Universidad Norbert Wiener

Facultad de Ingeniería y Negocios

Implementación de una data center del Centro de Monitoreo y Video Vigilancia de una Municipalidad

Trabajo de Suficiencia Profesional para optar el título profesional en Ingeniero de Sistemas e Informática

Estudiante:
Bch. Tasayco Coronado, Victor Carlos

Identificador orcid:
https://orcid.org/0000-0002-6373-148X

Asesor:
Mg. Julio Alfredo Martin Córdova Forero

Identificador orcid del asesor:
0000-0001-5317-8927

Lima, Perú
2023

Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, Victor Carlos Tasayco Coronado, egresado de la Facultad de Ingeniería y Negocios ☒Escuela Académica Profesional de Ingenierías Universidad privada Norbert Wiener declaro que el trabajo académico **"Implementación de un Data Center del Centro de Monitoreo y Video Vigilancia de una Municipalidad"** Asesorado por el docente: Córdova Forero, Julio Alfredo Martin DNI 09924829 ORCID: 0000-0001-5317-8927 tiene un índice de similitud de 9% (nueve) con código oid:14912:231948523 verificable en el reporte de originalidad del software Turnitin.

Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.

……

Firma de autor
Egresado: Victor Carlos Tasayco Coronado
DNI: 43094714

……

Firma
Córdova Forero, Julio Alfredo Martin
DNI:09924829

Lima, 20 de abril del 2023

Resumen

El siguiente informe tiene como propósito **"La implementación de un Data Center del Centro de Monitoreo y Video Vigilancia"** con objetivos de reducir la inseguridad percibida por la ciudadanía, como también proveer de sistemas de vigilancia y monitoreo inteligente y así poder fortalecer la institución de seguridad.

Se mencionan como bases teóricas Normas y Estándares de Infraestructura para la implementación de los Data Centers, su clasificación según al tipo de Centro de Datos que se implementa y se toman conceptos sobre la protección de redes de Datos y Fibra Óptica, como implementación de última generación en acceso y velocidad de los datos de la información que se requiere optimizar. También se hace mención de la topología de la red implementada y los diferentes dispositivos interconectados que involucran la solución tales como Switches, Servidores, NVRs, ONUs, OLTs, Splitters, cámaras del tipo LPRs y Multisensores con conexión de fibra óptica y radioenlace.

La metodología que se utilizó para la realización del informe fue la búsqueda y consulta de bases teóricas que nos permitió aplicar y experimentar la experiencia profesional y retos que se presentaban en el proyecto o Implementación de la Sede de Monitoreo.

Como conclusión y solución integral de dicha sede se llevó a ir un paso más contra la inseguridad; a favor de la población y poder disminuir la delincuencia, robos, violencia en el distrito todo esto en conjunto para una coordinación de apoyo a la policía Nacional en los casos de investigación.

PALABRAS CLAVE seguridad ciudadana, data center, topología de red, Fibra Óptica

Abstract

In the following report, the purpose is "The implementation of a Data Center of the Monitoring and Video Surveillance Center" with the objectives of reducing the insecurity perceived by citizens, as well as providing intelligent surveillance and monitoring systems and thus being able to strengthen the institution of security.

Norms and Infrastructure Standards for the implementation of Data Centers are mentioned as theoretical bases, their classification according to the type of Data Center that is implemented and concepts on the protection of Data and Fiber Optic networks are taken, as a state-of-the-art implementation in access and data speed of the information that needs to be optimized. Mention is also made of the implemented network topology and the different interconnected devices that involve the solution such as Switches, Servers, NVRs, ONUs, OLTs, Splitters, LPRs and Multisensores type cameras with fiber optic connection and radio link.

The methodology that was obtained for the preparation of the report was the search and consultation of scientific articles and updating courses that were carried out based on professional experience and challenges that arose in the project or Implementation of the Monitoring Headquarters.

As a conclusion and integral solution of said headquarters, it took to go one step further against insecurity; in favor of the population and to be able to reduce crime, robberies, violence in the district, all this together for a coordination of support for the National Police in investigation cases.

KEYWORDS citizen security, data center, network topology, Fiber Optic

Índice

Índice de Tablas

Introducción

El siguiente informe de Trabajo de Suficiencia Profesional basado en la experiencia; tiene como tema la implementación de un Data Center del Centro de Monitoreo y Video Vigilancia de una Municipalidad, y como objetivo de reducir la inseguridad percibida por la ciudadanía, fomentando una cooperación activa entre las instituciones y las comunidades organizadas.

Tiene como importancia la implementación del DC que permite el almacenamiento seguro y eficiente de grandes cantidades de datos generados por cámaras de seguridad y otros dispositivos de vigilancia. Además, el procesamiento y análisis de estos datos en tiempo real es crucial para detectar posibles amenazas y responder de manera rápida y efectiva a situaciones de emergencia. La justificación para la implementación de un DC es brindar una mayor seguridad tanto en espacios públicos como privados, facilita la investigación y prevención de delitos y faltas, y puede reducir la tasa de crimen en una zona determinada del distrito.

La estructura del informe tiene como primer capítulo, los antecedentes y descripción de la Institución en donde se implementó la solución seguida por la problemática que vive el distrito y así obteniendo los objetivos como el de reducir la inseguridad percibida por la ciudadanía, fomentando una cooperación activa entre las instituciones y las comunidades organizadas, así como la mención de una descripción general de la experiencia laboral. Como segundo capítulo los fundamentos teóricos en la cual nos basamos como sustento de la experiencia laboral y con definiciones sobre como la seguridad de la información es importante, y ciertas normas aplicables a la solución nos lleva a una mejor calidad de trabajo. También la implementación de la tecnología, en los diferentes equipos y dispositivos configurados en la solución nos ayuda a potenciar los objetivos trasados para la sede de Monitoreo y Video Vigilancia. En el tercer capítulo revisamos las diferentes funciones, procedimientos, actividades y tareas que ayudaron a darle el uso correspondiente a la tecnología para su optimo desempeño con el software implementado y el día a día, complementando con el aporte de mi experiencia laboral y como se fueron sumando actividades y procedimientos para la mejora. Se mencionan propuestas de la experiencia laboral que ayudaron a futuro una mejor calidad y desempeño a la solución realizada como el de proponer software para detectar las distintas incidencias que se presenten

en la red, aplicativo de incidencias para los visualizadores, cubrir turno las 24 horas con el fin de solventar las incidencias que se presenten en la sede de Monitoreo; así como también conclusiones y recomendaciones para la mejora continua.

La implementación del centro de monitoreo de video vigilancia tiene como alcances la centralización y resguardo de la información generada por los sistemas de seguridad, lo que permite una gestión más eficiente y rápida de los datos para la toma de decisiones. Además, mejora la seguridad de la información y la calidad del servicio para la seguridad ciudadana. Sin embargo, como limitaciones se encuentran los altos costos de implementación, mantenimiento y actualización de la infraestructura y el personal altamente capacitado necesario para su operación. También, es importante considerar la necesidad de contar con una adecuada infraestructura eléctrica, de enfriamiento y seguridad física para su correcto funcionamiento y protección de los datos.

Capítulo I: Antecedentes y descripción General de la experiencia

1.1 Descripción de la Institución

La sede Central de Monitoreo de Seguridad Ciudadana que pertenece al Distrital Limeño que se encuentra ubicada a una altitud que varía desde 150 a 811 m.s.n.m en el cono Norte y dirección física Jirón José G. Higino 100, Comas 15326.

El Distrito tiene una superficie de 48.72 km2 que representa el 5% de la extensión del territorio de Lima Norte y el 1.7% de la superficie de Lima Metropolitana y es el cuarto distrito más poblado del Perú.

Con la creciente migración tanto de pobladores de provincia y migrantes extranjeros al país y en los distintos conos de Lima trajo consigo una mayor demanda de seguridad en la población ya que son los casos de robo, delincuencia y denuncias las que fueron reportados en hasta el este último año 2022 por el INEI.

El distrito se sectoriza por zonas siendo la zona 4 donde se encuentra ubicado la Central de Monitoreo de Seguridad Ciudadana con una Ubicación Limites central. En esta zona se desarrolla dos tipos de estructuras edáficas: con suelos accidentados y otra con relieve semiplano entre la avenida Tupac Amaru.

Figura 1

Mapa del Distrito de Comas y Ubicación de la Sede de monitoreo donde se realiza la Experiencia Profesional.

Sectorización del Distrito por zonas

Se incluyen como parte de la experiencia General la conexión de las cámaras por fibra óptica y radio enlace, también de realizar el seguimiento de los Workstation en la sala de visualizadores en tiempo real, el óptimo funcionamiento del Data Center con los diferentes dispositivos instalados en la topología de red implementada.

La revisión de los anexos y el reporte del barrido de las cámaras conectadas en tiempo real fueron parte de la experiencia profesional, así como también las revisiones de las grabaciones de cada cámara instalada.

A continuación, se menciona las zonas en donde cubren parte de las cámaras de video vigilancia para el distrito de Comas.

El Sector Zonal 1 ubicada en la margen sur de Comas limitando por el norte con el sector 2, 6 y 11, hacia el sur con los Distritos de los Olivos e Independencia. Por el Este y Oeste Los Olivos e Independencia respectivamente.

La zona presenta suelos inestables con pendientes que oscilan entre 20 y 40 grados y son de riesgo potencial. Las actividades en la zona son el comercio de productos alimenticios.

En el sector 2 al sur con el sector 2 y 13, por el norte con el sector, en el este con el Distrito de Independencia.

En el sector 3 limita en el norte con el sector 4, en el este y oeste con el distrito Independencia y sector 13 respectivamente.

Por el sector 4 con la zona 5 y 9 lado norte, por el sur sector 3,10 y 1. Oeste los sectores 10 y 9.

