impiden conexiones a sitios que no sean de confianza ni a otros

lugares considerados una amenaza para la seguridad o inapropiados para la organización.

2.2.2.10. Sistemas de detección de intrusión.

Los ataques son cada vez más sofisticados. Todo esto hace que proteger la red sea cada vez más difícil. Los sistemas de detección de intrusión (IDS, *Intrusion detection systems*) aparecieron para dar respuesta al creciente número de ataques a los principales lugares de interés y redes.

> Para, Soriano (2014) los IDS son una especie de sistema de gestión de seguridad para los ordenadores y redes. Un IDS recopila y analiza información de un ordenador o una red para identificar posibles violaciones de seguridad, incluyendo tanto el mal uso (ataques desde dentro de la organización) como las intrusiones (ataques de fuera de la organización). (p. 70).

2.2.2.11. Basados en red o basados en equipos.

- **Basados en red, (NIDS, *Network-based system*):** se analizan las comunicaciones que se intercambian por la red. El NIDS puede detectar mensajes maliciosos diseñados de forma que las reglas de filtrado de un firewall no lo detecten.
- **Basados en equipo *(*HIDS, *Host-based system*):** el IDS analiza toda la actividad en cada equipo individual.

2.2.2.12. Sistemas pasivos o sistemas reactivos.

- **Sistema pasivo:** el IDS detecta un posible fallo de seguridad, registra la información y envía las señales de alerta.
- **Sistema reactivo:** el IDS responde a una actividad sospechosa cerrando la sesión de un usuario o reprogramando el firewall para bloquear el tráfico de red que tiene su origen en una entidad sospechosa.

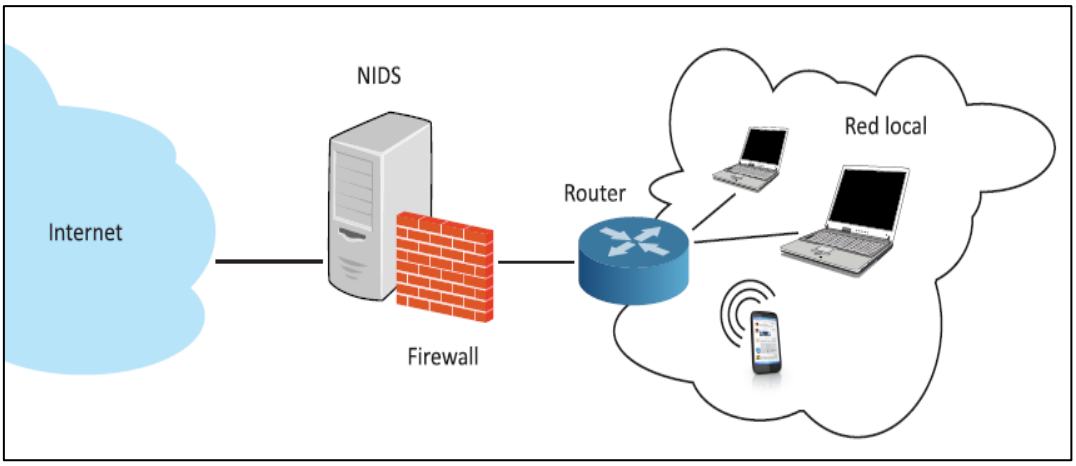


Figura 5. Diagrama con firewall e IDS
Nota: Tomado de Soriano (2014, p. 71)

En definitiva, un IDS se diferencia de un firewall en que este último limita el acceso entre redes con el fin de prevenir la intrusión y no indican un ataque desde el interior de la red. Un IDS evalúa una posible intrusión una vez que ha tenido lugar y señaliza una alarma. Asimismo, el IDS también analiza los posibles ataques que se originan dentro de un sistema.

2.2.2.12.1. Dimensión normas de seguridad para infraestructura de la data center.

Las actividades que se desarrollan en las entidades públicas y privadas actualmente poseen un Data Center con infraestructura física y tecnológica adecuada, donde se maneja de forma centralizada la información de toda la institución, denominada por lo general Departamento de Sistemas, Departamento de TI, entre otras nomenclaturas. Dichas unidades le permiten trabajar de forma ágil y segura, sin embargo, los Data Center muchas veces no cumplen con todos los requisitos establecidos en los estándares y normas aceptados internacionalmente, ya que no tiene en consideración factores importantes para preservar un servicio continuo, sin fallas y con seguridad. Es por ello, que estas normas y estándares se encargan de describir los procedimientos para asegurar que se encuentren correctamente protegidos y/o documentados, y evitar que cualquier tipo de evento no programado, cause pérdidas significativas que puedan llegar a comprometer a la institución de alguna manera (Jaramillo, Jácome, Ordóñez, Gaona, Carrión, & Palma, 2017, p. 150).

En tal sentido, el estándar especifica los requerimientos mínimos para la infraestructura de telecomunicaciones de Data Centers y cuartos de cómputo incluyendo Data Centers empresariales de único inquilino y Data Centers de "hosting" de Internet multi-inquilinos, además está basado en el *Uptime Institute* y contiene algunas recomendaciones Eléctricas, Mecánicas, Telecomunicaciones y Arquitectónicas.

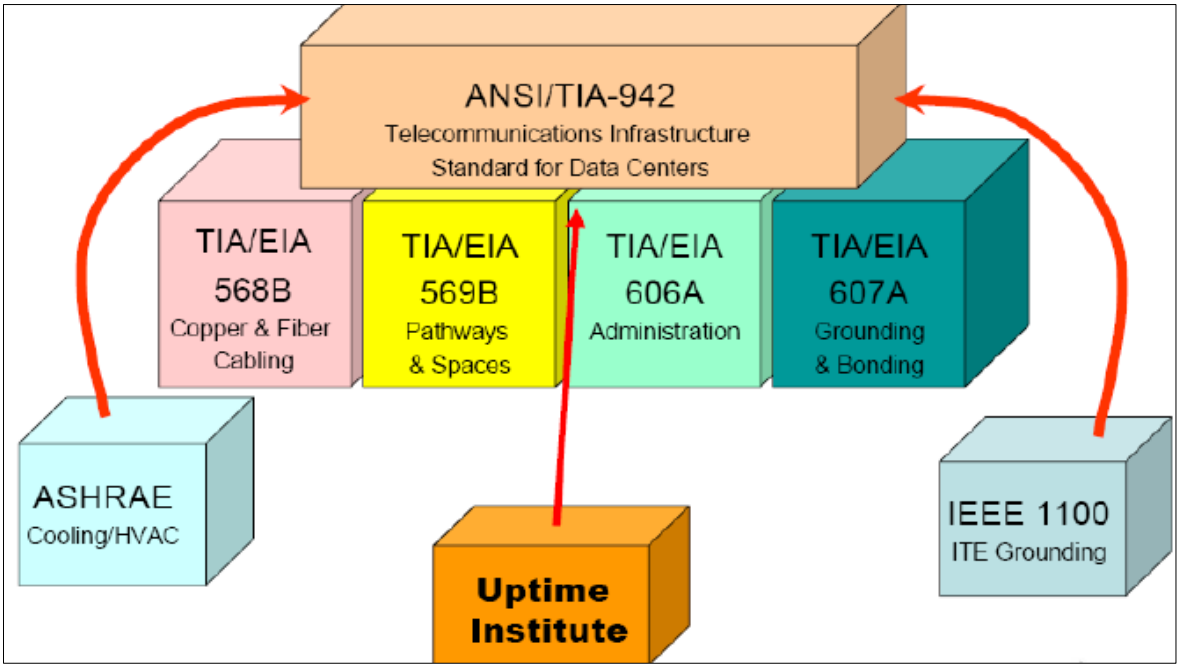


Figura 6. Bloques de construcción de un Data Center
Nota: Tomado de Peñaloza (2015). Standard TIA-942

2.2.2.13. Propósito de la Norma ANSI/TIA/EIA 942.

El propósito de esta norma es proporcionar requisitos y directrices para el diseño y la instalación de un centro de datos o sala de ordenadores. Está diseñado para ser utilizado por los diseñadores que necesitan un conocimiento global del diseño del centro de datos, incluyendo la planificación de las instalaciones, el sistema de cableado, y el diseño de la red (Peñaloza, 2015).

El Estándar ANSI/TIA/EIA 942, tiene como alcance definir una guía de diseño para Infraestructuras TI (Tecnologías de la Información), que garantice: Seguridad operacional, continuidad del servicio, disponibilidad y solidez, asimismo, brinda información acerca de la disposición espacial, infraestructura de cableado,

niveles de redundancia, es decir, especifica los requerimientos mínimos para la infraestructura de telecomunicaciones de Data Centers, además está basado en el *Uptime Institute* y contiene algunas recomendaciones Eléctricas, Mecánicas, Telecomunicaciones y Arquitectónicas (Polo, 2012).

Además, la norma permitirá el diseño de centros de datos para ser considerado temprano en el proceso de desarrollo de la construcción, lo que contribuye a las consideraciones arquitectónicas, al proporcionar información que corta a través de los esfuerzos de diseño multidisciplinar; promover la cooperación en las fases de diseño y construcción.

2.2.2.14. Norma ISO/IEC 27002.

Es una guía que contiene un conjunto de buenas prácticas para la seguridad de la información. Está conformada por un total de 39 objetivos de control y 133 controles que se encuentran agrupados en 11 dominios que cubren aspectos específicos de la seguridad de la información. La norma está estructurada en 16 capítulos de los cuales los cuatro primeros hacen referencia a los aspectos generales de la norma, mientras que los capítulos siguientes describen cada uno de los dominios que son parte de esta norma. (ISO/IEC 27000, 2016). A continuación, se describen de manera resumida los dominios integrantes de esta norma:

- Políticas de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicación y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento.

Finalmente, la aplicación de la Norma ISO/IEC 27002 y el Estándar TIA/EIA 942, son idóneas para el análisis, porque permiten cubrir la insuficiencia de la gestión de seguridad de la información y la infraestructura para la adecuada implementación, debido a que éstas engloban las mejores prácticas recopiladas de normas y estándares para el mejoramiento de la seguridad física y lógica. Es decir, los centros de datos en particular pueden beneficiarse de la infraestructura que se planifica con antelación para apoyar el crecimiento y los cambios en los sistemas informáticos que los centros de datos están diseñados para soportar.

2.3. Definición de términos básicos

Central de detección y extinción de incendios. Se define como un sistema electrónico encargado de la protección a instalaciones que tengan un grado de vulnerabilidad para que se presente un incendio, es un conjunto de dispositivos guiados mediante un controlador que permiten dar una señal de alerta sobre algún evento que se pueda generar en el lugar protegido, acompañado de un sistema de extinción que se accionara en el momento que se presente un incendio (Neira, 2008, p. 14).

Data Center. Concebido como una guía para los diseñadores e instaladores de centro de datos, provee los lineamientos tomando en cuenta cuatro sub sistemas, telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico (Norma Estándar TIA 942, 2005).

Detección de incendios. Es el componente de un sistema de detección de incendio que contiene, al menos, un sensor que controla de manera continua o a intervalos regulares, un fenómeno físico y/o químico asociado a un incendio y que emite una señal al equipo de control y señalización (Norma UNE EN 54-1 23007, 2011).

Extinción de incendios. Los métodos de extinción de incendios varían de acuerdo al sistema y el elemento encargado de sofocar las llamas. Encontramos entonces de diversos tipos, cada cual se adecua al tipo de vivienda o edificio en el cual son utilizados (Neira, 2008, p. 39).

Normas de seguridad para infraestructura de la Data Center. Considera el

estándar ANSI/TIA/EIA 942, que tiene como alcance definir una guía de diseño para Infraestructuras TI (Tecnologías de la Información), que garantice: Seguridad operacional, continuidad del servicio, disponibilidad y solidez (Polo, 2012).

Seguridad de la información y redes. Se define como la protección de nuestros activos, es decir, protegerlos de atacantes que invaden nuestras redes, desastres naturales, condiciones ambientales adversas, cortes de energía, robo o vandalismo u otros estados indeseables, por lo tanto, intentaremos protegernos contra las formas más probables de ataque, en la mejor medida que podamos, dado nuestro contexto (Vega, 2021, p. 9).

Sistema de detección de incendios. Son los medios muy eficaces para proteger a las personas, las instalaciones, los equipos, los bienes y los materiales de los peligros derivados de un incendio, si son instalados, mantenidos y utilizados adecuadamente (Llenas, 2016, citado en Esplugas, 2016, p. 5).

Planes de contingencias. Son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, victimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de producción industrial, potencialmente dañinos (Ley N° 28551, 2005).

Plan de contingencia informático. Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización (Ministerio del Ambiente, 2020, p. 5).

Plan contra incendios. Es el documento que se refiere a la gestión de la Brigada contra Incendios específicamente instruida para el control de incendios y emergencias asociadas a los riesgos y amenazas en las instalaciones (Soto & Mora, 2017, p. 82).

III. MÉTODOS Y MATERIALES

3.1. Hipótesis de la investigación

3.1.1. Hipótesis general.

Hi: El diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020, 2020.