En el sector 5, por el norte limita la zona 12, 8 y el Distrito de Carabayllo. El Este con el Distrito de San Juan de Lurigancho y el Oeste sector 9 y 8.

En el sector 6 con actividades comerciales de mayor importancia a lo largo de la avenida Universitaria y avenida 22 de agosto.

El sector 7 limitando por el Norte con la zona 9,10 y 14. Siendo un sector con más áreas verdes y parques habilitadas. Y caracterizada la zona por lugares de recreación entre otras.

El sector 8 y 9 son zonas que se caracterizan por tener ocurrencia de fenómenos naturales y antrópicos como el afloramiento de aguas subterráneas.

Con el sector 10 y 11 existen establecimientos de ventas de productos alimenticios, lubricantes, mecánicas y vulcanizados.

Zona 12 con la que mayormente se realizaron programas en favor a la salud ambiental a través de programas de letrinización.

Antiguamente el territorio del sector 13 se dedicaba a la extracción de materiales de tipo no metálico utilizados en construcción.

El sector 14 con territorio agrícola y ganadera, última en el distrito donde aún se conservan las actividades agropecuarias de cultivo, frutales, forrajes y crianza de ganado.

1.2 Antecedentes

Chaglla T. et. al (2021) realiza un análisis de los establecimientos y concluyo que el sistema actual de videovigilancia no proporciona la cobertura necesaria, lo que resulta en lugares críticos con gran nivel de vulnerabilidad, que deben ser corregidos de inmediato. La investigación incluye el estudio y análisis de diferentes tipos de sistemas de circuito cerrado de televisión (CCTV), incluyendo sus diferentes maneras de funcionamiento, equipos y requisitos técnicos. Además, se adoptó la norma NFPA 731 para determinar la ubicación, instalación, rendimiento, pruebas y mantenimiento de los sistemas de seguridad. Se concluyó en presentar el estudio técnico del sistema de videovigilancia, que incluye la estructura, instalación de los equipos y herramientas que fueron necesarias para cumplir de manera efectiva, confiable, segura y estable para el sistema implementado en la universidad.

En su trabajo de grado de Beltran G. y Montealegre J. (2018) el objetivo principal de este proyecto es evaluar la calidad de transmisión de vídeo en formato MPEG4 en el estándar 802.11 mediante un sistema de cámaras de vigilancia bajo el protocolo TCP/IP V4. Se utiliza esta tecnología inalámbrica para el monitoreo de la vigilancia perimetral en el municipio de Yaguará. Se concluye con la examinación de aspectos técnicos, que muestran las ventajas y desventajas en su implementación y se ofrecen sugerencias y recomendaciones para garantizar la calidad en el funcionamiento del sistema con los requerimientos exigidos.

Corzo L. (2019) detalla los estudios llevados a cabo para crear una infraestructura tecnológica en servicios de la seguridad ciudadana en el distrito de Santiago de Cusco. El proyecto incluye el estudio, diseño e implementación de los subsistemas de seguridad electrónica, con el objetivo de satisfacer las necesidades fundamentales que es de proteger a los ciudadanos y turistas. Estos subsistemas, en conjunto, permiten el monitoreo constante del distrito y sus habitantes, mediante video y audio. Teniendocomo resultado, el presupuesto general y el cronograma del proyecto.

Temoche A. (2019) en su tesis titulada “Propuesta de Implementación de Data Center en Presta Sullana - Sullana:2019” menciona los lineamientos que debe cumplir un Centro de Datos cumpliendo con las normas y estándares que garantice una buena comunicación entre los servicios. El estudio realizado fue de tipo descriptivo y cuantitativo, sin un diseño experimental específico. El personal de la empresa se consideró como la población objeto de estudio y se utilizó una encuesta y un Checklist como instrumentos metodológicos para determinar el diagnóstico de las variables. Con la aplicación de los instrumentos de recolección de datos se llega a los resultados que coinciden con la hipótesis general planteada en la investigación, la cual afirmaba que el diagnóstico situacional del Centro de Datos determinaría mejoras y continuidad en el servicio de la empresa Presta Sullana. Por lo tanto, se acepta y demuestra esta hipótesis. La investigación se justifica en la necesidad de contar con el diagnóstico del Centro de Datos para determinar mejoras en el servicio.

Castro F. (2018) en su Tesis: “Propuesta de Mejoramiento del Sistema de Video Vigilancia en la Seguridad Ciudadana distrito de la Esperanza 2018” menciona la importancia de implementar equipos tecnológicos al personal de seguridad ciudadana para proveer de capacidad de respuesta en tiempo real e información oportuna frente a la delincuencia, robos o actos delictivos que se presenten en el Distrito.

Así también plateando como objetivos de la propuesta a la identificación de los niveles de inseguridad ciudadana, evaluar la cobertura, control y monitoreo del sistema actual de videovigilancia determinando los puntos de ubicación y cantidades instaladas en el distrito.

Y en base a los resultados obtenidos de la población y personal de seguridad en el distrito es que lo lleva a proponer la mejora en el Sistema de Video Vigilancia con implementación e instalación de cámaras de video de acuerdo a características técnicas y necesidades de mejora del sistema de detección y control.

Cabe mencionar el sistema de red que se implemento fue el GEPON que se basa en red de distribución primaria del tipo anillo. Explicando el cableado principal que se llevó a cabo para distribuir la red óptica en los diferentes puntos del distrito y como destino los dispositivos que lleva la implementación como cámaras, gabinetes, splitters, cables de fibra, OLT y ONUs

Diaz Huarancca (2018) En su estudio de tesis se enfoca en el problema de cómo mejorar la seguridad de activos en el campus universitario sede Paturpampa de la Universidad Nacional

de Huancavelica utilizando un Sistema Videovigilancia IP. El objetivo general es desarrollar este sistema con el propósito de mejorar la seguridad en el campus, mientras que la hipótesis general que se busca confirmar es que la implementación del Sistema Videovigilancia IP tendrá un efecto positivo en la seguridad de activos en el campus. La metodología utilizada es el Método Científico, con una investigación aplicada de nivel descriptivo-explicativo. La principal conclusión obtenida es que la implementación del Sistema Videovigilancia IP que mejora la seguridad de activos en el campus universitario .

1.3 Problemática

La dinámica delictiva a nivel global está marcada por la presencia y el incremento de la violencia y la actividad criminal, la cual se manifiesta diariamente a través de diversos delitos como homicidios, robos, secuestros, extorsiones, violaciones y otros. Estas conductas delictivas limitan la seguridad ciudadana en todos los ámbitos de la actividad humana a nivel mundial.

Solo por mencionar PNUD (2020) el Programa de las Naciones Unidas en el año 2017 propuso un enfoque sociológico para la identificación de la violencia, que se basa en cuatro factores. El primer factor es el "delito aspiracional", que se refiere a la desigualdad y la movilidad social. El segundo factor se conoce como la "teoría del tejido social", la cual establece indicadores relacionados con las familias monoparentales y los cambios económicos generados por la liberalización del comercio, entre otros aspectos macroeconómicos. El tercer factor se refiere a los "facilitadores del delito y la violencia", como las armas, el alcohol y las drogas. Por último, el cuarto factor es la "carencia de capacidades institucionales de los Estados", que engendran el crimen en todas sus formas y comprometen gravemente la seguridad ciudadana.

La inseguridad ciudadana es una situación seria que afecta la vida de las personas y las comunidades. Algunos de los efectos negativos de la inseguridad ciudadana incluyen:

La inseguridad ciudadana puede aumentar la delincuencia, incluyendo robos, violaciones y asaltos.

Pérdida de confianza en las instituciones: La inseguridad ciudadana puede erodar la confianza en las instituciones encargadas de garantizar la seguridad, como la policía y el sistema judicial.

Reducción de la calidad de vida: La inseguridad ciudadana puede limitar la libertad de movimiento y afectar negativamente la calidad de vida de las personas.

Pérdida de inversiones y turismo: La inseguridad ciudadana puede disuadir a las empresas y turistas de invertir y visitar una comunidad, lo que puede afectar negativamente la economía local.

Aumento de la tensión social: La inseguridad ciudadana puede crear tensiones y conflictos entre las personas y las comunidades, lo que puede socavar la cohesión social y el sentido de comunidad.

Con todo esto la inseguridad ciudadana es uno de los problemas que ha ido afectando a los sectores del distrito de Comas por los delitos contra el patrimonio y seguridad pública, seguido de delitos contra la mujer y grupos vulnerables, siendo un punto sobre fenómenos delictivos que priorizados en el plan nacional de seguridad Ciudadana 2019-2023.

Es importante abordar la inseguridad ciudadana de manera efectiva y colaborativa para mejorar la seguridad en las comunidades y mejorar la calidad de vida de las personas. Esto requiere una combinación de medidas preventivas y de respuesta, proveer al pueblo y entidades de justicia con herramientas, dispositivos y mecanismos que mejoren la calidad de vida de los ciudadanos, incluyendo iniciativas comunitarias, programas de educación, tecnología y empleo, y fortalecimiento de las instituciones encargadas de la seguridad.

1.4 Objetivos

Objetivos Generales

Mejorar la colaboración entre diferentes sectores y organismos en el distrito de Comas con el objetivo de reducir la inseguridad percibida por la ciudadanía, fomentando una cooperación activa entre las instituciones y las comunidades organizadas.

Objetivos Específicos

1. Realizar una evaluación de la situación actual de seguridad en el distrito de Comas. Fomentar la colaboración de las instituciones educativas para fortalecer los buenos valores. Alentar la participación de los organismos sociales y trabajar juntos con la policía del Perú para establecer nuevas juntas vecinales.