3.1.2. Hipótesis específicas.

H1: La central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

H2: Los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

3.2. Variables de estudios

3.2.1. Definición conceptual.

Variable “1”: Sistema de detección de incendios

Son los medios muy eficaces para proteger a las personas, las instalaciones, los equipos, los bienes y los materiales de los peligros derivados de un incendio, si son instalados, mantenidos y utilizados adecuadamente (Llenas, 2016, citado en Esplugas, 2016, p. 5).

Variable “2”: Data Center

El centro de datos (Data Center) es una instalación donde se concentran todos los recursos necesarios para el procesamiento de información de una organización o empresa (Escobar, 2015, p. 10)

3.2.2. Definición operacional.

Variable “1”: Sistema de detección de incendios

La variable 1 se operacionalizará por intermedios de las dimensiones Central de detección y extinción de incendios, y Planes de contingencia; y ellos a través de sus respectivos indicadores, los que serán evaluados en un cuestionario valorado en Escala de Likert que contiene 10 ítem, como se visualiza en la tabla 2.

Variable “2”: Data Center

La variable 2 se operacionalizará por intermedios de las dimensiones Seguridad de la información y redes, y Normas de seguridad para infraestructura del Data Center; y ellos a través de sus respectivos indicadores, los que serán evaluados en un cuestionario valorado en Escala de Likert que contiene 10 ítem, como se visualiza en la tabla 2.

Tabla 2.
Operacionalización de variables

Variable	Dimensión	Indicador	Ítems	Instrumento	Escala
Sistema de detección de incendios	Central de detección y extinción de incendios	Capacidad de respuesta	1	Cuestionario	(1) Nunca (2) La mayoría de las veces no (3) A veces (4) La mayoría de las veces sí (5) Siempre
		Rapidez y la fiabilidad	2		
		Estrategias	3		
		Equipo de control y señalización	4		
		Agentes limpios	5		
	Planes de contingencia	Instrumentos de gestión	6		
		Procedimientos específicos	7		
		Planeamiento	8		
		Plan de contingencia informático	9		
		Plan contra incendios	10		
Data Center	Seguridad de la información y redes	Buenas prácticas y metodologías	11	Cuestionario	(1) Nunca (2) La mayoría de las veces no (3) A veces (4) La mayoría de las veces sí (5) Siempre
		Confidencialidad	12		
		Integridad	13		
		Disponibilidad	14		
		Políticas de seguridad	15		
	Normas de seguridad para infraestructura del Data Center	Infraestructura física y tecnológica	16		
		Estándar especifica	17		
		Guía de diseño	18		
		Estándar ANSI/TIA/EIA 942	19		
		Norma ISO/IEC 27002	20		

3.3. Tipo y nivel de la investigación

3.3.1. Tipo de Investigación.

Teniendo en cuenta la naturaleza de los objetivos previstos, el estudio de investigación reunió las condiciones necesarias para ser denominado como una “investigación aplicada”. Es decir, la “Investigación Aplicada”, tiene la finalidad de resolver problemas encontrados dentro de la organización con enfoque de la búsqueda de información de nuevos conocimientos para la aplicación y desarrollo de la investigación.

Según, los autores Hernández, Méndez, Mendoza y Cuevas (2017):

> La investigación aplicada, hace preguntas enfocadas en solucionar problemas específicos de un tiempo y un lugar o en generar desarrollo tecnológico. Por lo regular se basa en teorías que han sido resultado de investigación básica, solo que, como su nombre lo indica, se pone a prueba la aplicación de esa teoría en un aspecto en concreto y sus resultados son útiles para ser implementados (p. 20).

3.3.2. Nivel de investigación.

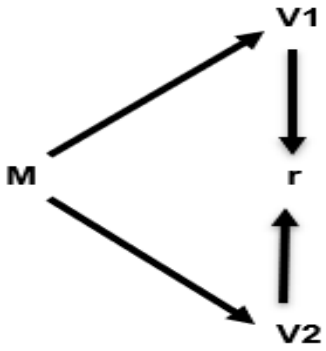
Se trató de una investigación de nivel correlacional, no sin antes haber sido descriptivo, pues se determina si el diseño del sistema de detección de incendios influye en la optimización de la data center en las municipalidades de Lima Metropolitana.

El nivel correlacional tiene por finalidad conocer la relación o grado de asociación entre las variables de estudios en una situación dada (Hernández & Mendoza, 2018, p,109).

3.4. Diseño de investigación

Por medio del diseño de la investigación se obtuvo toda la información necesaria y requerida para aceptar o rechazar la hipótesis. Se aplicó el diseño de tipo No Experimental de corte transversal correlacional. Es no experimental debido a que no se manipuló ninguna variable, debido a que se recolectó datos en un solo momento en un tiempo y correlacional porque se establecieron relaciones entre las

variables (Hernández & Mendoza, 2018, p.178). De acuerdo al diagrama de experimento y variables:



Donde:

M: Muestra
V1: Sistema de detección de incendios
V2: Data Center
r: relación entre variables

3.5. Población y muestra de estudio

3.5.1. Población.

La población objeto de estudio, estuvo conformada por 43 Gerencias de Tecnologías de Información de las municipalidades distritales de Lima Metropolitana.

3.5.2. Muestra.

La muestra se consideró censal, pues se seleccionó el 100% igual a la población de personas, al considerarla un número manejable de sujetos.

Según Ramírez, (2010), establece la muestra censal, aquella donde todas las unidades de investigación son consideradas como muestra, por ser una población pequeña. De allí, que la población a estudiar se precise como censal por ser simultáneamente universo, población y muestra: P = M.

En este sentido, la muestra fue igual a la población de 43 personas de las Gerencias de Tecnologías de Información de las municipalidades distritales de Lima Metropolitana, que fueron entrevistados para la aplicación del instrumento.

3.6. Técnicas e instrumento de recolección de datos

3.6.1. Técnicas de recolección de datos.

La técnica que se utilizó en este estudio fue la Encuesta. Es una de las técnicas de recolección de información más usadas, que se fundamenta en un cuestionario o conjunto de preguntas que se preparan con el propósito de obtener información de las personas (Bernal, 2010, p. 194).

3.6.2. Instrumentos de recolección de datos.

El instrumento de recolección de datos fue el Cuestionario aplicado a la muestra censal. Un cuestionario es un conjunto de preguntas respecto a una o más variables que se van a medir. El contenido de las preguntas de un cuestionario es tan diverso como los aspectos que evalúa (Hernández, et al., 2017, p. 155).

3.7. Métodos de análisis de datos

Según Bernal (2010, p. 194) para la recopilación de información implica una serie de pasos. Aquí se presenta un esquema general que puede usarse para la recolección de los datos necesarios, y su posterior análisis para responder a los objetivos y para probar la hipótesis de la investigación, o ambos.

Estos pasos son los siguientes:

Se administró la encuesta a los entrevistados entre personas de las Gerencias de Tecnologías de Información de las Municipalidades distritales de Lima Metropolitana, con la finalidad de obtener el recojo de información sobre las variables de investigación; las mismas que han sido diseñadas para una adecuada recolección de datos, mediante el empleo de la escala de Likert.

El escalamiento de Likert es un método que, trata de un enfoque vigente y bastante popularizado. “Consiste en un conjunto de ítems presentados en forma de afirmaciones para medir la reacción del sujeto en tres, cinco o siete categorías”. (Hernández, et al., 2014, p. 238). Se ha establecido para cada pregunta del cuestionario, el entrevistado responderá las alternativas de la escala de 1 a 5:

Tabla 3.
Valoración de Encuesta – Cuestionario

Codificación	Categorización
1	Nunca
2	La mayoría veces no
3	A veces
4	La mayoría veces si
5	Siempre

Asimismo, para el procesamiento de datos se utilizó la Estadística Descriptiva, esto permitió conocer y entender cómo se comportan los datos en cada variable y dimensiones, mediante las medidas de frecuencias, tablas y gráficos para cada pregunta, que arrojará porcentajes para los resultados, permitiendo establecer las interpretaciones de dichos resultados.

Para las pruebas de las hipótesis de la presente investigación, se empleó la estadística inferencial, mediante la Prueba estadística de Correlación Rho de Spearman para medir la intensidad de la relación de las variables por ser datos que no cumplen con los supuestos de distribución normal, cuya fórmula es la siguiente:

$$r_s = 1 - \frac{6\sum d^2}{n(n^2-1)}$$

r_s = Coeficiente de correlación por rangos de Spearman

d = Diferencia entre los rangos (X menos Y)

n = Numero de datos

Con el objetivo de categorizar las variables y dimensiones se presenta el baremo (niveles y rangos) utilizado para la elaboración de los análisis de asociación.

Finalmente, la aplicación de los métodos de análisis de datos se da en base a los resultados con el uso de los siguientes parámetros:

- Coeficiente de confiabilidad Alfa de Cronbach
- Estadística descriptiva para dar respuesta al objetivo e hipótesis general a través de las tablas de frecuencias y de contingencias.
- Método del análisis factorial, a fin de reducir la dimensionalidad de los datos en un número mínimo de dimensiones capaces de explicar el máximo de información contenida en los datos de los resultados de la variable y las dimensiones. (De la Fuente, 2011, p. 1).
- Estadística inferencial, con prueba de Correlación Rho de Spearman
- Se realizó la tabulación de los datos mediante la Técnica del Software SPSS ver. 25.0, para validar, procesar y contrastar hipótesis.

3.8. Aspectos éticos

Se cumplió con todo lo establecido en el Reglamento de la Universidad respetando las normas establecidas para los grados y títulos profesionales de los estudiantes egresados de las diversas Carreras de la Universidad Privada TELESUP; aprobado mediante Directiva de Taller de Tesis, 2019.

Asimismo, se cumplió en la presente investigación con el Código de Ética respetando los derechos de autoría y propiedad intelectual para la investigación de la Universidad Privada Telesup.

Finalmente, la investigación fue desarrollado teniendo en cuenta las normas establecidas por la Universidad Privada TELESUP, ciñéndose a la estructura metodológica establecida en el “Reglamento de Grados y Títulos de pregrado”; con la finalidad de establecer la relación entre el sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

IV. RESULTADOS

4.1. Presentación e interpretación de resultados

a. Los resultados obtenidos fueron analizados en el Nivel Descriptivo y en el Nivel Inferencial, a través de las características de la población muestral, respecto al Sistema de detección de incendios y la relación con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020. Con el fin de hacer esta descripción de forma ordenada y comprensible se considera el análisis e interpretación de los datos (Análisis exploratorio), analizados en el nivel descriptivo variable por variable.

b. En el nivel descriptivo, se han utilizado frecuencias y porcentajes para determinar los niveles predominantes de la variable Sistema de detección de incendios (**Central de detección y extinción de incendios y los p**lanes de contingencia**)** y la Data center (Seguridad de la información y redes y las normas de seguridad para infraestructura del Data Center), llevada a cabo en las municipalidades de Lima Metropolitana; en el nivel inferencial, se ha hecho uso de la estadística de análisis no paramétrico y como tal se ha utilizado el coeficiente de correlación Spearman, ya que se investiga el grado de influencia entre las dos variables cuantitativas medidas en un nivel ordinal.

c. Se empleó el instrumento descrito en el párrafo “a” Cuestionario para las variables Sistema de detección de incendios “1” y Data center “2”, donde se aplicó la “confiabilidad de los instrumentos”; mediante el coeficiente de Alfa de Cronbach para comprobar la consistencia interna, basado en el promedio de las correlaciones entre los ítems para evaluar cuánto mejoraría (o empeoraría) la fiabilidad de la prueba si se excluye un determinado ítem, procesado con la aplicación estadística SPSS ver. 25. Su fórmula determinó el grado de consistencia y precisión, de acuerdo a la tabla siguiente:

Tabla 4.

Valoración del Coeficiente de Confiabilidad

Valor	Consistencia
-1 – 0	No es confiable
0.01 - 0,49	Baja confiabilidad
0,5 – 0,75	Moderada confiabilidad
0,76 – 0,89	Fuerte confiabilidad
0,9 – 1,00	Alta confiabilidad

Nota: Adaptado Hernández y Mendoza et., al (2018)

Coeficiente Alfa de Cronbach

$$\frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_t^2}\right]$$

En dónde:

K = El número de ítems

$\sum \mathbf{S_i^2}$ = Sumatoria de varianzas de los ítems

$\mathbf{S_t^2}$ = Varianza de la suma de los ítems

œ = Coeficiente de Alfa de Cronbach

Este instrumento se utilizó en la prueba piloto de una muestra de 25 entrevistados para determinar si el diseño del sistema de detección de incendios influye en la optimización de la data center en las municipalidades de Lima Metropolitana, cuya base de datos de la prueba piloto se muestra en el (Anexo 4).