2. Proveer sistemas de vigilancia y monitoreo inteligente en la ciudad para detectar y prevenir delitos y actividades peligrosas de manera eficiente y oportuna, mejorando así la seguridad de la población y fortaleciendo la confianza en las autoridades responsables.

3. Incluir el uso de cámaras de seguridad y análisis de datos para identificar patrones y tendencias, así como mecanismo de alerta y respuesta de emergencia con la finalidad de garantizar la seguridad de la población y mejorar las fuerzas de seguridad en la prevención a la resolución de delitos.

1.5 Descripción General de la Experiencia

En esta sección se brindará una breve explicación de las funciones de los colaboradores del área de trabajo en la Sub Gerencia de Informática, empezando como parte de ello el de planificar, dirigir, evaluar y supervisar al momento de desarrollar e implementar los sistemas informáticos, así como también de asignar y distribuir los equipamientos de hardware y software a las diferentes áreas usuarias o unidades orgánicas.

Según el MOF (2009) el de establecer metodologías de desarrollo de sistemas de información, informar de avances y operaciones de los diferentes sistemas que estén a cargo de la subgerencia.

Proponer regulaciones para el manejo de sistemas de información y hardware, encargándose de la administración de la red municipal, control de accesos y seguridad de la información.

Proveer del soporte técnico necesario a las unidades o áreas de las sedes en el uso de sistemas informáticos y equipos; así como también la actualización de información en portales institucionales de acuerdo a las normas establecidas.

Monitorear y controlar el uso de servicios y tráficos en la red, enviar correos electrónicos a usuarios registrados.

Proporcionar mantenimiento de los equipos informáticos de la institución; también el de proponer planes de renovación de los equipos informáticos si estos fueran necesario para ciertas áreas y el cual participar en los procesos de adquisición de equipamiento informático.

Mantenimiento preventivo y correctivo de los equipos de cómputo como también llevar el control de inventario de los equipos y software de la Institución.

Implementar gestión de las herramientas tecnológicas en su diseño y desarrollo para la toma de buenas decisiones; así como también proponer capacitaciones y desarrollo de temas informáticos para el personal de la Municipalidad con el fin de mejorar su productividad.

Elaborar, ejecutar y evaluar periódicamente el Plan Operativo Informático Institucional en el corto, mediano y largo plazo, según con los objetivos del Plan Estratégico Institucional.

La coordinación con organismos públicos y privados en asuntos de su competencia; así como también; brindar asesoramiento en su campo de especialidad.

Derogar al personal a cargo, funciones específicas del área en asuntos relacionados con su unidad organizativa.

Habiendo hecho mención de las funciones y en lo que le compete según el (MOF) al área de la Sub Gerencia de Informática Y Gobierno electrónico cabe mencionar el propósito del puesto que se desarrollara en la implementación del Data Center para la sede de Monitoreo y Video vigilancia de la Municipalidad.

Es por lo ya mencionado que también se cumplen con los objetivos de *proveer sistemas de vigilancia y monitoreo inteligente en las ciudades para detectar y prevenir delitos y actividades peligrosas de manera eficiente y oportuna, mejorando así la seguridad de la población y fortaleciendo la confianza en las autoridades responsables.*

Incluir el uso de cámaras de seguridad y análisis de datos para identificar patrones y tendencias, así como mecanismo de alerta y respuesta de emergencia y mejorar las fuerzas de seguridad en la prevención a la resolución de delitos.

Esta implementación de la solución hará que se lleve un reporte de la gestión de la red de datos, su correcto funcionamiento y mantenimiento de los diferentes dispositivos informáticos que comprenden la solución ya sean el cableado estructurado, las unidades de procesamiento, switches, routers, NVRs, Estaciones de trabajo (WorkStations), anexos, Cámaras LPR- PTZ y softwares para su administración de los dispositivos.

Capítulo II: Fundamentos Teóricos

2.1 Bases Teórica

Teoría de Sistemas

Fatorachian H. y Kazemi H. (2021) Menciona en su estudio del impacto de la Industria 4.0 en el desempeño de la cadena de suministro Con base en esta investigación, se espera que la aplicación de tecnologías habilitadoras de Industria 4.0 genere mejoras significativas en el rendimiento de SCM al permitir un enfoque holístico hacia la gestión de la cadena de suministro como resultado de una amplia integración de la cadena de suministro, así como el intercambio de información y la transparencia en toda la cadena de suministro. Además, estas tecnologías permiten enormes mejoras de rendimiento dentro de los procesos individuales de la cadena de suministro, como compras, producción, gestión de inventario y venta minorista, al permitir la integración, la digitalización y la automatización de procesos, y generar nuevas capacidades analíticas.

Ding L. et al. (2020) se centra en la identificación de parámetros de sistemas autorregresivos controlados utilizando información de observación. La teoría de sistemas se aplica en este caso para descomponer el sistema autorregresivo controlado en dos subsistemas y analizar cómo interactúan entre sí. En particular, el artículo utiliza el principio de identificación jerárquica para descomponer el sistema en dos subsistemas y luego propone un algoritmo iterativo basado en gradientes de dos etapas para estimar los parámetros de cada subsistema. Además, para mejorar el rendimiento del seguimiento de los parámetros variables en el tiempo, se deriva un algoritmo iterativo basado en gradientes de innovación múltiple de dos etapas basado en la teoría de identificación de innovación múltiple.

En general, la aplicación de la teoría de sistemas en este artículo permite analizar cómo las diferentes partes del sistema interactúan entre sí y cómo se pueden optimizar estas interacciones para mejorar el rendimiento del sistema en términos de identificación de parámetros. El ejemplo proporcionado en el artículo ilustra la efectividad de los algoritmos propuestos y cómo la teoría de sistemas puede ser aplicada en la práctica para resolver problemas complejos en diferentes campos de la ciencia y la ingeniería.

Zhu Y. y Zheng W. (2019) En particular, el artículo utiliza la técnica de aproximación suave y la propiedad de conmutación de tiempo de permanencia modal para restringir las conmutaciones entre subsistemas no lineales. Además, se introduce un tipo de conmutación autónoma, dependiente de la partición de estado, dentro de cada subsistema afín por partes

aproximado (PWA). la teoría de sistemas se utiliza en este artículo para analizar cómo los diferentes subsistemas interactúan entre sí en un sistema conmutado no lineal y cómo se pueden optimizar estas interacciones para mejorar la estabilidad y el control del sistema completo. El enfoque propuesto en este artículo demuestra la efectividad de la teoría de sistemas en la práctica para resolver problemas complejos en diferentes campos de la ciencia y la ingeniería.

Según Carmona D. (2011) en su enfoque en la teoría de Sistemas que pasa por etapas como son de Modelación de la Realidad, Etapa de Utilización y trabajo con el modelo y pautas de acción, Etapa de decisión, Etapa de puesta en marcha y Etapa de Operación y evaluación llegando a la conclusión de ser Niveles de Organización, planteando como Estructura de Supersistema – Sistema – Subsistema y en conjunto interactúan entre sí para lograr un objetivo.

Desongles C. et al. (2006) menciona en su Teoria General de Sistemas un conjunto de elementos funcionales independientes, aunque relacionados entre si, que s eunen formando un todo complejo como puede ser una entrada, un proceso, una salida, etc. Con objetivos concretos que suponen su meta.

Teniendo como evaluación ambas teorias puedo concluir para implementar un sistemas en todo ambito y rama de la ciencia y tecnología pasan por ciertas etapas y a la vez jerrarquizandolas con la idea de cumplir metas y objetivos.

Gestión de la Seguridad de Información

Medina Garzón y Vásquez Rodríguez (2020) su proyecto tiene como finalidad inicialmente analizar el estado actual de la seguridad de la información aplicando la norma 27001 y la norma 27002 debido a la información tan delicada y teniendo en cuenta que la información es el mayor activo de una empresa estos permiten reducir las vulnerabilidades y amenazas que puedan surgir en las entidades, tomando como base las normas mencionadas.

Mokrani Gallego O. (2021) explica de una forma práctica los principales conceptos a tener en cuenta a la hora de diseñar una infraestructura de red para que no sea vulnerable a ataques y cumpla con la serie ISO 27000 de estándares de seguridad publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional. Una vez conocidas las peculiaridades de la red, sus componentes y sus pequeños matices en cuanto a configuración se refiere, se procederá a integrar distintas herramientas de seguridad, auditoría

y gestión de vulnerabilidades que nos ayudarán a mantener libre de amenazas la integridad de los datos.

Para hablar sobre seguridad de información hoy en la actualidad haremos mención de Disterer, G. (2013). ISO/IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información. "La existencia de las normas ISO 27000 a ISO 27002 se remonta a 1993, cuando un británico asociación profesional, el Centro Nacional de Cómputo (NCC), publicó un documento titulado "PD 0003 A Code of Práctica para la Gestión de la Seguridad de la Información". El British Standards Institute (BSI) adoptó esto y emitió "BS 7799-1 TI—Técnicas de seguridad—Código de práctica para la gestión de la seguridad de la información" como estándar nacional en 1995.

La parte complementaria "BS 7799-2 Sistemas de gestión de la seguridad de la información—Especificación con guía de uso" permite a las empresas certificar sus procesos. ISO armonizó esta norma con otras como ISO 9001 y desarrolló la ISO 27001 en octubre de 2005. Desde entonces, las empresas pueden certificar sus procesos de acuerdo a este estándar internacional.

ISO 27001 formó la base para ISO 27 K familia de normas, que abarca varias normas para la seguridad de la información. En 2007 la antigua ISO 17799 estándar fue asignado a la familia ISO 27 K como ISO 27002. En 2009 se emitió ISO 27000 para proporcionar una descripción general, introducción y explicación de la terminología con el título "TI—Técnicas de seguridad—Sistemas de gestión de seguridad de la información—Visión general y vocabulario".