Este proceso compromete una mejora continua en el proceso de investigación, luego de varios tratamientos, consejos y reformulaciones de las preguntas se alcanzó el siguiente nivel de índices de los ítems. En el cuadro de diálogo que aparece, podemos ver el resultado de Alfa. A mayor valor de Alfa, mayor fiabilidad. El mayor valor teórico de Alfa es 1, y en general 0.76 se considera un valor aceptable. En el caso de nuestro resultado es el siguiente:

Tabla 5.
Resumen del procesamiento de los casos

		N	%
Casos	Válidos	25	100,0
	Excluidos[a]	0	,0
	Total	25	100,0

a. Eliminación por lista basada en todas las variables del procedimiento

Tabla 6.
Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,936	20

d. El coeficiente de Alfa de Cronbach obtenido es de 0,936, lo cual permite decir que el Test en su versión de 20 ítems tiene una alta confiabilidad, de acuerdo al criterio de confiabilidad de valores. Por lo tanto, se recomienda el uso de dicho instrumento para recoger información con respecto a las variables de estudios: Sistema de detección de incendios "X" y Data center "Y"

4.1.1. Análisis e interpretación de la variable "1": Sistema de detección de incendios.

Para evaluar la variable Sistema de detección de incendios, procedimos elaborar un instrumento de medición conformado por 10 ítems, dividido en dos partes en cada dimensión, recogiendo información referente a las dimensiones: **Central de detección y extinción de incendios y** Planes de contingencia, que son factores que influyen directamente en los Sistema de detección de incendios. Frente a cada pregunta del cuestionario, el entrevistado respondió las alternativas que le permitió evaluar en la escala de 1 a 4 de acuerdo al detalle siguiente:

Siempre = 5, La mayoría veces si = 4, A veces = 3, Mayoría veces no = 2 y Nunca = 1.

Tabla 7.
Norma de corrección sobre el Sistema de detección de incendios

Escala de Valores	Factores sobre el Sistema de detección de incendios		
	Sistema de detección de incendios	**Central de detección y extinción de incendios**	Planes de contingencia
	Rango	Rango	Rango
Siempre	41- 50	21 - 25	21 - 25
La mayoría veces si	31 – 40	16 – 20	16 – 20
A veces	21 – 30	11 – 15	11 – 15
La mayoría veces no	11 – 20	06 – 10	06 – 10
Nunca	01 – 10	01 – 05	01 – 05

Una vez obtenido las puntuaciones para cada factor del Sistema de detección de incendios se sumó las puntuaciones de cada factor para así poder dar una calificación general al cuestionario obteniéndose una puntuación mínima de 1 y una máxima de 50 de los valores en los niveles de medición.

Tabla 8.
Nivel de percepción sobre el Sistema de detección de incendios

		Frecuencia	**Porcentaje**
Válido	Nunca	1	2,3
	La mayoría veces no	6	14,0
	La mayoría veces si	21	48,8
	Siempre	15	34,9
	Total	43	100,0

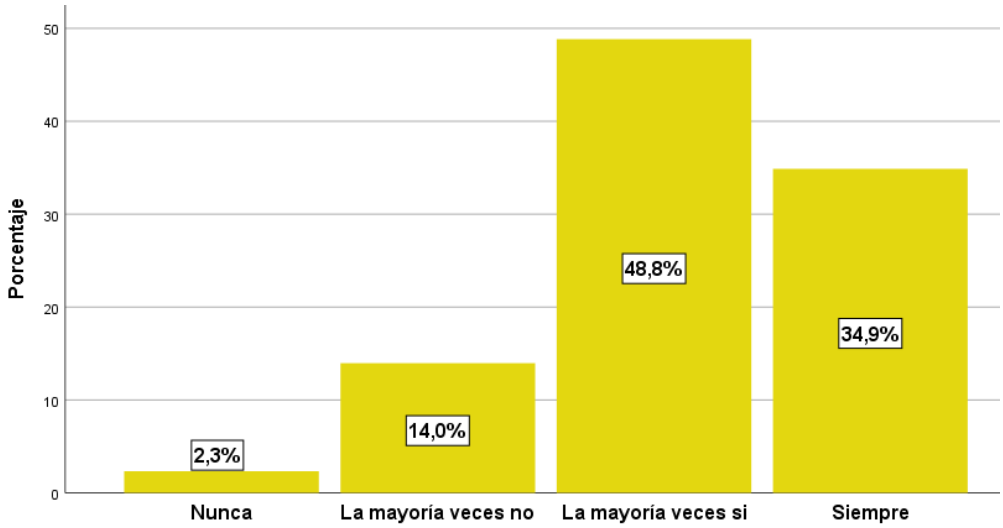


Figura 7. Nivel de percepción sobre el Sistema de detección de incendios

Interpretación:

En la Tabla 8 y Figura 7, se presenta el nivel de conocimiento sobre el sistema de detección de incendios en las municipalidades de Lima Metropolitana. Se observó que el 48,8% la mayoría de las veces si tiene conocimiento de dicho sistema, seguido del 34,9% que siempre lo realizan, mientras el 14,0% la mayoría de veces no y solo el 2,3% respondieron nunca sobre la variable de estudios.

a) Dimensión: Central de detección y extinción de incendios

Tabla 9.
Nivel de percepción sobre la Central de detección y extinción de incendios

		Frecuencia	Porcentaje
Válido	Nunca	1	2,3
	La mayoría veces no	8	18,6
	La mayoría veces si	17	39,5
	Siempre	17	39,5
	Total	1	2,3

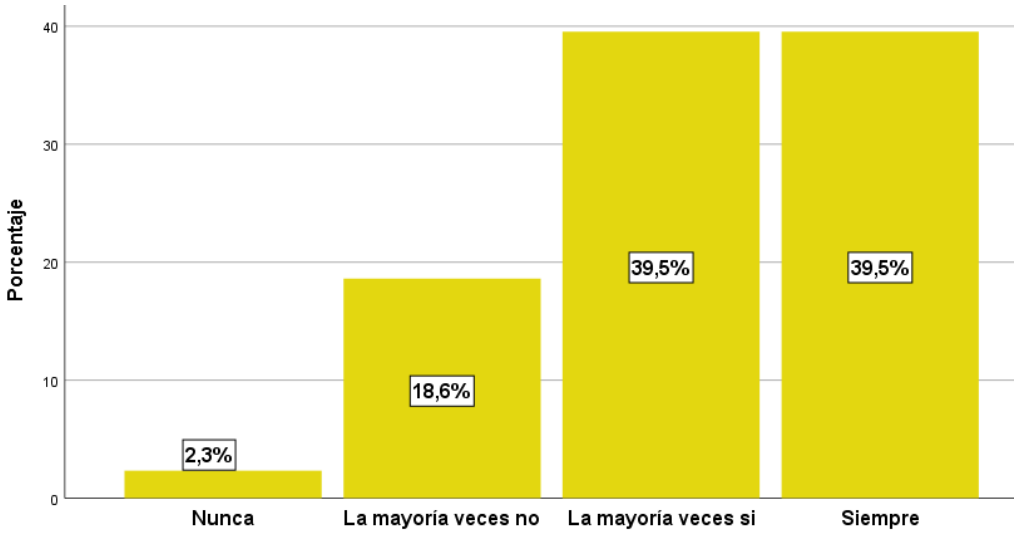


Figura 8. Nivel de percepción sobre la Central de detección y extinción de incendios

Interpretación:

En la Tabla 9 y Figura 8, se presenta el nivel de conocimiento sobre la **Central de detección y extinción de incendios** en las municipalidades de Lima Metropolitana. Se observó que el 39,9% que siempre tienen conocimiento, seguido por el otro 39,5% la mayoría de veces si tiene en cuenta, mientras el 18,6% la mayoría de veces no y solo el 2,3% respondieron nunca sobre la dimensión de la variable de estudios.

b) Dimensión: Planes de contingencia

Tabla 10.
Nivel de percepción sobre los Planes de contingencia

		Frecuencia	Porcentaje
Válido	Nunca	1	2,3
	La mayoría veces no	8	18,6
	La mayoría veces si	19	44,2
	Siempre	15	34,9
	Total	43	100,0

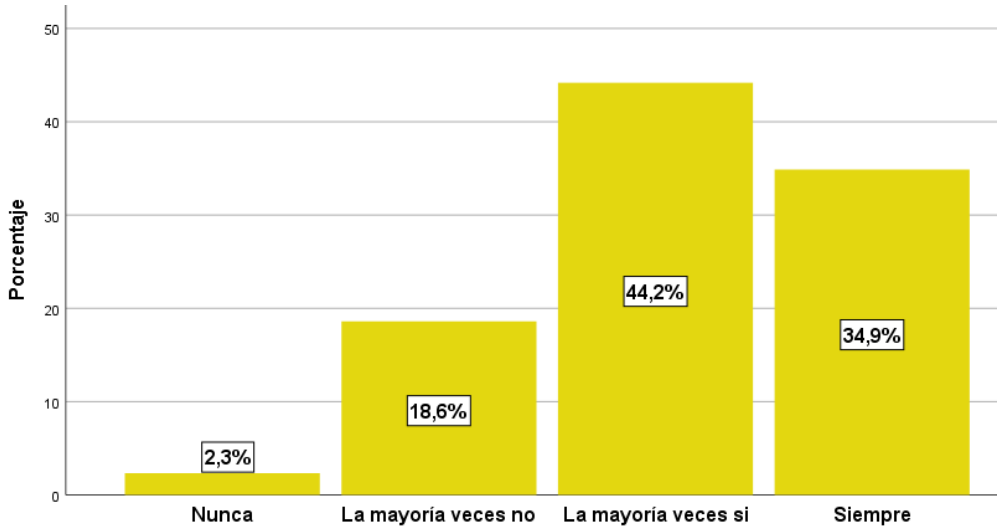


Figura 9. Nivel de percepción sobre los Planes de contingencia

Interpretación:

En la Tabla 10 y Figura 9, se presenta el nivel de conocimiento sobre los planes de contingencias en las municipalidades de Lima Metropolitana. Se observó que el 44,2% que la mayoría de veces si tienen conocimiento del plan, seguido por el 34,9% siempre, mientras el 18,6% la mayoría de veces no y solo el 2,3% respondieron nunca sobre la dimensión de la variable de estudios.

4.1.2. Análisis e interpretación de la variable "2": Data center.

Para evaluar la variable Data center, procedimos elaborar un instrumento de medición conformado por 10 ítems, dividido en dos partes en cada dimensión, recogiendo información referente a las dimensiones: Seguridad de la información y redes y las Normas de seguridad para infraestructura del Data Center, que son factores que influyen directamente en el Data center. Frente a cada pregunta del cuestionario, el entrevistado respondió las alternativas que le permitió evaluar en la escala de 1 a 5 de acuerdo al detalle siguiente:

Siempre = 5, La mayoría veces si = 4, A veces = 3, Mayoría veces no = 2 y Nunca = 1.

Tabla 11.
Norma de corrección sobre el Data center

Escala de Valores	Data Center	Factores sobre el Data center	
		Seguridad de la información y redes	Normas de seguridad para infraestructura del Data Center
	Rango	Rango	Rango
Siempre	41 – 50	21 - 25	21 - 25
La mayoría veces si	31 – 40	16 – 20	16 – 20
A veces	21 – 30	11 – 15	11 – 15
La mayoría veces no	11 – 20	06 – 10	06 – 10
Nunca	01 – 10	01 – 05	01 – 05

Una vez obtenido las puntuaciones para cada factor de la Data center se sumó las puntuaciones de cada factor para así poder dar una calificación general al cuestionario obteniéndose una puntuación mínima de 1 y una máxima de 50 de los valores en los niveles de medición.

Tabla 12.
Nivel de percepción sobre el Data center

		Frecuencia	Porcentaje
Válido	Nunca	1	2,3
	La mayoría veces no	7	16,3
	La mayoría veces si	9	20,9
	Siempre	26	60,5
	Total	43	100,0

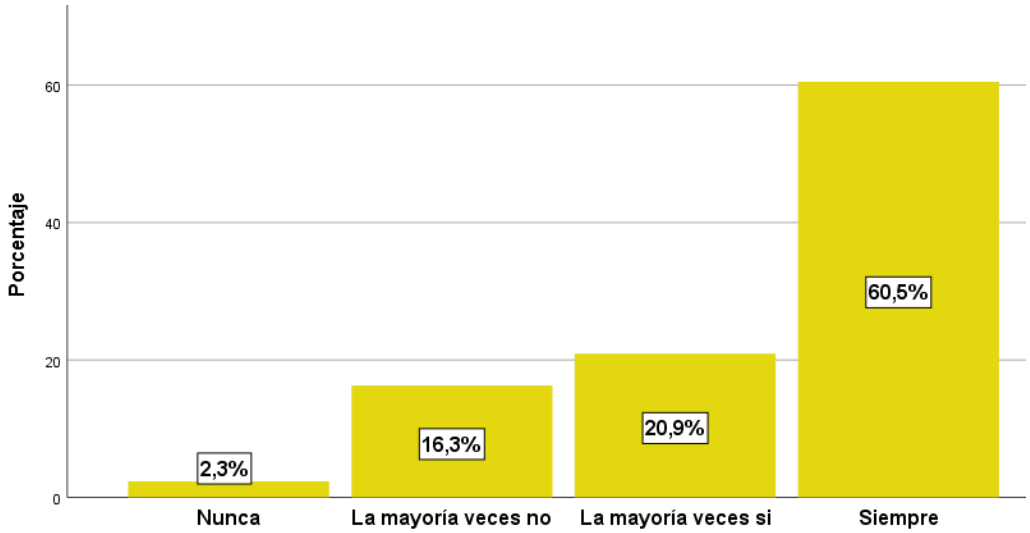


Figura 10. Nivel de percepción sobre el Data center

Interpretación:

En la Tabla 12 y Figura 10, se presenta el nivel de conocimiento sobre el data center implementadas en las municipalidades de Lima Metropolitana. Se observó que el 60,5% que siempre tienen conocimiento de la central de datos, seguido del 20,9% que la mayoría de veces si conocen, mientras el 16,3% la mayoría de veces no y solo el 2,3% respondieron nunca sobre la variable de estudios.

a) Dimensión: Seguridad de la información y redes

Tabla 13.
Nivel de percepción sobre la Seguridad de la información y redes

		Frecuencia	Porcentaje
Válido	Nunca	1	2,3
	La mayoría veces no	5	11,6
	La mayoría veces si	13	30,2
	Siempre	24	55,8
	Total	43	100,0

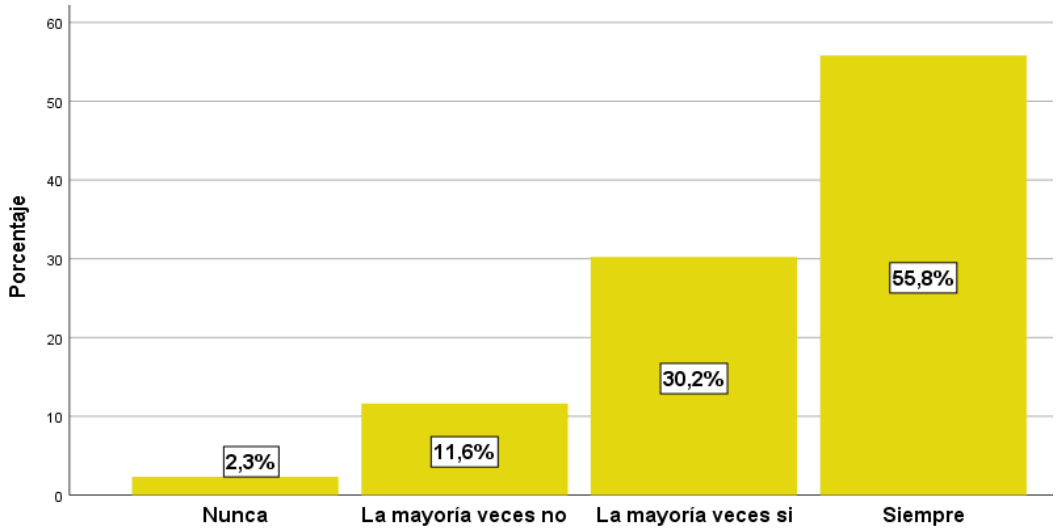


Figura 11. Nivel de percepción sobre la Seguridad de la información y redes

Interpretación:

En la Tabla 13 y Figura 11, se presenta el nivel de conocimiento sobre la Seguridad de la información y redes en las municipalidades de Lima Metropolitana. Se observó que el 55,8% que siempre tienen conocimiento de la seguridad de información implementada, seguido por el 30,2% de la mayoría de veces sí, mientras el 11,6% la mayoría de veces no y solo el 2,3% respondieron nunca sobre la dimensión de la variable de estudios.

b) Dimensión: Normas de seguridad para infraestructura del Data Center

Tabla 14.
Nivel de percepción sobre las Normas de seguridad para infraestructura

		Frecuencia	Porcentaje
Válido	Nunca	3	7,0
	La mayoría veces no	5	11,6
	La mayoría veces si	8	18,6
	Siempre	27	62,8
	Total	43	100,0

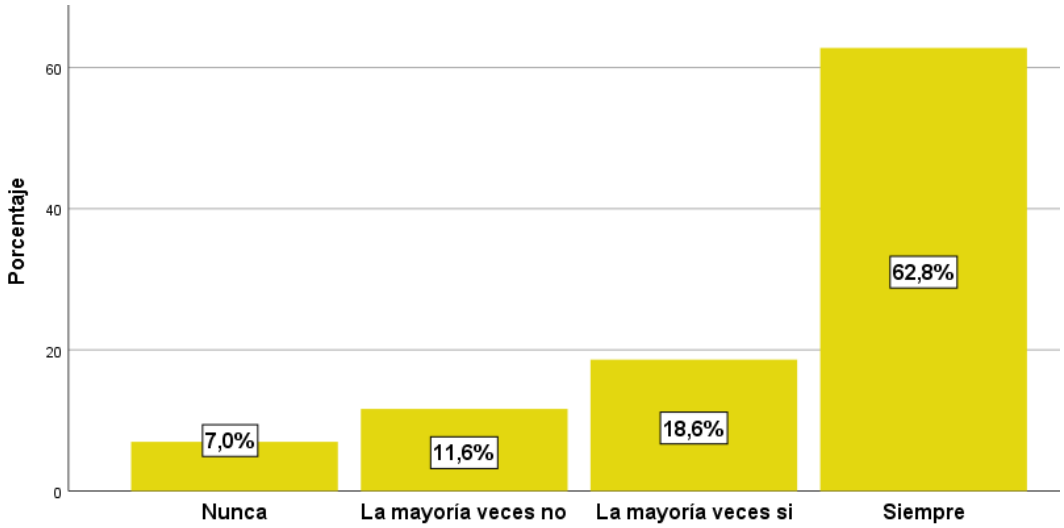


Figura 12. Nivel de percepción sobre las Normas de seguridad para infraestructura del Data Center

Interpretación:

En la Tabla 14 y Figura 12, se presenta el nivel de conocimiento sobre las normas de seguridad para infraestructura de la data center en las municipalidades de Lima Metropolitana. Se observó que el 62,8% que siempre tienen conocimiento de las normas de seguridad para infraestructura, seguido por el 18,6% de la mayoría de veces sí, mientras el 11,6% la mayoría de veces no y solo el 7,0% respondieron nunca sobre la dimensión de la variable de estudios.

4.1.3. Contrastación de las hipótesis.

Para el proceso de la contrastación de hipótesis, se ha determinado con el análisis no paramétrico, en vista que, la selección de la muestra es censal, igual que la población, por ende, no se realiza la prueba de normalidad. El nivel de medición de las variables es ordinal (no paramétrico), a través de la técnica no paramétrica de correlación Rho de Spearman.

Según Hernández y Mendoza, 2018 (p. 367) los coeficientes rho de Spearman, simbolizado como *rs,* son medidas de correlación o influencia para variables en un nivel de medición ordinal (ambas), de tal modo que los individuos, casos o unidades de análisis de la muestra pueden ordenarse por rangos (jerarquías). Son coeficientes utilizados para relacionar estadísticamente escalas tipo Likert.

Para establecer dicho grado de asociación se toma en cuenta la tabla de valoración de los “índices de correlación”, como se muestra en la tabla siguiente:

Tabla 15.
Índices de correlación para el Rho Spearman

Valor de Rho	Significado
-1.00	Correlación negativa grande y perfecta
-0.90 a -0.99	Correlación negativa muy alta
-0.70 a -0.89	Correlación negativa alta
-0.40 a -0.69	Correlación negativa moderada
-0.20 a -0.39	Correlación negativa baja
-0.01 a -0.19	Correlación negativa muy baja
0.00	Correlación nula
+0.01 a +0.19	Correlación positiva muy baja
+0.20 a +0.39	Correlación positiva baja
+0.50 a +0.69	Correlación positiva moderada
+0.70 a +0.89	Correlación positiva alta
+0.90 a +0.99	Correlación positiva muy alta
+1.00	Correlación positiva grande y perfecta

Nota: tomado de Martínez y Campos, (2015, p. 185).

Antes de aplicar la correlación de Rho de Spearman:

H_o (hipótesis nula) representa la afirmación de que no existe asociación o influencia entre las dos variables estudiadas.

H_a (hipótesis alternativa) afirma que hay algún grado de asociación o influencia entre las dos variables.

4.1.3.1. Prueba de la hipótesis general.

El diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

Hipótesis estadísticas:

H_o: Hipótesis nula ($r_{sxy} = 0$), El diseño del sistema de detección de incendios no se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

H_a: Hipótesis alterna: ($r_{sxy} \neq 0$), El diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

Nivel de significancia = 5% (0,05)

Regla de decisión: Si p valor < 0,05 entonces se procede a rechazar la H_o

Tabla 16.
Correlación de Rho Spearman entre el sistema de detección de incendios y la data center

				Sistema de detección de incendios	**Data center**
Rho de Spearman	Sistema de detección de incendios	Coeficiente de correlación		1,000	,756**
		Sig. (bilateral)		.	,000
		N		43	43
	Data center	Coeficiente de correlación		,756**	1,000
		Sig. (bilateral)		,000	.
		N		43	43

**. La correlación es significativa en el nivel 0,01 (bilateral).

Conclusión:

Se observa la Tabla 16, que el Coeficiente de correlación de Rho Spearman mostró una correlación positiva alta (rs=0,756) y la Significancia (Sig. bilateral), P-valor (p = 0.000 < 0.05), entre estas variables de estudios. Por lo tanto, se decidió rechazar la hipótesis nula (H_o) y aceptar la alterna (H_a); es decir, que: “El diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020”.

4.1.3.2. Prueba de las hipótesis específicas.

4.1.3.2.1. Hipótesis específica 1.

La central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

Hipótesis estadísticas:

H_o: Hipótesis nula: ($r_{sxy} = 0$), La central de detección y extinción de incendios no se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

H_a: Hipótesis alterna: ($r_{sxy} \neq 0$), La central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

Nivel de significancia = 5% (0,05)

Regla de decisión: Si p valor < 0,05 entonces se procede a rechazar la H_o

Tabla 17.
Correlación de Rho Spearman entre la central de detección y extinción de incendios y la data center

			Central de detección y extinción de incendios	**Data center**
Rho de Spearman	Central de detección y extinción de incendios	Coeficiente de correlación	1,000	,613**
		Sig. (bilateral)	.	,000
		N	43	43
	Data center	Coeficiente de correlación	,613**	1,000
		Sig. (bilateral)	,000	.
		N	43	43

**. La correlación es significativa en el nivel 0,01 (bilateral).

Conclusión:

Se observa la Tabla 17, que el Coeficiente de correlación de Rho Spearman mostró una correlación positiva moderada (rs=0,613) y la Significancia (Sig. bilateral), P-valor (p = 0.000 < 0.05), entre estas variables de estudios. Por lo tanto, se decidió rechazar la hipótesis nula (H_o) y aceptar la alterna (H_a); es decir, que: "La central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020".

4.1.3.2.2. Hipótesis específica 2.

Los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

Hipótesis estadísticas:

H_o: Hipótesis nula: (r_{sxy} = 0), Los planes de contingencia no se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

H_a: Hipótesis alterna: (r_{sxy} ≠ 0), Los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

Nivel de significancia = 5% (0,05)

Regla de decisión: Si p valor < 0,05 entonces se procede a rechazar la H_o

Tabla 18.

Correlación de Rho Spearman entre los planes de contingencia y la data center

			Planes de contingencia	**Data center**
Rho de Spearman	Planes de contingencia	Coeficiente de correlación	1,000	,624**
		Sig. (bilateral)	.	,000
		N	43	43
	Data center	Coeficiente de correlación	,624**	1,000
		Sig. (bilateral)	,000	.
		N	43	43

**. La correlación es significativa en el nivel 0,01 (bilateral).

Conclusión:

Se observa la Tabla 18, que el Coeficiente de correlación de Rho Spearman mostró una correlación positiva moderada (rs=0,624) y la Significancia (Sig. bilateral), P-valor (p = 0.000 < 0.05), entre estas variables de estudios. Por lo tanto, se decidió rechazar la hipótesis nula (H_o) y aceptar la alterna (H_a); es decir, que: “Los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020”.

V. DISCUSIÓN

5.1. Análisis de discusión de resultados

El objetivo de la presente investigación consistió en establecer la relación entre el sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020. En este sentido, realizado el trabajo de campo que consistió en la aplicación del instrumento de recolección de datos con el cuestionario debidamente validados por juicio de expertos y confiables, se obtuvo evidencia empírica para realizar la contrastación de las hipótesis de investigación.

- Con respecto al contraste de la hipótesis general, dio como resultado que, el diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, de acuerdo con el nivel de significancia de ,000 < 0,05 y el coeficiente rho de Spearman = 0,756 representando una correlación positiva alta.

Al respecto, Ruiz y Uribe (2019) en su investigación sobre el "Sistema de detección de incendios", determino que el proceso de adjudicación e implementación del sistema de detección de incendios en una subestación de distribución eléctrica viene cumpliendo la normatividad, con base a las especificaciones técnicas determinadas por la compañía, para la mejor solución del sistema de detección de incendios en las subestaciones eléctricas que permitiría proteger el sistema de equipamiento informático en toda las instalaciones de la empresa. Dicha investigación, permitió ahondar y profundizar que importante son la exigencia del cumplimiento de las normas para implementar acorde a las especificaciones técnicas, que trae relación el tema de estudio sobre el diseño del sistema de detección de incendios para optimización de la data center en las municipalidades de Lima Metropolitana, que permitiría proteger en una eventualidad de emergencia y amenaza, los cuales garantizaría la evacuación y salvaguardar la información activo importante de las gerencias de tecnologías.