La infraestructura de un centro de datos también requiere una cuidadosa consideración de la seguridad de la infraestructura de TI. Esto puede incluir seguridad física para el edificio, como entrada de llave electrónica, video constante y vigilancia humana de las instalaciones, acceso cuidadosamente controlado al servidor y espacios de almacenamiento, etc. Esto garantiza que solo el personal autorizado pueda acceder a la infraestructura de hardware del centro de datos y reduce la posibilidad de daños malintencionados o robo de datos.

Fuera del centro de datos hay una infraestructura de Internet, que incluye medios de transmisión, como cables de fibra óptica, satélites, microondas (línea de vista), antenas, enrutadores, agregadores, repetidores, balanceadores de carga y otros componentes de red que controlan las rutas de transmisión. Las infraestructuras de Internet están diseñadas, construidas

y operadas por proveedores de servicios de Internet (ISP), como Verizon y AT&T. Cuando una empresa contrata a un ISP para el acceso a Internet, el ISP generalmente se conecta a la infraestructura del centro de datos dentro de un espacio de construcción dedicado y seguro. Stephen J. Bigelow, (2020)

El modelo de software como servicio (SaaS) ofrece beneficios similares para cargas de trabajo específicas. Un proveedor externo aloja hardware, software, servidores, almacenamiento y otros componentes de infraestructura, y permite a los usuarios acceder a las cargas de trabajo alojadas del proveedor en lugar de implementar y mantener esas cargas de trabajo localmente. Por ejemplo, los usuarios pueden emplear cargas de trabajo SaaS para bases de datos, aplicaciones de recursos humanos, aplicaciones analíticas, suites de productividad de oficina y muchas otras.

Normas Y Estándares de Infraestructura para Data Centers
ANSI/BICSI 002 y ANSI TIA-942

BICSI (ANSI/BICSI) Nos establece el estándar en diseño de los Centro de Datos (ANSI/BICSI 002-2019, 2019) como las siguientes clases:

Clase F0: Esta clase se refiere a las instalaciones más básicas, que se limitan a la instalación de cables y la conexión de equipos de telecomunicaciones en un solo punto de entrada del edificio. Esta clase no proporciona redundancia ni tolerancia a fallos en el sistema de telecomunicaciones.

Clase F1: Esta clase se refiere a instalaciones más avanzadas, que proporcionan redundancia en el sistema de telecomunicaciones mediante la instalación de rutas y equipos duplicados. Esta clase también incluye la protección contra incendios y la protección contra descargas eléctricas.

Clase F2: Esta clase se refiere a instalaciones aún más avanzadas que la Clase F1, con una mayor redundancia y tolerancia a fallos. Esta clase también incluye la protección contra incendios y la protección contra descargas eléctricas, pero con mayores requisitos de capacidad de energía y enfriamiento.

Clase F3: Esta clase se refiere a instalaciones de alta disponibilidad que ofrecen redundancia completa en todos los componentes de la infraestructura de telecomunicaciones.

Clase F4: Esta clase se refiere a instalaciones de misión crítica que proporcionan la mayor redundancia y tolerancia a fallos posible.

Ruldeviyani Y. et. al (2017) propone como gestión los estándares de Centro de Datos (ANSI/TIA-942 y ANSI/BICSI-002) que luego se clasifican por componentes. En conclusión, la investigación propone el desarrollo de una guía de evaluación de gestión de Centro de Datos a partir de los estándares existentes y la utilización de un enfoque de estudio de caso e investigación acción para evaluar su aplicación en un contexto específico. Esto es importante para asegurar el correcto funcionamiento del Centro de Datos y optimizar su capacidad de apoyo a los servicios de TI.

Hydeman y Swenson, (2010) la Publicación especial de ASHRAE trata sobre Pautas térmicas para entornos de procesamiento de datos y la Norma de infraestructura de telecomunicaciones para centros de datos ANSI/TIA-942-1 2005. A través de estas investigaciones, han descubierto que los límites de humedad más bajos se proporcionaron principalmente para reducir el potencial de descarga electrostática (ESD) en los centros de datos. En conclusión, el artículo examina las pautas que recomiendan el control de la humedad en los centros de datos, centrándose en dos pautas en particular.

Riffan T. et. al. (2018) Nos menciona que se necesita un diseño de centro de datos en DISKOMINFO Gobierno local de Bandung la regencia puede alcanzar los estándares que se han determinado especialmente para la consideración del diseño del cableado Sistema de automatización de edificios en el centro de datos DISKOMINFO Gobierno local de la regencia de Bandung. El resultado de esta investigación es analizar y dar resultado a los procesos de los Centros de Datos que existen en DISKOMINFO Local Gobierno de Bandung Regency basado en el estándar ANSI/BICSI 002. El resultado final de esta investigación es un resultado propuesto sobre el procesamiento del centro de datos en Consideraciones de diseño de cableado Sistema de automatización de edificios.

Esquema de Programación consciente de emergencia de datos

Qiu et al. (2018) en su publicación (A Data-Emergency-Aware Scheduling Scheme for Internet of Things in Smart Cities) menciona en la investigación sobre la programación de paquetes de datos, se han identificado tres tipos principales en los últimos años: primero en llegar, primero en ser atendido (FCFS), fecha límite más temprana primero (EDF) y tarea de emergencia monótona de primera velocidad. Aunque el algoritmo FCFS es ampliamente utilizado y se utiliza en colas de prioridad multinivel, algunos estudios se han centrado en la programación de paquetes de datos de un solo nodo y no han considerado el impacto entre diferentes nodos. Por lo tanto, es necesario un algoritmo eficiente que pueda asignar los recursos de la red de manera racional y garantizar la puntualidad de los paquetes de datos de emergencia. En el esquema de programación de paquetes para ciudades inteligentes, se deben proporcionar algunos datos más detallados junto con la información importante, como la información de alarma en el servicio de monitoreo de incendios.

La principal contribución de este algoritmo es el uso de un mecanismo de reconocimiento de emergencia de datos para garantizar la puntualidad de los paquetes de datos de emergencia cuando múltiples nodos envían paquetes al mismo nodo de destino simultáneamente. Además, EARS controla estrictamente los intervalos de tiempo para mejorar el rendimiento de la red mediante el uso de diffserv para paquetes relevantes basados en la información de emergencia del paquete. Los resultados de los experimentos de simulación muestran que EARS supera a trabajos anteriores en términos de retraso de extremo a extremo, tasa de pérdida de paquetes y tiempo de espera de paquetes de datos.

Jemmali et al. (2022) en este estudio se aborda el problema de asignación de enrutadores en situaciones de asignación de datos de alta prioridad y emergencia, y se introduce un nuevo componente de red denominado programador y se imponen restricciones de ventana para los enrutadores. Para resolver este problema se desarrollan cuatro algoritmos diferentes, que se aplican en un escenario particular con varios enrutadores y 2200 instancias.

En conclusión, propone el uso de técnicas de inteligencia artificial para resolver el problema de asignación de enrutadores en situaciones de asignación de datos de alta prioridad y emergencia, y se desarrollan y aplican cuatro algoritmos diferentes para este fin, obteniendo resultados aceptables en términos de intervalo y tiempo de ejecución.

Booba y Gopal (2015) propone una técnica de planificación de paquetes basada en prioridad (PPS) para mejorar la eficiencia y escalabilidad de la transmisión de información en redes

inalámbricas, especialmente en situaciones de tiempo no real. La técnica PPS utiliza una cola de prioridad de tres niveles para asignar prioridad a los paquetes de información y permitir que los paquetes críticos sean transmitidos de manera oportuna. Además, se utiliza un umbral para colocar los paquetes de información no críticos en dos colas alternativas y evitar un retraso excesivo de extremo a extremo.

Concluye que la técnica de programación de paquetes propuesta es efectiva para mejorar la eficiencia y escalabilidad de la transmisión de información en redes inalámbricas, especialmente en situaciones de tiempo no real.

Gupta y Sharma (2019) se propone el uso de técnicas de programación, en particular la técnica de programación dinámica de paquetes de prioridad multinivel, para lograr un uso eficiente de los recursos disponibles en las redes, especialmente la duración de la batería. También se menciona la utilización de un algoritmo de enrutamiento basado en zonas en el que los nodos sensores están dispuestos en zonas para proporcionar equidad y minimizar el retraso para la red que involucra datos en tiempo real y no en tiempo real.

la programación de datos es fundamental para optimizar el uso de los recursos en las redes de sensores inalámbricos, y la combinación de técnicas de programación y algoritmos de agrupamiento puede mejorar significativamente la eficiencia energética y prolongar la vida útil de la red.

Cultura de Seguridad de la Información

Para la importancia de la seguridad como cultura en las personas Cooper, MD (2018) en su libro (The Safety Culture Construct: Theory and Practice.) Encuentra un consenso sobre 6 características principales de la cultura de seguridad al examinar la investigación académica:

- gestión/supervisión – sistemas de seguridad – riesgo – presión de trabajo – competencia – procedimientos y reglas.

Y por lo general, estas están contenidas en los sistemas modernos de gestión de la seguridad implementados en muchos países. Las empresas deben priorizar estas características de la cultura de seguridad para efectuar un cambio.

La interpretación de lo que constituye la cultura de seguridad varía según la persona, lo que influye en sus intentos de mejora. En esencia, la cultura de seguridad se trata de un enfoque proactivo para mejorar la seguridad ocupacional, y refleja la manera en que las personas

piensan y/o se comportan en relación con la seguridad. Para mejorar la postura proactiva, se debe enfocar en los problemas de seguridad relevantes, que se encuentran dentro de las características de seguridad comunes (gestión/supervisión, sistemas de seguridad, riesgo, presión laboral, competencia, procedimientos y reglas).

Wang et al. (Wang, Wang, Su, & Ge, 2020) propone el uso del mecanismo de posibilidades de análisis empresarial para mejorar la gestión de datos de computación en la nube y la seguridad de la información. Además, se menciona la importancia de la cultura y la integración de procesos de negocios de TI en la gestión de la seguridad de la información.

el estudio concluye que la cultura de la seguridad de la información y la integración de procesos de negocios de TI son fundamentales para mejorar la gestión de datos de computación en la nube seguridad. Además, se propone el uso del mecanismo de posibilidades de análisis empresarial como una herramienta efectiva para lograr esta mejora.

Trang y Brendel (2019) propone que, para hacer cumplir las políticas de seguridad de la información, las organizaciones a menudo implementan mecanismos de sanción, pero la eficacia de este enfoque ha sido mixta. Se argumenta que los moderadores contextuales y metodológicos juegan un papel crucial al conceptualizar la teoría de la disuasión en estudios de seguridad.

La teoría de la disuasión puede ser aplicable en la seguridad de la información, pero se necesita considerar el contexto y los moderadores metodológicos para comprender su eficacia en diferentes situaciones.

Da Veiga et al. (2020) propone que una cultura fuerte de seguridad de la información puede ayudar a minimizar las amenazas que los seres humanos representan para la protección de la información y, por lo tanto, reducir las violaciones de datos o incidentes en las organizaciones. La investigación se enfocó en definir y comprender el concepto de cultura de seguridad de la información, así como identificar los factores necesarios para inculcar una cultura ideal y su impacto potencial.

2.2 Bases Conceptuales

Data Center – Centro de Datos

EL Centro de Computo o Centro de procesamiento de Datos (CPD) es un espacio dedicado para albergar información más importante de una Empresa o Compañía, el cual debe ser seguro y disponible, aplicar las mejores prácticas garantizan que se mantengan dichas condiciones.

Dovgyi, S. , Kopiika, O. (2023) Los Centro de Datos tienen por objeto mantener en buen estado técnico los siguientes elementos: dispositivos de red, equipos de cómputo, dispositivos de almacenamiento de datos, servicio de despliegue automático de software, servicio de red, servicio de seguridad perimetral, servicio de directorio, servicio de archivo e impresión, servicio de gestión de datos, servicio de aplicaciones empresariales, servicio de gestión de TI, servicio de copia de seguridad y recuperación.

Uptime Institute

El Uptime Intitute (2018) es una organización que se enfoca en mejorar la disponibilidad y eficiencia de los centros de datos. La organización ha desarrollado un sistema de clasificación llamado (Infraestructura para Centros de Datos Tier Standard: Topología) que se utiliza para evaluar la capacidad y la fiabilidad de un centro de datos en términos de tiempo de actividad.

Nos da niveles de clasificación de Tier Standard que se describen de la siguiente manera:

Tier I: Es el nivel más básico de clasificación. Un centro de datos Tier I tiene una infraestructura de TI básica y puede tener una capacidad limitada de enfriamiento y energía. La disponibilidad de un CD Tier I es de aproximadamente el 99.671%, lo que significa que puede tener una interrupción del servicio de hasta 28.8 horas por año.

Tier II: Este nivel de clasificación agrega ciertas mejoras al nivel Tier I, como la inclusión de sistemas redundantes para la energía y el enfriamiento. El tiempo de inactividad esperado para un centro de datos Tier II es del 99.741%, lo que significa que puede tener una interrupción del servicio de hasta 22 horas por año.

Tier III: Este nivel de clasificación proporciona una mayor redundancia en la infraestructura del centro de datos y se espera que tenga una disponibilidad del 99.982%, lo que significa que puede tener una interrupción del servicio de hasta 1,6 horas por año.

Tier IV: Este nivel de clasificación es el más alto en términos de disponibilidad y fiabilidad. Un centro de datos Tier IV cuenta con la mayor cantidad de redundancia posible en la infraestructura, lo que significa que puede resistir interrupciones de servicio imprevistas sin afectar la operación normal del Data Center. La disponibilidad esperada para un Data Center Tier IV es del 99.995%, lo que significa que puede tener una interrupción del servicio de hasta 26,3 minutos por año

Componentes de Infraestructura – Centro de Datos

La infraestructura del CD a menudo incluye los elementos de energía y refrigeración que es importantes para admitir el hardware. La infraestructura de hardware del centro de datos generalmente involucra servidores; subsistemas de almacenamiento, dispositivos de red, enrutadores y cableado físico; y dispositivos de red dedicados, como firewalls de red. Stephen Bigelow J. (2020)

Gestión de infraestructuras

Según Carrion B. (2019) La infraestructura de tecnología de la información (TI) debe ser capaz de ofrecer una plataforma adecuada para las aplicaciones y funciones de TI necesarias por una organización o individuo, independientemente de su diseño o configuración. La gestión efectiva de la infraestructura de TI es fundamental y debe ser respaldada por herramientas de software que permitan a los administradores de TI visualizar la infraestructura como una única entidad y acceder a detalles operativos precisos de cualquier dispositivo dentro de la infraestructura. Esta capacidad de gestión centralizada resulta en una administración de la infraestructura más eficiente y efectiva. Una gestión sólida también permite a los administradores de TI optimizar los recursos para diferentes cargas de trabajo y entender y manejar con mayor facilidad el impacto de cualquier cambio en los recursos interconectados.

La gestión de la infraestructura a menudo se divide en varias categorías. Por ejemplo, un sistema de gestión de edificios (BMS) proporciona las herramientas que informan sobre los parámetros de las instalaciones del centro de datos, incluidos el uso y la eficiencia de la energía, la temperatura y el funcionamiento de la refrigeración, y las actividades de seguridad física. La gestión de sistemas incluye la amplia gama de conjuntos de herramientas que utiliza un equipo

de TI para configurar y gestionar servidores, dispositivos de red y almacenamiento. Cada vez más, las herramientas de administración de sistemas se están extendiendo para admitir centros de datos remotos, junto con recursos de nube pública y privada. Las herramientas de administración también están haciendo un uso extensivo de la automatización y la orquestación; para mejorar la eficiencia, reducir los errores y cumplir con las mejores prácticas u objetivos comerciales establecidos.

Protección de Redes De Datos

New J. (2018) manual de redes heterogéneas págs. 72-1 y 72-12. Los controles de acceso son necesarios para evitar el acceso local no autorizado a la red y para controlar el acceso remoto a través de los puertos de acceso telefónico. Los tres niveles mínimos de acceso de usuario generalmente asignados son: acceso público, privado y compartido. El acceso público permite que todos los usuarios tengan acceso de solo lectura a la información del archivo. El acceso privado brinda a usuarios específicos acceso de lectura y escritura de archivos, mientras que el acceso compartido permite que todos los usuarios lean y escriban archivos.

Fibra Óptica Multimodo

Las fibras multimodo (MMF) son un ejemplo de un medio altamente dispersor, que codifica la luz coherente que se propaga dentro de ellas para producir patrones aparentemente aleatorios. Por lo tanto, para aplicaciones tales como formación de imágenes y proyección de imágenes a través de un MMF, se requieren mediciones cuidadosas de la relación entre las entradas y salidas de la fibra. Mostramos, como prueba de concepto, que una red neuronal profunda puede aprender la relación entrada-salida en un MMF de 0,75 m de largo. Específicamente, demostramos que una red neuronal convolucional profunda (CNN) puede aprender las relaciones no lineales entre la amplitud del patrón moteado (pérdida de información de fase) obtenido en la salida de la fibra y la fase o la amplitud en la entrada de la fibra. Efectivamente, la red realiza una tarea de inversión no lineal. Obtuvimos fidelidades de imagen (correlaciones) tan altas como ~ 98% para reconstrucción y ~ 94% para proyección de imagen en el MMF en comparación con la imagen recuperada utilizando el conocimiento completo de la transmisión del sistema caracterizada con la matriz medida compleja. Mostramos además que la red se puede entrenar para transferencia de aprendizaje, es decir, puede transmitir imágenes a través del MMF, que pertenece a otra clase que no se usa para entrenamiento/prueba.