Asimismo, Cárdenas (2017) en su investigación sobre el "Análisis de

arquitecturas modernas de Data Center", demostró que existen diferentes tipos de estándares que permiten una correcta implementación y funcionamiento de una data center, que pueden funcionar con estándares mínimas de temperaturas, humedad, seguridad, protección contra incendios y considerar evaluar el impacto ambiental, teniendo en cuenta el popular estándar TIA-942, que dispone de los patrones de diseño de redundancia para catalogar a una data center en TIERS. Asimismo, las nubes públicas proveen agilidad, escalabilidad, y alta disponibilidad para desplegar recursos IT de forma rápida. Dicha investigación es de suma importancia porque permitió analizar la implementación con estándares que se están tomando en cuenta en el presente estudio con el fin de optimizar la data center en las municipalidades de Lima Metropolitana, los cuales fueron de mucha relevancia ya que el 75,6% representa una correlación positiva alta para proceder con el diseño del sistema de detección de incendios para la protección de la data center en las gerencias de TI de las municipalidades.

- En lo que respecta al contraste de la hipótesis específica 1, dio como resultado que, la central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, de acuerdo con el nivel de significancia de ,000 < 0,05 y el coeficiente rho de Spearman = 0,613 representando una correlación significativa positiva moderada.

De igual manera, Castillo (2018) en su estudio sobre el "Modelo de optimización de recursos de un data center que brinda infraestructura como servicio (IAAS) de manera controlable y auditable a pymes de la provincia del Santa", demostró que, actualmente la infraestructura TI – servidores de las PYMES no cumplen con normas y buenas prácticas por la información recopilada y, por ende, ninguna satisface a los requerimientos de la gerencia de dichas empresas. En este contexto, la investigación contribuye como se debe tomar en cuenta para mejorar la optimización de la data center para una mejor administración de los servidores alineado a la seguridad de la información, priorizando la norma ANSI 942 que abarca la gestión y control de la data center y la norma ISO 27001 que permitirá garantizar que el servicio de Infraestructura como Servicio cuente con un buen sistema de gestión de seguridad de la información, que debe disponer la central de

detección y extinción de incendios para la optimización de la data center en las municipalidades de Lima Metropolitana.

De igual manera, Córdova, Fernández, Salgado y Soberón (2017) en su investigación sobre la “Dirección del proyecto: sistema de detección, alarma y extinción de incendios de planta Atocongo”, demostraron que, la finalización del proyecto en mención cumplirá con la normativa nacional vigente al inicio del proyecto y desarrollará las operaciones asegurando la integridad de todos los trabajadores y de los activos de la organización dando continuidad sostenible de las actividades operativas y comerciales. Dicho estudio contribuyó con la variable de estudio para ahondar sobre la central de detección y extinción de incendios para protección y optimización de la data center en las municipalidades de Lima Metropolitana, en vista que, el 61,3% de los encuestados manifestaron estar de acuerdo aplicar las normas y su aplicación.

- Con respecto al contraste de la hipótesis específica 2, dio como resultado que, los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, de acuerdo con el nivel de significancia de ,000 < 0,05 y el coeficiente rho de Spearman = 0,624 representando una correlación positiva moderada.

Al respecto, Idrovo (2017) en su investigación sobre el “Rediseño integral del sistema de protección contra incendios en un edificio multipropósito”, demostró que a través del Método Gretener y la evaluación sistemática, se logró identificar y evaluar el riesgo de incendio de la edificación, lo que permitirá en base al cumplimiento de la normativa legal aumentar el nivel de seguridad de la instalación, es decir, disponer de un plan de respuesta a emergencias equivale a disponer un plan de contingencia frente a cualquier eventualidad, los cuales contribuirá con asegurar la prevención y protección de la infraestructura de TI para optimización de la data center en las municipalidades de Lima Metropolitana.

Para Molano y Rodríguez (2017), en su estudio sobre el diseño del sistema contra incendios de extinción y detección permitió a través de las técnicas de cálculo por software computarizado agilizar el proceso de diseño y optimizar los tamaños de la red contra incendio. Esta investigación permitió sentar las bases con

el tema de estudio, en vista que, existe correlación positiva moderada entre los planes de contingencia y la optimización de la data center en las municipalidades de Lima Metropolitana, lo cual busca contribuir al cambio efectiva cuanto exista alguna emergencia para apagar incendios y por ende, mejorar la protección de la data center para el servicio a la ciudadanía.

En definitiva, podemos notar en los resultados de la correlación obtenida en cada prueba de hipótesis fue de positiva alta y moderada, esto es debido a que mayor gestión de diseño del sistema de detección de incendios mayor será la optimización de la data center en las municipalidades de Lima Metropolitana.

VI. CONCLUSIONES

A través de esta investigación se presenta la información para establecer la relación entre la central de detección y extinción de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020, a partir de ella se ha llegado a establecer las siguientes conclusiones:

1) Se estableció que, efectivamente el diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020; los resultados demuestran que el 48,8 % respondieron que la mayoría de veces, si tienen conocimiento de dicho sistema de detección de incendios implementadas en las áreas o departamentos de las gerencias tecnológicas; asimismo, el 60,5 % indicaron que siempre tienen conocimiento para la optimización de la data center para la toma de decisiones al disponer de información, referidas en las Tablas 6 y 10.

2) Se estableció que la central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020; donde los resultados demuestran que el 39.9% respondieron que siempre tienen conocimiento sobre la implementación de la central de detección y extinción de incendios; y el 60,5 % indicaron que siempre tienen conocimiento para la optimización de la data center al disponer de información en tiempo real en las municipalidades de Lima Metropolitana, referidas en las Tablas 7 y 10.

3) Se estableció que los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020; por lo tanto, los resultados demuestran que el 44,2% respondieron que la mayoría de veces, si tienen conocimiento del plan para poner en marcha ante cualquier emergencia; y el 60,5 % indicaron que siempre tienen conocimiento con el fin de optimizar la data center al disponer de información para brindar mejor servicio en la gestión pública en las municipalidades de Lima Metropolitana, referidas en las Tablas 8 y 10.

VII. RECOMENDACIONES

Las recomendaciones que se presentan están en relación con los resultados de la investigación:

1) Se recomienda al área de Gerencia de Tecnologías de Información de las municipalidades de Lima Metropolitana, desarrollar proyectos de mejora continua en diseño del sistema de detección de incendios para optimización de la data center, bajo lineamientos de la norma NFPA 72 (Código nacional de alarma y señalización contra incendios) que permitirá brindar seguridad y detección de incendios, señalización y comunicaciones de emergencia en la infraestructura de tecnologías de información; en vista que, la correlación obtenida entre las variables de estudios fue del 75.6% que los entrevistados percibieron sobre el diseño del sistema de detección de incendios y la optimización de la data center.

2) Se recomienda al área de Gerencia de Tecnologías de Información de las municipalidades de Lima Metropolitana, capacitar al personal sobre la operatividad del sistema electrónico encargado de la protección de la central de detección y extinción de incendios para dar una señal de alerta sobre algún evento de riesgo, a fin de reducir, prevenir asegurar y facilitar la protección de la infraestructura de la data center y la información histórica; en vista que, la correlación obtenida entre las variables fue del 61.3% que los entrevistados percibieron sobre la central de detección, extinción y la optimización de la data center.

3) Se recomienda al área de Gerencia de Tecnologías de Información de las municipalidades de Lima Metropolitana, promover la actualización de los planes de contingencia para establecer las políticas, los sistemas de organización, implementación de medidas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres y tecnológicos potencialmente dañinos, a fin de mantener la optimización de la data center que integra los sistemas de información y comunicación, que afecte alguno de sus servicios en la organización; en vista que, la correlación obtenida entre las variables de estudios fue del 62.4% que los entrevistados percibieron sobre los planes de contingencia y la optimización de la data center.

REFERENCIAS BIBLIOGRÁFICAS

Alcocer, A. (31 de marzo de 2010). *Cloud Computing. Características de las Aplicaciones en Cloud.* Recuperado de http://www.societic.com/2010/03/c

Benalcázar, A. (2017). *Arquitectura de un data center con herramientas DEVOPS*. Universidad Nacional De La Plata. Argentina.

Bernal, C. (2010). *Metodología de la Investigación*. Administración, economía, humanidades y ciencias sociales. Tercera Edición. Pearson Educación, Prentice Hall**.** Universidad de La Sabana, Colombia.

Cárdenas, S. E. (2017). *Análisis de arquitecturas modernas de Data Center* (Tesis para optar el Título de Ingeniero Civil en Informática). Universidad Técnica Federico Santa María, Valparaíso, Chile.

Castillo, G. J. (2018). *Modelo de optimización de recursos de un data center que brinda infraestructura como servicio (IAAS) de manera controlable y auditable a pymes de la provincia del santa* (Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas e Informática). Escuela de Posgrado de la Universidad Nacional del Santa, Chimbote, Perú.

Córdova, B. (2014). El informe de Investigación Cuantitativa. 1ra Ed. Editorial San Marcos E.I.R.L., editor Lima – Perú.

Córdova, D.C. (2012). *Data Center para mejorar la infraestructura de comunicación de datos en el departamento de sistemas informáticos y redes de comunicación (DISIR) de la Universidad Técnica de Ambato*.

Córdova, J., Fernández, I., Salgado, N., y Soberón, R. (2017). *Dirección del proyecto: sistema de detección, alarma y extinción de incendios de planta Atocongo* (Tesis para optar el grado académico de Administración y Dirección de Proyectos). Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú.

Decreto Supremo Nº 048-2011-PCM (26 mayo 2011). Que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD)

De la Fuente, S. (2011). *Análisis Factorial*. Facultad de Ciencias Económicas y Empresariales de la Universidad Autónoma de Madrid (UAM), España.

Edapi (2018). Detección y Extinción de Incendios. Infraestructura Data Center. https://www.edapi.cl/deteccion-y-extincion-de-incendios/

Escobar, J. J. (2015). *Diseño de Infraestructura de un Data Center TIER IV de acuerdo a las especificaciones técnicas de la norma TIA-942*. Pontificia Universidad Católica del Ecuador.

Espinoza Ortega, M. G. (2021), Estudio y diseño de un data center aplicando la norma ANSI/TIA 942 para ISP AZOTEL S.A. (Tesis de Maestría) Universidad Católica de Santiago de Guayaquil. Ecuador. Recuperado de: http://201.159.223.180/bitstream/3317/16622/1/T-UCSG-POS-MTEL-196.pdf

Esplugas, J. P. (2016). Guía para el diseño, uso y mantenimiento de los sistemas de detección automática de incendios. ASEPEYO.

González, J. A., y Vanegas, C. A. (2006). *La seguridad en las redes de comunicaciones*. Revista vínculos, *3*(1), 70-91.

Gutiérrez Olaya, H., & Valencia Ospina, A. (2006). Plan de manejo ambiental para la arenera el vínculo localizado en el municipio de Soacha (Cundinamarca) expediente Car Nº 2334.

Hernández, R. y Mendoza, C. P. (2018) *Metodología de la Investigación, Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana Editores, S.A. de C. V. Ciudad de México.

Hernández, R., Méndez, S., Mendoza, C. P. y Cuevas, A. (2017). Fundamentos de Investigación. Primera Edición. McGRAW-HILL Interamericana Editores, S.A. DE C.v. Ciudad de México.

Hernández, R., Fernández, C., Baptista, P. (2014). Metodología de la Investigación. 6ta Edición, McGRAW-HILL Interamericana Editores, S.A. DE C.V. México D.F, 2014, Pág. XXIV.

Idrovo, C. (2017). *Rediseño integral del sistema de protección contra incendios en un edificio multipropósito* (Tesis para optar el Título de Magister en Salud

Ocupacional y Seguridad en el Trabajo). Universidad del Alzuay, Cuenca, Ecuador.

INDECI (2018). Planes de contingencia. https://www.indeci.gob.pe/preparacion/planes/planes-de-contingencia/

ISO/IEC 27000. (2016). Information technology–Security techniques–Information security management systems–Overview and vocabulary. https://www.iso.org/standard/66435.html

ISO/IEC 27002 (en español) -Otros estándares de seguridad de la información: http://www.iso27000.es/iso27002.html

Jaramillo, C., Jácome, L., Ordóñez, Á., Gaona, M., Carrión, J., & Palma, M. (2017). Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja. *Maskana*, *8*, 149-162.

Larico, G. R. (2020). *Sistemas hiperconvergentes para mejorar la gestión tecnológica en centros de datos de la Universidad Nacional Amazónica de Madre De Dios* (Tesis para optar el grado académico de Doctor en Ingeniería de Sistemas). Escuela Universitaria de Posgrado, Universidad Nacional Federico Villareal.

Ley N° 28551 (19 junio 2005). Ley que establece la obligación de elaborar y presentar planes de contingencia.

Ley N° 29664 (18 febrero 2011). Que se crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

López, D. (2012). Data Center, Diseño Sostenible. BICSI Andino. 7 Congreso y Muestra Comercial.

Ministerio del Ambiente (2020). Plan de contingencia informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones.