La videovigilancia en los Centro de Datos

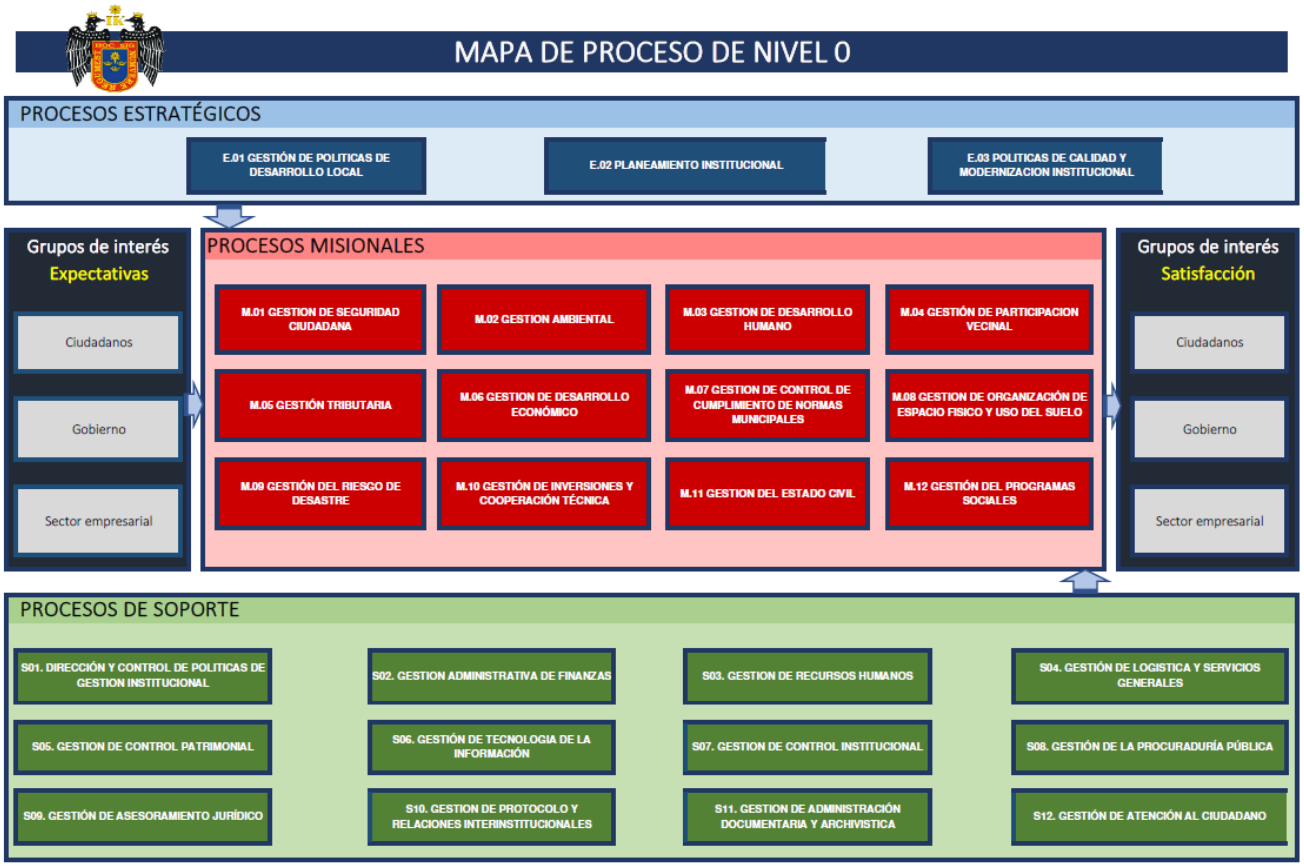
Según Sun, Z., et. al (2016) Transacciones IEEE en circuitos y sistemas para tecnología de video 28 (1), 2605045, págs. 193-205. La videovigilancia requiere almacenar cantidades

masivas de datos de video, lo que resulta en un rápido aumento del consumo de energía de almacenamiento. Con la popularización de la videovigilancia, el almacenamiento ecológico para videovigilancia es muy atractivo. Los métodos de ahorro de energía existentes para el almacenamiento masivo se concentran principalmente en los datos centros, principalmente con acceso aleatorio, mientras que el almacenamiento de videovigilancia tiene características inherentes de carga de trabajo y patrón de acceso, que pueden aprovecharse al máximo para ahorrar más energía. Se propone un diseño dinámico de datos en paralelo parcial (DPPPL) para el almacenamiento de videovigilancia ecológica. Adopta una estrategia paralela parcial dinámica, que asigna dinámicamente el espacio de almacenamiento con un grado apropiado de paralelismo parcial de acuerdo con los requisitos de rendimiento. El paralelismo parcial beneficia la conservación de energía al programar solo discos parciales para trabajar; un grado dinámico de paralelismo puede proporcionar rendimientos apropiados para cargas de trabajo de varias intensidades. DPPDL se evalúa mediante una videovigilancia simulada que consta de 60-300cámarascon 1920 × 1080 píxeles. El experimento muestra que DPPDL es más eficiente desde el punto de vista energético, al tiempo que tolera la falla de un solo disco y proporciona un margen de rendimiento de más del 20 %. En promedio, ahorra un 7 %, 19 %, 31 %, 36 %, 56 % y 59 % más de energía que CacheRAID, Semi-RAID, Hibernator, MAID, eRAID5 y PARAID, respectivamente.

2.3 Información de la Organización

Figura 2

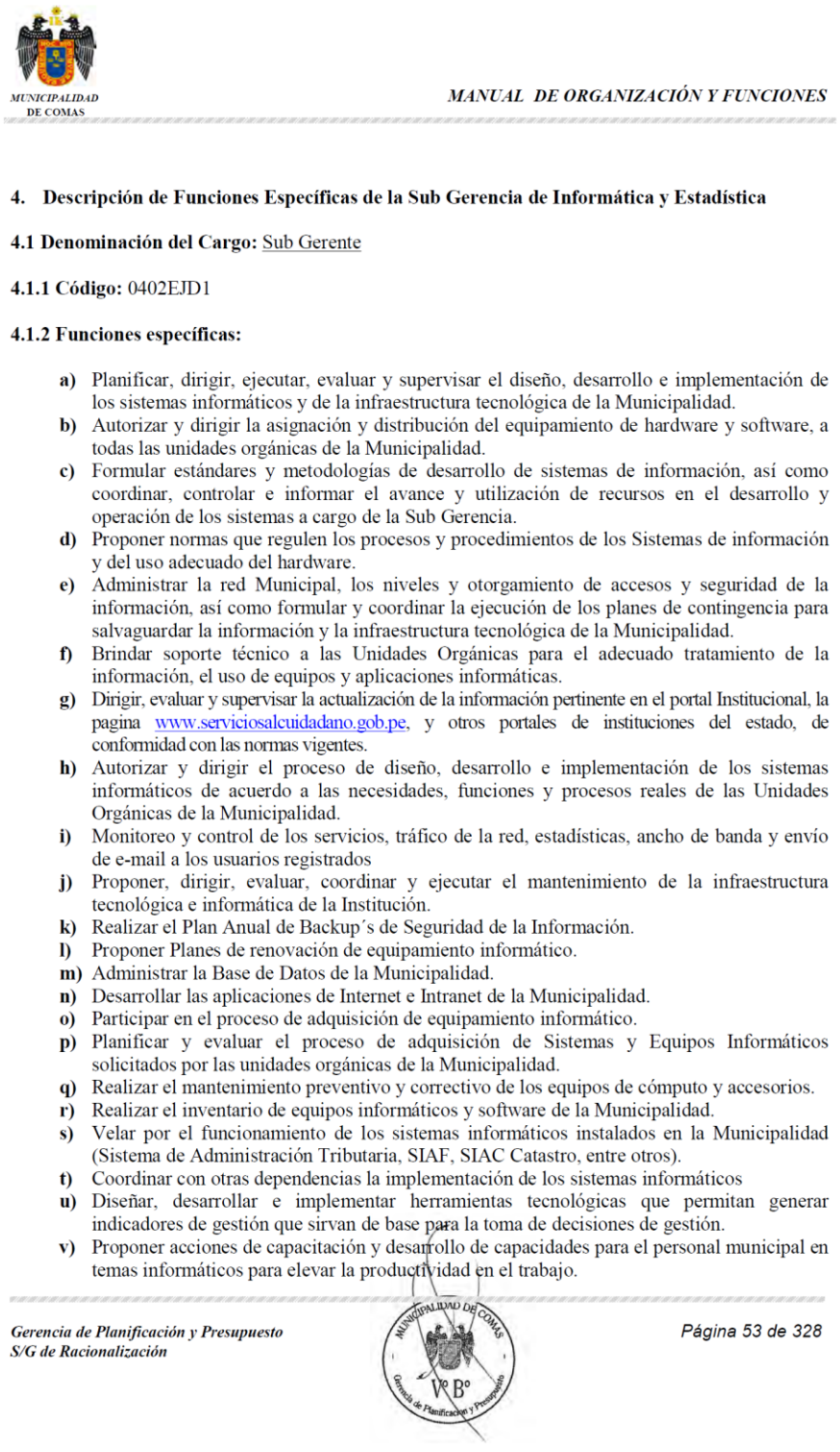
MAPRO (Mapa de Proceso de la Municipalidad Distrital)



Nota: Instrumento administrativo que apoya el que hacer institucional para la coordinación, dirección, evaluación y el control administrativo elaborado por la Municipalidad Distrital extraído del portal web Municomas.gob.pe

Figura 3

MOF (Manual de Organización Y Funciones)



MUNICIPALIDAD DE COMAS

MANUAL DE ORGANIZACIÓN Y FUNCIONES

4. Descripción de Funciones Específicas de la Sub Gerencia de Informática y Estadística

4.1 Denominación del Cargo: Sub Gerente

4.1.1 Código: 0402EJD1

4.1.2 Funciones específicas:

a) Planificar, dirigir, ejecutar, evaluar y supervisar el diseño, desarrollo e implementación de los sistemas informáticos y de la infraestructura tecnológica de la Municipalidad.
b) Autorizar y dirigir la asignación y distribución del equipamiento de hardware y software, a todas las unidades orgánicas de la Municipalidad.
c) Formular estándares y metodologías de desarrollo de sistemas de información, así como coordinar, controlar e informar el avance y utilización de recursos en el desarrollo y operación de los sistemas a cargo de la Sub Gerencia.
d) Proponer normas que regulen los procesos y procedimientos de los Sistemas de información y del uso adecuado del hardware.
e) Administrar la red Municipal, los niveles y otorgamiento de accesos y seguridad de la información, así como formular y coordinar la ejecución de los planes de contingencia para salvaguardar la información y la infraestructura tecnológica de la Municipalidad.
f) Brindar soporte técnico a las Unidades Orgánicas para el adecuado tratamiento de la información, el uso de equipos y aplicaciones informáticas.
g) Dirigir, evaluar y supervisar la actualización de la información pertinente en el portal Institucional, la pagina www.serviciosalcuidadano.gob.pe, y otros portales de instituciones del estado, de conformidad con las normas vigentes.
h) Autorizar y dirigir el proceso de diseño, desarrollo e implementación de los sistemas informáticos de acuerdo a las necesidades, funciones y procesos reales de las Unidades Orgánicas de la Municipalidad.
i) Monitoreo y control de los servicios, tráfico de la red, estadísticas, ancho de banda y envío de e-mail a los usuarios registrados
j) Proponer, dirigir, evaluar, coordinar y ejecutar el mantenimiento de la infraestructura tecnológica e informática de la Institución.
k) Realizar el Plan Anual de Backup´s de Seguridad de la Información.
l) Proponer Planes de renovación de equipamiento informático.
m) Administrar la Base de Datos de la Municipalidad.
n) Desarrollar las aplicaciones de Internet e Intranet de la Municipalidad.
o) Participar en el proceso de adquisición de equipamiento informático.
p) Planificar y evaluar el proceso de adquisición de Sistemas y Equipos Informáticos solicitados por las unidades orgánicas de la Municipalidad.
q) Realizar el mantenimiento preventivo y correctivo de los equipos de cómputo y accesorios.
r) Realizar el inventario de equipos informáticos y software de la Municipalidad.
s) Velar por el funcionamiento de los sistemas informáticos instalados en la Municipalidad (Sistema de Administración Tributaria, SIAF, SIAC Catastro, entre otros).
t) Coordinar con otras dependencias la implementación de los sistemas informáticos
u) Diseñar, desarrollar e implementar herramientas tecnológicas que permitan generar indicadores de gestión que sirvan de base para la toma de decisiones de gestión.
v) Proponer acciones de capacitación y desarrollo de capacidades para el personal municipal en temas informáticos para elevar la productividad en el trabajo.

Gerencia de Planificación y Presupuesto
S/G de Racionalización

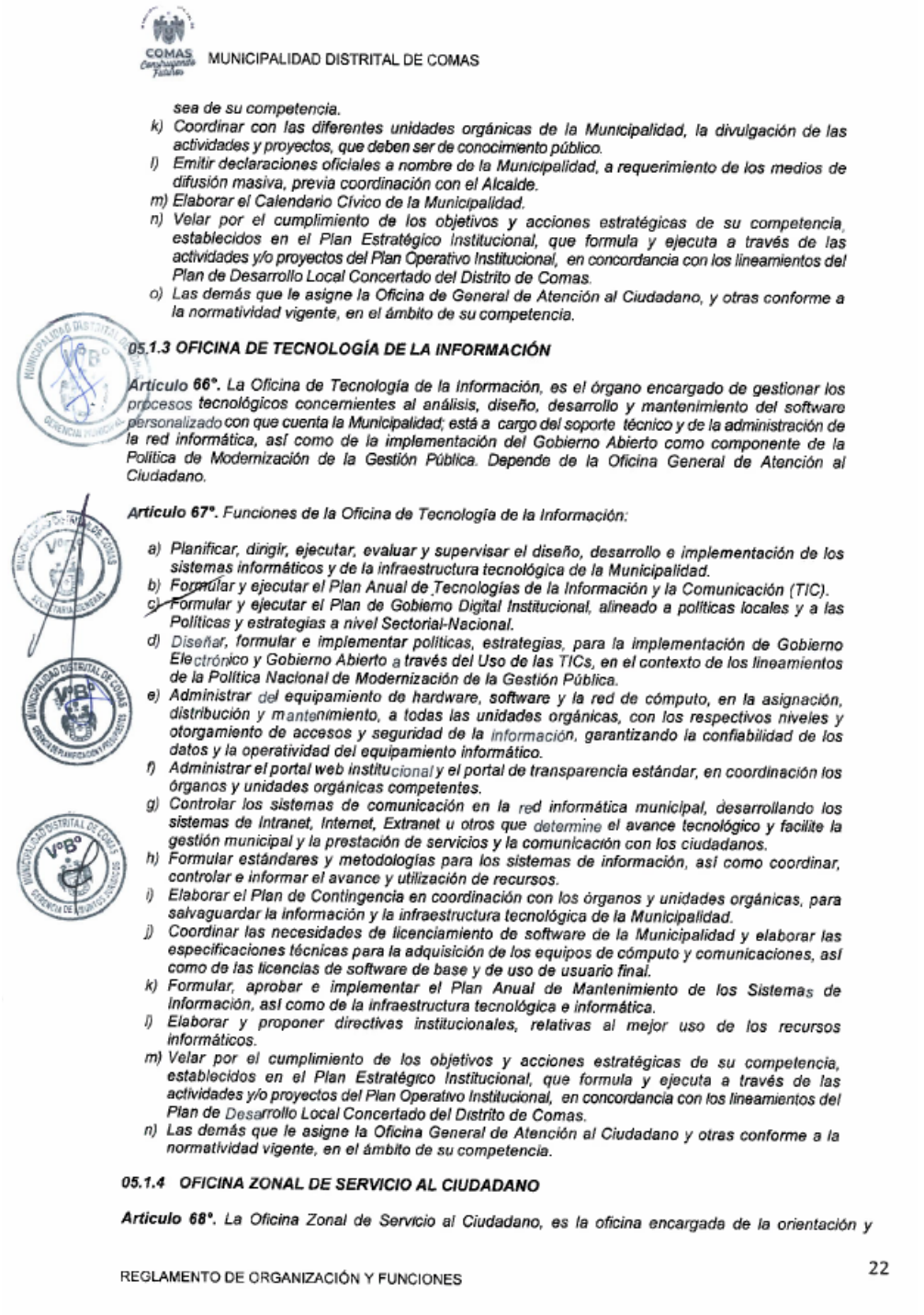
MUNICIPALIDAD DE COMAS
VºBº
Gerencia de Planificación y Presupuesto

Página 53 de 328

Nota: El Manual de Organización y Funciones informe por la resolución de Alcaldia N154-2009-AMC extraído del portal web Municomas.gob.pe p.53

Figura 4

ROF (Reglamento de Organización Y Funciones)



MUNICIPALIDAD DISTRITAL DE COMAS

sea de su competencia.

k) Coordinar con las diferentes unidades orgánicas de la Municipalidad, la divulgación de las actividades y proyectos, que deben ser de conocimiento público.

l) Emitir declaraciones oficiales a nombre de la Municipalidad, a requerimiento de los medios de difusión masiva, previa coordinación con el Alcalde.

m) Elaborar el Calendario Cívico de la Municipalidad.

n) Velar por el cumplimiento de los objetivos y acciones estratégicas de su competencia, establecidos en el Plan Estratégico Institucional, que formula y ejecuta a través de las actividades y/o proyectos del Plan Operativo Institucional, en concordancia con los lineamientos del Plan de Desarrollo Local Concertado del Distrito de Comas.

o) Las demás que le asigne la Oficina de General de Atención al Ciudadano, y otras conforme a la normatividad vigente, en el ámbito de su competencia.

05.1.3 OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

***Artículo 66°.** La Oficina de Tecnología de la Información, es el órgano encargado de gestionar los procesos tecnológicos concernientes al análisis, diseño, desarrollo y mantenimiento del software personalizado con que cuenta la Municipalidad; está a cargo del soporte técnico y de la administración de la red informática, así como de la implementación del Gobierno Abierto como componente de la Política de Modernización de la Gestión Pública. Depende de la Oficina General de Atención al Ciudadano.*

***Artículo 67°.** Funciones de la Oficina de Tecnología de la Información:*

a) Planificar, dirigir, ejecutar, evaluar y supervisar el diseño, desarrollo e implementación de los sistemas informáticos y de la infraestructura tecnológica de la Municipalidad.

b) Formular y ejecutar el Plan Anual de Tecnologías de la Información y la Comunicación (TIC).

c) Formular y ejecutar el Plan de Gobierno Digital Institucional, alineado a políticas locales y a las Políticas y estrategias a nivel Sectorial-Nacional.

d) Diseñar, formular e implementar políticas, estrategias, para la implementación de Gobierno Electrónico y Gobierno Abierto a través del Uso de las TICs, en el contexto de los lineamientos de la Política Nacional de Modernización de la Gestión Pública.

e) Administrar del equipamiento de hardware, software y la red de cómputo, en la asignación, distribución y mantenimiento, a todas las unidades orgánicas, con los respectivos niveles y otorgamiento de accesos y seguridad de la información, garantizando la confiabilidad de los datos y la operatividad del equipamiento informático.

f) Administrar el portal web institucional y el portal de transparencia estándar, en coordinación los órganos y unidades orgánicas competentes.

g) Controlar los sistemas de comunicación en la red informática municipal, desarrollando los sistemas de Intranet, Internet, Extranet u otros que determine el avance tecnológico y facilite la gestión municipal y la prestación de servicios y la comunicación con los ciudadanos.

h) Formular estándares y metodologías para los sistemas de información, así como coordinar, controlar e informar el avance y utilización de recursos.

i) Elaborar el Plan de Contingencia en coordinación con los órganos y unidades orgánicas, para salvaguardar la información y la infraestructura tecnológica de la Municipalidad.

j) Coordinar las necesidades de licenciamiento de software de la Municipalidad y elaborar las especificaciones técnicas para la adquisición de los equipos de cómputo y comunicaciones, así como de las licencias de software de base y de uso de usuario final.

k) Formular, aprobar e implementar el Plan Anual de Mantenimiento de los Sistemas de Información, así como de la infraestructura tecnológica e informática.

l) Elaborar y proponer directivas institucionales, relativas al mejor uso de los recursos informáticos.

m) Velar por el cumplimiento de los objetivos y acciones estratégicas de su competencia, establecidos en el Plan Estratégico Institucional, que formula y ejecuta a través de las actividades y/o proyectos del Plan Operativo Institucional, en concordancia con los lineamientos del Plan de Desarrollo Local Concertado del Distrito de Comas.

n) Las demás que le asigne la Oficina General de Atención al Ciudadano y otras conforme a la normatividad vigente, en el ámbito de su competencia.