Molano Pinzón, J. A. y Rodríguez Leguizamón, L. F. (2017), Diseño del sistema contra incendios de extinción y detección para la facultad tecnológica de la universidad distrital Francisco José De Caldas, conforme a la norma NFPA Y LA NSR-10. (Tesis de Pregrado). Universidad Distrital Francisco José

Caldas. Bogotá. Colombia. Recuperado de: https://repository.udistrital.edu.co/bitstream/handle/11349/6037/MolanoJeisonRodriguezLuis2017.pdf?sequence=1&isAllowed=y

Montaño Guerrero, R. A. y Bustíos Arteaga, J. L. J. (2020). Diseño de un data center con arquitectura convergente para optimizar los procesos informáticos de la municipalidad distrital de José Leonardo Ortiz. (Tesis de Pregrado). Escuela Profesional de Ingeniería Electrónica. Universidad Nacional Pedro Ruiz Gallo. Lambayeque. Perú. Recuperado de https://repositorio. unprg.edu.pe/bitstream/handle/20.500.12893/8862/Monta%C3%B1o_Guerrero_Richard_Alan_y_Bust%C3%ADos_Arteaga_Jorge_Luis_Jes%C3%BAs.pdf?sequence=1&isAllowed=y

Neira, J. A. (2008). Instalaciones de Protección contra Incendios. FC Editorial. España.

Norma UNE EN 54-1 23007 (2011). Sistemas de detección y alarma de incendio. Parte 1: Introducción.

NFPA 72, Código Nacional de Alarmas de Incendio y Señalización, Español.

Paltán, H. (2013). El desarrollo de estándares y procedimientos para la creación de un data center en la UPSE. Universidad Estatal Península De Santa Elena. Ecuador.

Parada, D., Flórez, A., y Gómez, U. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Información tecnológica, 29*(1), 27-38.

Peñaloza, M. (2015). Standard TIA-942. *Diseño y Cableado de un Centro de Datos.* Disponible de: "http://docplayer.es/960551-Standard-tia-942-diseno-y-cableado-de-un-centro-de-datos-disenar-en-base-a-estandares-y-mejores-practicas-temario.html"

Positiva Compañía de Seguros de Colombia (2015). Plan de Emergencia y Contingencias Instituto Distrital de Recreación y Deporte Bogotá D.C.

Polo, N. L. (2012). Diseño de un data center para el ISP READYNET CÍA.LTDA. Fundamento en la norma ANSI/TIA/EIA-942.Tesis de Pregrado, 203 pp. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional,

Quito, Ecuador.

Pracht, U., y Architektur, J. (2011). Meine oder deine Architektur? Von der Entwicklung zum Betrieb mit DevOps, 1–6. Disponible en: https://www.sigs-datacom.de/uploads/tx_dmjournals/pracht_OS_Architekturen_11.pdf

Ramírez, T. (2010). Como hacer un proyecto de investigación. (1º. Ed.). Caracas: Panapo.

Robinson, A. (2016). *InfoSec Reading Room Continuous Security: Implementing the Critical Controls in a DevOps Environmen*. Disponible en: https://www.sans.org/reading-room/whitepapers/critical/continuous-security-implementing-critical-controls-devops-environment-36552

Ruiz, J. E. y Uribe, M. C. (2019*). Sistema de detección de incendios* (Tesis para optar el Título de Especialista en Gerencia de Proyectos). Área de Posgrados de la Universidad Piloto de Colombia, Bogotá.

Soriano, M. (2014). *Seguridad en redes y seguridad de la información*. *Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad_de_ Red_e_ Informacion. pdf*.

Soto, A. J. y Mora, L. A. (2017). Diseño del plan de emergencias y contingencias para la PYME: Proyectos Integrales Sima S.A.S. Universidad Distrital Francisco José de Caldas. Bogotá, Colombia.

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., y Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36,* 100581.

Tecnologías emergentes para-Data Center. (7 de mayo, 2018). https://evaluandocloud.com/tecnologias-emergentes-data-center/

TIA 942 (2005). Telecommunications Infrastructure Standard for Data Centers. Editorial Telecommunications Industry Association

Uptime Institute (2015). *The Global Data Center Authority*. Disponible en: "https://es.uptimeinstitute.com/about-ui/global-authority"

Vega, E. (2021). Seguridad de la información. Editorial Área de Innovación y Desarrollo, S.L. Primera edición: marzo 2021. DOI: https://doi.org/10.17993/tics.2021.4

Wang, Q., Dunlap, T., Cho, Y., y Qu, G. (2017, April). DoS attacks and countermeasures on network devices. In *2017 26th Wireless and Optical Communication Conference (WOCC)* (pp. 1-6). IEEE.

Yrupailla Delgado, J. A. (2021), Planificación de un Data Center para la gestión de los servidores en el Operador Logístico JMA. (Tesis de Pregrado). Escuela Profesional de Ingeniería de Sistemas. Universidad César Vallejo. Lima. Perú. Recuperado de: https://repositorio.ucv.edu.pe/bitstream/ handle/ 20.500.12692/63995/Yrupailla_DJA-SD.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1. Matriz de consistencia

<table>
<tr><th colspan="5">SISTEMA DE DETECCIÓN DE INCENDIOS Y LA RELACIÓN CON LA OPTIMIZACIÓN DE LA DATA CENTER EN LAS MUNICIPALIDADES DE LIMA METROPOLITANA, 2020.</th></tr>
<tr><th>PROBLEMA GENERAL</th><th>OBJETIVO GENERAL</th><th>HIPÓTESIS GENERAL</th><th>VARIABLE</th><th>METODOLOGÍA</th></tr>
<tr><td>¿Qué relación existe entre el diseño del sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020?</td><td>Establecer la relación entre el sistema de detección de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.</td><td>Hi: El diseño del sistema de detección de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020, 2020.</td><td rowspan="4">Variable 1:
Sistema de detección de incendios

Dimensiones:
- Central de detección y extinción de incendios.
- Planes de contingencia.

Variable 2:
Data Center

Dimensiones:
- Seguridad de la información y redes.
- Normas de seguridad para infraestructura del Data Center</td><td rowspan="4">Tipo de investigación
Aplicada
Nivel de investigación
Correlacional
Diseño de investigación
No experimental de corte transversal
Población
43 gerencias de Tecnologías de Información
Muestra
Muestra censal
Técnica de recolección de datos
Encuesta
Instrumento de recolección de datos
Cuestionario</td></tr>
<tr><th>PROBLEMAS ESPECÍFICOS</th><th>OBJETIVOS ESPECÍFICOS</th><th>HIPÓTESIS ESPECÍFICAS</th></tr>
<tr><td>¿Qué relación existe entre la central de detección y extinción de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020?</td><td>Establecer la relación entre la central de detección y extinción de incendios y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.</td><td>H1: La central de detección y extinción de incendios se relaciona significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.</td></tr>
<tr><td>¿Qué relación existe entre los planes de contingencia y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020?</td><td>Establecer la relación entre los planes de contingencia y la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.</td><td>H2: Los planes de contingencia se relacionan significativamente con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.</td></tr>
</table>

Anexo 2. Matriz de operacionalización de variables

VARIABLE	DIMENSIONES	INDICADORES	REDACCION DE ITEMS	TIPO DE INSTRUMENTO	ESCALA DE MEDICION
V1: Sistema de detección de incendios	**Dimensión:** Central de detección y extinción de incendios	Capacidad de respuesta Rapidez y la fiabilidad Estrategias Equipo de control y señalización Agentes limpios	1. ¿Las Municipalidades distritales de Lima Metropolitana cuentan con capacidad de respuesta a través de un sistema de detección y extinción de incendios? 2. ¿El personal de las Gerencias de Tecnologías de Información se encuentra capacitado para valorar el sistema de detección y extensión de incendios con rapidez y fiabilidad en la detección de emergencias? 3. ¿En las instalaciones de las Municipalidades distritales de Lima Metropolitana se implementa estrategias para la detección, alarma y comunicación ante una emergencia de incendio desde una central de control de operaciones? 4. ¿Se encuentran en buen estado las instalaciones eléctricas y el equipo de control y señalización el sistema de detección y extinción de incendios en las municipalidades? 5. ¿En las instalaciones eléctricas el sistema de extinción de incendios con agentes limpios, cumple con las normas NFPA 2100 para preserva la vida de las personas?	Cuestionario	1) Nunca 2) La mayoría de las veces no 3) A veces 4) La mayoría de veces si 5) Siempre

	Dimensión: Planes de contingencia	Instrumentos de gestión Procedimientos específicos Planeamiento Plan de contingencia informático Plan contra incendios	6. ¿Las gerencias de tecnologías de información viabilizan los instrumentos de gestión para establecer los objetivos, estrategias y programas que orientan las actividades para la prevención, la reducción de riesgos y la atención en casos de desastres y emergencias? 7. ¿Considera Ud., que los planes de contingencias son procedimientos específicos prestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento de escenarios prestablecidos? 8. ¿Las gerencias de tecnologías de información conoce los procedimientos de la Ley 29664 como un instrumento técnico de planeamiento especifico y gestión obligatoria, cuyo propósito es proteger la vida humana y el patrimonio? 9. ¿Las gerencias de tecnologías de información actualizan permanentemente el plan de contingencia informático para dar seguridad a la información y proteger el equipamiento informático? 10. ¿Existe un plan contra incendios para la gestión de la Brigada contra Incendios y el control de incendios y emergencias asociadas a los riesgos y amenazas en las en las municipalidades distritales?	Cuestionario	1) Nunca 2) La mayoría de las veces no 3) A veces 4) La mayoría de veces si 5) Siempre

VARIABLE	DIMENSIONES	INDICADORES	REDACCION DE ITEMS	TIPO DE INSTRUMENTO	ESCALA DE MEDICION
V2: Data Center	**Dimensión:** Seguridad de la información y redes	Buenas prácticas y metodologías Confidencialidad Integridad Disponibilidad Políticas de seguridad	11. ¿En caso de corte de energía eléctrica se dispone de los equipos para proteger los servidores como parte de las buenas prácticas y metodologías que busquen proteger la información y los sistemas de información? 12. ¿Se realiza respaldos frecuentes de los archivos para garantizar la confidencialidad de la información accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación? 13. ¿Las gerencias de tecnologías de información implementan las seguridades informáticas que aseguraría la integridad y los recursos sean modificados por quienes están autorizados para gestionar los sistemas de información? 14. ¿Las gerencias de tecnologías de información cuenta políticas de cambio de contraseñas para disponibilidad de acceder a los datos cuando sea solicitado por la gestión municipal oportunamente? 15. ¿Existe lineamientos y formas de comunicación con los usuarios para el cumplimiento de un manual de políticas de seguridad que permitiría optimizar las tareas informáticas?	Cuestionario	1) Nunca 2) La mayoría de las veces no 3) A veces 4) La mayoría de veces si 5) Siempre

	Dimensión: Normas de seguridad para infraestructura del Data Center	Infraestructura física y tecnológica Estándar especifica Guía de diseño Estándar ANSI/TIA/EIA 942 Norma ISO/IEC 27002	1) ¿La implementación de un Data Center con infraestructura física y tecnológica adecuada, garantiza el manejo de forma centralizada la información de toda la institución para la toma de decisiones? 2) ¿Considera Ud., que el uso de normas y estándares específicas para el Data Center permitirá una gestión efectiva de la seguridad de información, de los recursos y datos en las municipalidades distritales? 3) ¿Considera Ud., que disponer de una guía de diseño para infraestructura de TI garantiza la planificación de las instalaciones, el sistema de cableado, y el diseño de la red en la implementación de la Data Center? 4) ¿Las gerencias de tecnologías de información tienen sobre el Estándar ANSI/TIA/EIA 942 como norma para proporcionar requisitos y directrices para el diseño y la instalación de un centro de datos o sala de ordenadores? 5) ¿Es de conocimiento de las gerencias de tecnologías de información sobre la Norma ISO/IEC 27002, que viabiliza como guía de buenas prácticas para la seguridad de la información en las municipalidades distritales?	Cuestionario	1) Nunca 2) La mayoría de las veces no 3) A veces 4) La mayoría de veces si 5) Siempre

Anexo 3. Instrumentos para la recolección de datos

Encuesta a los gerentes de tecnologías de información con respecto al Diseño del sistema de detección de incendios para optimización de la data center en las municipalidades de Lima Metropolitana, 2020.

CUESTIONARIO

Estimado participante, a continuación, te presento un cuestionario relacionado sobre la *"*Sistema de detección de incendios y la relación con la optimización de la data center en las municipalidades de Lima Metropolitana, 2020.*",* tu respuesta es sumamente relevante; por ello debes leerlo en forma detallada y, luego, marcar una de las cinco alternativas.

RESPONDA A LAS SIGUIENTES PREGUNTAS SEGÚN SU CRITERIO, MARQUE CON UNA "X" EN LA ALTERNATIVA QUE CORRESPONDA:

Nunca	La mayoría de las veces no	A veces	La mayoría de las veces si	Siempre
01	02	03	04	05

N º	VARIABLES / DIMENSIONES	01	02	03	04	05
VARIABLE SISTEMA DE DETECCIÓN DE INCENDIOS						
	Dimensión Central de detección y extinción de incendios					
1	¿Las Municipalidades distritales de Lima Metropolitana cuentan con capacidad de respuesta a través de un sistema de detección y extinción de incendios?					
2	¿El personal de las Gerencias de Tecnologías de Información se encuentra capacitado para valorar el sistema de detección y extensión de incendios con rapidez y fiabilidad en la detección de emergencias?					
3	¿En las instalaciones de las Municipalidades distritales de Lima Metropolitana se implementa estrategias para la detección, alarma y comunicación ante una emergencia de incendio desde una central de control de operaciones?					
4	¿Se encuentran en buen estado las instalaciones eléctricas y el equipo de control y señalización el sistema de detección y extinción de incendios en las municipalidades?					
5	¿En las instalaciones eléctricas el sistema de extinción de incendios con agentes limpios cumple con las normas NFPA 2100 para preserva la vida de las personas?					
	Dimensión Planes de contingencia					
6	¿Las gerencias de tecnologías de información viabilizan los instrumentos de gestión para establecer los objetivos, estrategias y programas que orientan las actividades para la prevención, la reducción de riesgos y la atención en casos de desastres y emergencias?					
7	¿Considera Ud., que los planes de contingencias son procedimientos específicos prestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento de escenarios prestablecidos?					

8	¿Las gerencias de tecnologías de información conoce los procedimientos de la Ley 29664 como un instrumento técnico de planeamiento especifico y gestión obligatoria, cuyo propósito es proteger la vida humana y el patrimonio?					
9	¿Las gerencias de tecnologías de información actualizan permanentemente el plan de contingencia informático para dar seguridad a la información y proteger el equipamiento informático?					
10	¿Existe un plan contra incendios para la gestión de la Brigada contra Incendios y el control de incendios y emergencias asociadas a los riesgos y amenazas en las en las municipalidades distritales?					
VARIABLE DATA CENTER						
	Dimensión Seguridad de la información y redes					
11	¿En caso de corte de energía eléctrica se dispone de los equipos para proteger los servidores como parte de las buenas prácticas y metodologías que busquen proteger la información y los sistemas de información?					
12	¿Se realiza respaldos frecuentes de los archivos para garantizar la confidencialidad de la información accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación?					
13	¿Las gerencias de tecnologías de información implementan las seguridades informáticas que aseguraría la integridad y los recursos sean modificados por quienes están autorizados para gestionar los sistemas de información?					
14	¿Las gerencias de tecnologías de información cuenta políticas de cambio de contraseñas para disponibilidad de acceder a los datos cuando sea solicitado por la gestión municipal oportunamente?					
15	¿Existe lineamientos y formas de comunicación con los usuarios para el cumplimiento de un manual de políticas de seguridad que permitiría optimizar las tareas informáticas?					
	Dimensión Normas de seguridad para infraestructura del Data Center					
16	¿La implementación de un Data Center con infraestructura física y tecnológica adecuada, garantiza el manejo de forma centralizada la información de toda la institución para la toma de decisiones?					
17	¿Considera Ud., que el uso de normas y estándares específicas para el Data Center permitirá una gestión efectiva de la seguridad de información, de los recursos y datos en las municipalidades distritales?					
18	¿Considera Ud., que disponer de una guía de diseño para infraestructura de TI garantiza la planificación de las instalaciones, el sistema de cableado, y el diseño de la red en la implementación de la Data Center?					
19	¿Las gerencias de tecnologías de información tienen sobre el Estándar ANSI/TIA/EIA 942 como norma para proporcionar requisitos y directrices para el diseño y la instalación de un centro de datos o sala de ordenadores?					
20	¿Es de conocimiento de las gerencias de tecnologías de información sobre la Norma ISO/IEC 27002, que viabiliza como guía de buenas prácticas para la seguridad de la información en las municipalidades distritales?					

Anexo 4. Validación de instrumento

N°	Dimensiones/ítems VARIABLE 1: SISTEMA DE DETECCIÓN DE INCENDIOS Dimensión: Central de detección y extinción de incendios	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		SI	NO	SI	NO	SI	NO	
1	¿Las Municipalidades distritales de Lima Metropolitana cuentan con capacidad de respuesta a través de un sistema de detección y extinción de incendios?	X		X		X		
2	¿El personal de las Gerencias de Tecnologías de Información se encuentra capacitado para valorar el sistema de detección y extensión de incendios con rapidez y fiabilidad en la detección de emergencias?	X		X		X		
3	¿En las instalaciones de las Municipalidades distritales de Lima Metropolitana se implementa estrategias para la detección, alarma y comunicación ante una emergencia de incendio desde una central de control de operaciones?	X		X		X		
4	¿Se encuentran en buen estado las instalaciones eléctricas y el equipo de control y señalización el sistema de detección y extinción de incendios en las municipalidades?	X		X		X		
5	¿En las instalaciones eléctricas el sistema de extinción de incendios con agentes limpios cumple con las normas NFPA 2100 para preserva la vida de las personas?	X		X		X		
	Dimensión: Planes de contingencia							
6	¿Las gerencias de tecnologías de información viabilizan los instrumentos de gestión para establecer los objetivos, estrategias y programas que orientan las actividades para la prevención, la reducción de riesgos y la atención en casos de desastres y emergencias?	X		X		X		
7	¿Considera Ud., que los planes de contingencias son procedimientos específicos prestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento de escenarios prestablecidos?	X		X		X		
8	¿Las gerencias de tecnologías de información conoce los procedimientos de la Ley 29664 como un instrumento técnico de planeamiento especifico y gestión obligatoria, cuyo propósito es proteger la vida humana y el patrimonio?	X		X		X		
9	¿Las gerencias de tecnologías de información actualizan permanentemente el plan de contingencia informático para dar seguridad a la información y proteger el equipamiento informático?	X		X		X		
10	¿Existe un plan contra incendios para la gestión de la Brigada contra Incendios y el control de incendios y emergencias asociadas a los riesgos y amenazas en las en las municipalidades distritales?	X		X		X		

N°	Dimensiones/ítems VARIABLE 2: DATA CENTER Dimensión: Seguridad de la información y redes	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		SI	NO	SI	NO	SI	NO	
11	¿En caso de corte de energía eléctrica se dispone de los equipos para proteger los servidores como parte de las buenas prácticas y metodologías que busquen proteger la información y los sistemas de información?	X		X		X		
12	¿Se realiza respaldos frecuentes de los archivos para garantizar la confidencialidad de la información accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación?	X		X		X		
13	¿Las gerencias de tecnologías de información implementan las seguridades informáticas que aseguraría la integridad y los recursos sean modificados por quienes están autorizados para gestionar los sistemas de información?	X		X		X		
14	¿Las gerencias de tecnologías de información cuenta políticas de cambio de contraseñas para disponibilidad de acceder a los datos cuando sea solicitado por la gestión municipal oportunamente?	X		X		X		
15	¿Existe lineamientos y formas de comunicación con los usuarios para el cumplimiento de un manual de políticas de seguridad que permitiría optimizar las tareas informáticas?	X		X		X		
	Dimensión: Normas de seguridad para infraestructura del Data Center							
16	¿La implementación de un Data Center con infraestructura física y tecnológica adecuada, garantiza el manejo de forma centralizada la información de toda la institución para la toma de decisiones?	X		X		X		
17	¿Considera Ud., que el uso de normas y estándares específicas para el Data Center permitirá una gestión efectiva de la seguridad de información, de los recursos y datos en las municipalidades distritales?	X		X		X		
18	¿Considera Ud., que disponer de una guía de diseño para infraestructura de TI garantiza la planificación de las instalaciones, el sistema de cableado, y el diseño de la red en la implementación de la Data Center?	X		X		X		
19	¿Las gerencias de tecnologías de información tienen sobre el Estándar ANSI/TIA/EIA 942 como norma para proporcionar requisitos y directrices para el diseño y la instalación de un centro de datos o sala de ordenadores?	X		X		X		
20	¿Es de conocimiento de las gerencias de tecnologías de información sobre la Norma ISO/IEC 27002, que viabiliza como guía de buenas prácticas para la seguridad de la información en las municipalidades distritales?	X		X		X		

Observaciones (precisar si hay suficiencia): **HAY SUFICIENCIA**

Opinión de aplicabilidad: Aplicable **(X)** Aplicable después de corregir ( ) No aplicable ( )

Apellidos y nombres del juez validador.

Mg. RAÚL GUALBERTO QUISPE TAYA

DNI: **08086028**

Especialidad del validador:

MAESTRO EN DOCENCIA UNIVERSITARIA

1 Pertinencia: El ítem corresponde al concepto teórico

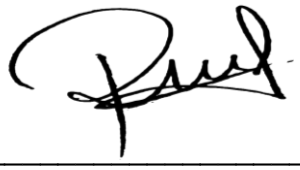
formulado:

2 Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

3 Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

18 de febrero del 2022



MG. RAUL GUALBERTO QUISPE TAYA

08086028

N°	Dimensiones/ítems VARIABLE 1: SISTEMA DE DETECCIÓN DE INCENDIOS Dimensión: Central de detección y extinción de incendios	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		SI	NO	SI	NO	SI	NO	
1	¿Las Municipalidades distritales de Lima Metropolitana cuentan con capacidad de respuesta a través de un sistema de detección y extinción de incendios?	X		X		X		
2	¿El personal de las Gerencias de Tecnologías de Información se encuentra capacitado para valorar el sistema de detección y extensión de incendios con rapidez y fiabilidad en la detección de emergencias?	X		X		X		
3	¿En las instalaciones de las Municipalidades distritales de Lima Metropolitana se implementa estrategias para la detección, alarma y comunicación ante una emergencia de incendio desde una central de control de operaciones?	X		X		X		
4	¿Se encuentran en buen estado las instalaciones eléctricas y el equipo de control y señalización el sistema de detección y extinción de incendios en las municipalidades?	X		X		X		
5	¿En las instalaciones eléctricas el sistema de extinción de incendios con agentes limpios cumple con las normas NFPA 2100 para preserva la vida de las personas?	X		X		X		
	Dimensión: Planes de contingencia							
6	¿Las gerencias de tecnologías de información viabilizan los instrumentos de gestión para establecer los objetivos, estrategias y programas que orientan las actividades para la prevención, la reducción de riesgos y la atención en casos de desastres y emergencias?	X		X		X		
7	¿Considera Ud., que los planes de contingencias son procedimientos específicos prestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento de escenarios prestablecidos?	X		X		X		
8	¿Las gerencias de tecnologías de información conoce los procedimientos de la Ley 29664 como un instrumento técnico de planeamiento especifico y gestión obligatoria, cuyo propósito es proteger la vida humana y el patrimonio?	X		X		X		
9	¿Las gerencias de tecnologías de información actualizan permanentemente el plan de contingencia informático para dar seguridad a la información y proteger el equipamiento informático?	X		X		X		
10	¿Existe un plan contra incendios para la gestión de la Brigada contra Incendios y el control de incendios y emergencias asociadas a los riesgos y amenazas en las en las municipalidades distritales?	X		X		X		

N°	Dimensiones/ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
	VARIABLE 1: DATA CENTER							
	Dimensión: Seguridad de la información y redes	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	
11	¿En caso de corte de energía eléctrica se dispone de los equipos para proteger los servidores como parte de las buenas prácticas y metodologías que busquen proteger la información y los sistemas de información?	X		X		X		
12	¿Se realiza respaldos frecuentes de los archivos para garantizar la confidencialidad de la información accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación?	X		X		X		
13	¿Las gerencias de tecnologías de información implementan las seguridades informáticas que aseguraría la integridad y los recursos sean modificados por quienes están autorizados para gestionar los sistemas de información?	X		X		X		
14	¿Las gerencias de tecnologías de información cuenta políticas de cambio de contraseñas para disponibilidad de acceder a los datos cuando sea solicitado por la gestión municipal oportunamente?	X		X		X		
15	¿Existe lineamientos y formas de comunicación con los usuarios para el cumplimiento de un manual de políticas de seguridad que permitiría optimizar las tareas informáticas?	X		X		X		
	Dimensión: Normas de seguridad para infraestructura del Data Center							
16	¿La implementación de un Data Center con infraestructura física y tecnológica adecuada, garantiza el manejo de forma centralizada la información de toda la institución para la toma de decisiones?	X		X		X		
17	¿Considera Ud., que el uso de normas y estándares específicas para el Data Center permitirá una gestión efectiva de la seguridad de información, de los recursos y datos en las municipalidades distritales?	X		X		X		
18	¿Considera Ud., que disponer de una guía de diseño para infraestructura de TI garantiza la planificación de las instalaciones, el sistema de cableado, y el diseño de la red en la implementación de la Data Center?	X		X		X		
19	¿Las gerencias de tecnologías de información tienen sobre el Estándar ANSI/TIA/EIA 942 como norma para proporcionar requisitos y directrices para el diseño y la instalación de un centro de datos o sala de ordenadores?	X		X		X		
20	¿Es de conocimiento de las gerencias de tecnologías de información sobre la Norma ISO/IEC 27002, que viabiliza como guía de buenas prácticas para la seguridad de la información en las municipalidades distritales?	X		X		X		

Observaciones (precisar si hay suficiencia): **HAY SUFICIENCIA**

Opinión de aplicabilidad: Aplicable **(X)** Aplicable después de corregir ( ) No aplicable ( )

Apellidos y nombres del juez validador.

DR. ANGEL NOÉ QUISPE TALLA

DNI:

Especialidad del validador:

DOCTOR EN CIENCIAS DE LA EDUCACIÓN

1 Pertinencia: El ítem corresponde al concepto teórico

formulado:

2 Relevancia: El ítem es apropiado para representar al componente o dimensión especifica del constructo

3 Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

09 de marzo del 2022

DR ANGEL NOÉ QUISPE TALLA

Anexo 5. Matriz de datos

N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
1	4	4	4	4	4	4	4	4	2	4	5	4	3	4	4	4	4	4	4	4
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	3	2	3	3	2	2	2	2	3	4	2	3	1	1	2	2	4	3	3	3
4	3	4	4	4	3	4	3	4	3	4	4	4	4	4	4	4	4	4	4	4
5	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	3
6	4	3	4	4	3	3	2	3	3	5	5	5	5	5	4	4	4	4	4	4
7	2	2	2	4	2	2	2	4	4	2	4	4	2	4	2	4	4	4	4	4
8	4	3	4	3	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4
9	4	3	2	3	4	2	2	4	1	4	4	1	3	4	1	4	1	4	4	5
10	4	4	4	2	2	4	2	2	2	4	4	4	4	4	4	4	4	4	4	4
11	2	2	3	3	1	2	1	3	1	2	3	4	2	1	1	1	1	1	1	1
12	4	4	4	4	5	4	4	5	3	1	4	4	5	4	4	5	4	1	4	4
13	4	4	4	4	4	4	4	4	2	4	5	4	3	4	4	4	2	4	4	4
14	1	1	3	1	1	3	1	1	1	1	3	1	1	3	1	1	1	1	3	1
15	3	2	2	2	2	3	3	3	3	2	3	4	2	4	3	4	3	2	3	4
16	2	4	2	3	2	2	3	4	4	2	4	4	1	4	2	4	4	4	4	3
17	4	3	2	3	5	2	2	4	1	4	4	1	3	2	1	4	1	1	4	5
18	4	5	4	1	2	1	2	2	2	3	4	4	1	4	4	4	3	4	4	4
19	4	2	2	3	5	2	1	3	1	2	3	5	2	1	1	1	1	1	1	1
20	2	2	3	1	1	1	1	5	3	3	3	2	2	1	3	1	2	1	1	4
21	1	3	3	4	3	4	4	4	3	4	4	5	5	4	2	4	4	1	3	4
22	3	1	3	3	3	3	3	3	1	3	3	3	2	3	3	3	3	2	3	3
23	2	2	2	2	2	2	2	5	2	2	2	3	2	4	2	2	2	4	4	5
24	2	2	2	1	4	3	4	3	3	3	5	3	4	4	3	4	3	3	4	3
25	4	3	2	4	3	3	2	4	3	4	4	5	5	5	2	5	4	3	2	4

Prueba Piloto

Base de datos (variables de estudios)

N°	Sistema de detección de incendios										Data center									
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
1	4	4	4	4	4	4	4	4	2	4	5	4	3	4	4	4	4	4	4	4
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	3	2	2	2	2	3	3	3	3	4	3	4	4	4	3	4	3	3	3	4
4	1	2	1	1	1	2	2	2	1	2	3	2	2	1	1	1	1	2	2	1
5	2	2	2	1	1	1	1	2	3	1	3	2	2	1	2	1	2	1	1	1
6	4	3	3	4	3	4	2	4	3	4	4	5	5	5	2	4	4	1	2	4
7	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
8	2	2	2	2	2	2	2	2	2	2	2	4	2	4	2	2	4	4	4	4
9	2	2	2	2	4	3	3	3	3	3	3	3	4	4	3	4	3	3	3	3
10	3	4	4	4	3	4	3	4	3	4	4	4	4	4	4	4	4	4	4	4
11	3	2	3	3	2	2	2	2	3	4	2	3	1	1	2	2	4	3	3	3
12	3	4	4	4	3	4	3	4	3	4	4	4	4	4	4	4	4	4	4	4
13	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	3
14	4	3	4	4	3	3	2	3	3	5	5	5	5	5	4	4	4	4	4	4
15	2	2	2	4	2	2	2	4	4	2	4	4	2	4	2	4	4	4	4	4
16	4	3	4	3	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4
17	4	3	2	3	4	2	2	4	1	4	4	1	3	4	1	4	1	4	4	5
18	4	4	4	2	2	4	2	2	2	4	4	4	4	4	4	4	4	4	4	4
19	2	2	3	3	1	2	1	3	1	2	3	4	2	1	1	1	1	1	1	1
20	4	4	4	4	5	4	4	5	3	1	4	4	5	4	4	5	4	1	4	4
21	4	4	4	4	4	4	4	4	2	4	5	4	3	4	4	4	2	4	4	4
22	1	1	3	1	1	3	1	1	1	1	3	1	1	3	1	1	1	1	3	1
23	3	2	2	2	2	3	3	3	3	2	3	4	2	4	3	4	3	2	3	4
24	4	2	5	1	1	1	5	2	5	1	5	2	2	1	2	1	2	2	1	1
25	4	3	3	4	3	4	2	4	3	4	4	5	2	5	2	3	1	1	2	4
26	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	4
27	1	2	2	2	2	2	2	2	2	2	4	4	2	5	2	3	4	4	4	4
28	2	2	1	2	1	3	3	1	3	5	3	3	4	4	4	4	3	3	3	3
29	3	4	2	4	3	4	3	4	2	4	2	4	4	4	4	4	1	4	4	4
30	2	2	3	3	3	2	2	3	3	1	2	3	1	1	2	2	4	3	3	3
31	3	4	4	2	3	4	4	4	3	4	2	4	4	4	4	4	4	2	4	4
32	4	3	1	3	3	5	3	3	3	1	3	3	3	3	3	3	1	4	4	3
33	4	3	4	4	4	3	2	4	3	5	5	5	5	2	4	4	4	4	4	4
34	2	4	2	3	2	2	3	4	4	2	4	4	1	4	2	4	4	4	4	3
35	4	3	2	3	5	2	2	4	1	4	4	1	3	2	1	4	1	1	4	5
36	4	5	4	1	2	1	2	2	2	3	4	4	1	4	4	4	3	4	4	4
37	4	2	2	3	5	2	1	3	1	2	3	5	2	1	1	1	1	1	1	1
38	2	2	3	1	1	1	1	5	3	3	3	2	2	1	3	1	2	1	1	4
39	1	3	3	4	3	4	4	4	3	4	4	5	5	4	2	4	4	1	3	4
40	3	1	3	3	3	3	3	3	1	3	3	3	2	3	3	3	3	2	3	3
41	2	2	2	2	2	2	2	5	2	2	2	3	2	4	2	2	2	4	4	5
42	2	2	2	1	4	3	4	3	3	3	5	3	4	4	3	4	3	3	4	3
43	4	3	2	4	3	3	2	4	3	4	4	5	5	5	2	5	4	3	2	4

Anexo 6. Propuesta de valor

SISTEMA DETECCIÓN Y ALARMA CONTRA INCENDIO

MANUAL DE OPERACIÓN DEL PANEL DETECCIÓN

ÍNDICE

1. INTRODUCCIÓN

Los sistemas de detección y alarma de incendios ayudan a proteger la vida de los colaboradores y las instalaciones del cliente, por ello es necesario conocer los componentes y el funcionamiento del sistema instalado.

2. OBJETIVO

Este manual de operación está diseñado como referencia diaria para los usuarios del sistema, el objetivo principal es que el usuario conozca los componentes del sistema y el reconocimiento de las alarmas del mismo.

3. COMPONENTES DEL SISTEMA DE DETECCIÓN Y ALARMA DE INCENDIOS

- El sistema de detección y alarma de incendios está compuesto por los siguientes equipos:
- detectores de Humo.
- detector de Temperatura
- sensores de Aniego.
- estaciones Manuales.
- módulos de Monitoreo.
- módulo de Control.
- sirenas con luces estroboscópicas.

4. DESCRIPCIÓN DEL SISTEMA.

- El Panel de control de alarma contra incendios (FACP) tiene tres funciones generales.
- Monitorea los dispositivos de iniciación de alarma de incendio (detectores de humo, detectores de calor y estaciones de extracción).
- Activa los dispositivos de notificación de alarma contra incendios (bocinas, luces estroboscópicas, mensajes de evacuación de audio) cuando se activa un punto de iniciación.
- Monitorea y controla el equipo de supervisión auxiliar (relés, dispositivos de seguridad).

Todos los dispositivos de iniciación (sensores de humo, de calor, estaciones manuales) y anunciación (luces y sirenas) se conectan al panel de detección y alarma de incendios, el cual tiene la capacidad de identificar donde ha ocurrido una alarma y activar las señales para la evacuación del personal.

Imagen 1: Interface del Operador del panel de detección y alarma de incendios.

5. CONDICIONES NORMALES

El panel de interfaz del operador muestra lo siguiente en condiciones normales. El LED de alimentación verde está encendido, lo que indica que el panel está recibiendo alimentación de CA. Todos los demás LED apagados.

La pantalla táctil informa que el sistema es normal, como se muestra a continuación.

Imagen 2: Sistema en condiciones normales.

6. CONDICIONES DE ALARMA.

Se produce una condición de alarma cuando se activa un dispositivo iniciador (como una estación de extracción manual, detector de humo, etc.). El panel de alarma y detección de incendios indica la presencia de la condición de alarma a través de los mensajes que muestra en la pantalla alfanumérica, al hacer parpadear el indicador de ALARMA y al activar los dispositivos de notificación del edificio (bocinas y luces estroboscópicas).

Cuando el FACP detecta una condición de alarma, el panel hace lo siguiente para indicar la presencia de la alarma.

- LED rojo, etiquetado Alarma de incendio parpadea
- Pulsos de alerta de tono (zumbador piezoeléctrico)

El piezo puede silenciarse al presionar en cualquier lugar de la pantalla táctil de la interfaz de usuario. Hasta que las condiciones de alarma sean reconocidas, volverá a sonar después de 1 minuto de inactividad en la interfaz de usuario.

7. RECONOCER Y SILENCIAR UNA ALARMA DE FUEGO.

Este tipo de alarmas se genera cuando un dispositivo de iniciación se ha activado, en el panel se mostrarán las siguientes alarmas:

Para reconocer y silenciar la alarma se deben de seguir los siguientes pasos:

1. Confirmar una alarma

2. Silenciar la alarma

3. Restablecer el sistema

Cada paso se explica en detalle en el resto de esta sección.

Confirmar una alarma:

se pueden configurar dos tipos de modos de reconocimiento en el panel:

1. Reconocimiento global todas las zonas dentro de la lista de alarmas de zona son reconocidas a la vez.

2. Reconocimiento individual cada zona dentro de la lista de alarmas de zona se reconoce por separado.

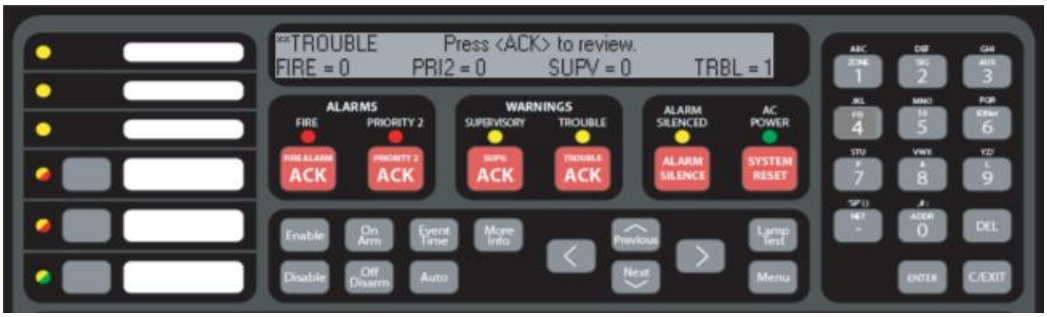


Imagen 3: Toca el botón ACK.

Nota: Reconocer una alarma no silencia las sirenas. Debe silenciar una alarma como se muestra en la sección "Silenciar la alarma"

Silenciar la alarma:

silenciar una alarma apaga todos los dispositivos de notificación audibles que están programados

para apagar cuando se presiona.

1. Toque el botón Funciones de alarma.
2. Presione el botón Alarm Silence
3. Confirmar

Nota: se puede esperar a que se silencie o presionar.

ADVERTENCIA: asegúrese de que la evacuación del edificio esté completa antes de silenciar la alarma

8. ACCIONAMIENTO Y RESTABLECIMIENTO DE ESTACION MANUAL

Las estaciones manuales instaladas son de doble acción, lo cual quiere decir que para activarlas se tiene que presionar el botón PUSH y jala firmemente la palanca hacia abajo (PULL DOWN), para restablecer la palanca y desactivar el interruptor de alarma se requiere el uso de una llave, se debe abrir la estación manual y cerrarla para restablecer la condición de alarma.

Imagen 4: Estación Manual doble acción.

9. APAGADO DEL PANEL DE DETECCIÓN DE INCENDIOS

a. Se procederá a bajar la llave térmica correspondiente del Tablero de Alimentación.

b. Luego se procederá a desconectar los porta-fusibles ubicados en los cables de conexión de las baterías.

10. MANTENIMIENTO

De acuerdo a las recomendaciones de la NFPA 72, para asegurar el correcto funcionamiento del sistema, los mantenimientos al sistema de detección y alarma de incendio del tipo preventivo se deben de realizar cada de 12 meses y las inspecciones periódicas cada 06 meses.