05.1.4 OFICINA ZONAL DE SERVICIO AL CIUDADANO

***Artículo 68°.** La Oficina Zonal de Servicio al Ciudadano, es la oficina encargada de la orientación y*

REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES 22

Nota: es el Reglamento de Organización y Funciones de una entidad, que se constituye en un documento técnico normativo de gestión institucional por Ordenanza Municipal N° 656-2023-MDC extraído del portal web Municomas.gob.pe p.22

2.4 Descripción del Puesto

Soporte y Administración de Redes en la Sede de Videovigilancia de la Municipalidad de Comas

El puesto de soporte de redes en un Data center para una sede de videovigilancia se encarga de asegurar el correcto funcionamiento de la infraestructura de redes que conecta los dispositivos de videovigilancia en la sede. Esto incluye la configuración, monitoreo y mantenimiento de los dispositivos de redes, como routers, switches y firewalls, para garantizar una transmisión confiable y segura de los datos de video. Además, este puesto también involucra la resolución de problemas de red y la colaboración con otros departamentos para implementar mejoras en la infraestructura de red. En general, la responsabilidad del soporte de redes en un Data center para una sede de videovigilancia es asegurar una transmisión eficiente y segura de los datos críticos relacionados con la videovigilancia.

Capítulo III: Aporte y desarrollo de la experiencia

3.1 Contextualización

Para poner en contexto el desarrollo de la experiencia profesional en la Implementación del Data Center de la Sede de Monitoreo, este se realizó en el Distrito de Comas – Lima – Perú; iniciando la solución en el año 2017 – y finalizando a su vez con la inauguración de la sede en el año 2021 por el mes de octubre.

La realización de la implementación sucede en acontecimientos con aspectos complicados ya que los años como 2020 se inicia una pandemia global fuera de los factores de muchos proyectos en realización, lo cual hace que se detenga y se avance de forma más lenta así obligando a las empresas y proyectos a que se adecuen al trabajo y todo el personal involucrado tomen medidas de sanidad rígida y obligatoria. En su implementación de la sede de monitoreo y todas sus instalaciones con dos años siguientes para su desarrollo se hacen esfuerzos por parte del Gobierno para reanudar las actividades en el país y diferentes departamentos de manera paulatina.

Todo esto para poder sacar adelante el proyecto y cumplir los objetivos planteados en medidas de seguridad para la población y apoyo a las autoridades competentes con la ayuda de tecnología, dispositivos e infraestructura de vanguardia. Dando Soluciones y resultados contra la baja de la inseguridad en el Distrito proveyéndole más puntos de visualización ante las incidencias de los robos, asaltos, violencia y todo lo que este en contra la perturbación del bienestar de los ciudadanos en el distrito.

Ahora los resultados de la solución e implementación del Centro de Datos dan origen de llevar su gestión y administración de la red teniendo el soporte tecnológico y profesional por parte del equipo de Informática y Gobierno Electrónico.

3.2 Descripción detallada de la Experiencia

A continuación, se hará mención a detalle de la Experiencia laboral en la sede de Monitoreo y Video Vigilancia como soporte y gestión en redes.

Revisión del Data Center

Parte de las funciones de soporte y gestión en la sede de videovigilancia es el ingreso al Data Center y revisar físicamente la funcionalidad de los dispositivos en donde se encuentran instalados:

Una red de tipo POL la cual es la futura red que se va a realizar en las casas que no es más que la penetración a través de la fibra óptica con ONT o ONU y por esos equipos pasan varios servicios, a diferencia de otros distritos que solamente tienen una ONT que solo tiene puertos de internet en el proyecto se implementaron ONT que tienen 2 puertos de telefonía, 4 puertos de internet, 1 puerto de fibra y wifi son equipos que también están implementándose para los hogares.

Lo que se quiere decir es que en cada cámara instalada se podría implementar un puerto telefónico de auxilio o caseta publica si se podría, ya que las ONUs tienen 6 puertos físicos; 2 de telefonía, 4 de Ethernet puerto PON y el wifi (hacer barrido en las OLT para saber cuántas ONUs tienes activas, se realizar mediante consola con línea de comando whatsup gold mapa de topología).

Capa 2 y Capa 3 todo lo que es routing y networking Capa 1 la red PON físicamente

Componente físico que es la parte interna el patch panel como cableado estructurado

Equipo de Voz IPVX antes PVX o IP PVX usa protocolo IP antes tenía que tener un MDF y cable físico.

3 servidores WAFE los servidores de la solución de video vigilancia Y 7 NVRs

La OLT es la que gestiona la red GPON es la central de procesamiento logico de la solución de fibra porque es la que asigna los servicios y recibe la conectividad a través de hilos, pero llega la conectividad física a través de los esplitters que estos están conectados a cada mufa y de la mufa reparte a las cámaras (la concepción lógica es diferente a la concepción física) las OLT gestiona del otro lado las ONU y detrás de las ONU son las cámaras las que están conectadas.

El router MIKROTIC te da los tres servicios el internet, firewall (seguridad gestionada) y la voz.

El servicio de Voz que es importante para la operatividad del centro son las de radio conectados al servicio tetras este está enmarcado a un servicio externo por el ministerio del interior que a su vez están asignadas por la policía nacional. La municipalidad tienes sus propios radios, pero en solicitud al ministerio para inscribirlo en el software que tienen y les da una frecuencia con la empresa Dolfin y poder así activar el servicio.

El data Center no califica ni a un TIER 1 por que como mínimo tendría que tener sus sistema de energía independiente bajo el estándar de la 942 e TIER-A si tuviese un suministro eléctrico propio ya podría tener alimentación propia climatización propia cableado independiente la

infraestructura y sistemas para prevenir un DLP (DATA LOSS PREVENTION) evitar cualquier perdida de información puertos de maquina bloqueados por los videos o tener un DR (DISASTRE RECOVER) administración del centro políticas los de informática velar por la 27001 seguridad de la información poner los lineamientos técnicos y operacionalmente lo determina el centro y normativamente los informáticos lo señalamos.

Parte del monitoreo de los servicios de la red GPON es revisar la accesibilidad a los diferentes dispositivos informáticos que se encuentran instalados como el router de la marca MIKROTIK y que los servicios de internet, la seguridad gestionada y la voz. Conocer de extremo a extremo todos los factores que intervienen en la solución implementada, para poder detectar posibles fallos en los elementos que la componen.

Parte de la administración de los diferentes dispositivos que componen la solución e implementación son las 122 cámaras conectadas a la red que están distribuidas en el distrito, su administración por medio del software Wisenet e instalada por la empresa tercera (TOP SALE). Es el monitoreo de las cámaras y sus diferentes funcionalidades que pasaremos a detallar las más importantes para su gestión.

Cada cámara tiene asignada un IP dentro de la red privada de la solución a la cual podemos acceder por media de las credenciales correspondiente al administrador.

Figura 5

Screem de Software WISENET

Nota: Software Wisenet para la administración de las cámaras de Videovigilancia “Screem tomado de la documentación de la página Wisenet”

Revisión de las Conexión de Cámaras por Software e IP

En cuanto al software para la verificación de las cámaras si están online en los diferentes puntos del Distrito podremos hacer un barrido por medio del nombre, número de cámara o IP de la cual esta asignada dicho dispositivo, pero, aunque es preciso recalcar que cada cámara está asociada a un NVR de los 7 ya mencionados en descripción de arriba del documento de los son los medios por las cuales se accede para poder llegar a ver las diferentes configuraciones que tiene el dispositivo.

Al momento de visualizar o hacer el llamado de uno de los dispositivos podremos hacerlo por medio de la aplicación o por el entorno web que también nos permite acceder a los dispositivos.

Ya estando en acceso a uno de los dispositivos (cámara) podremos tener un listado de funcionalidades y características que mencionaremos y podremos ir modificando según la acción o la configuración que necesitemos para la cámara:

Tenemos las funcionalidades básicas como son las de desplazamiento, acercamiento y alejamiento según sea el caso para la manipulación de la cámara puede ser una multisensor que contiene 5 lentes entre ellas una PTZ para hacer giro de 360° dando un alcance de 100 metros.

La opción Video y audio para poder para poder manejar parámetros de resolución o tipo de tomas específicas.

En la sección Network para configurar o visualizar las direcciones de red y servidor a la que está conectándose el dispositivo.

Una de las partes más avanzada y de mucho interés es la sección de Analítica de la imagen que realiza el software en conjunto con las cámaras instaladas permitiendo sectorizar áreas virtuales para detectar movimientos en lugares específicos.

Ya mostrado uno de los ambientes importantes en la sede de monitoreo se tiene otros como lo son la de Visualizadores, videoteca, sala de crisis, Call Center y el Video Wall.

Parte de las actividades dentro de la sede es realizar un barrido del estado de cámaras, estos varían dependiendo a su tipo de enlace, se tiene por radio enlace o Fibra Óptica.

Al realizar el ingreso a la cámara se verifica si el enlace es estable y los datos como la fecha y su leyenda de ubicación física se encuentran correcto. Si en caso no transmita datos o imagen en línea se procede a revisarlo en el NVR al cual este asignado con su respectivo canal, si que corresponde al ingreso se procede a reiniciar o refrescar la conexión a la cámara.

Si encaso no se pueda acceder se ni en el en vivo ni al NVR se realiza un aviso de revisión de la cámara, pero yendo al punto donde se encuentra ubicado físicamente, pero por lo general si fuera el caso era por el tipo de enlace ya que las cámaras que están por radioenlace tienen una antena a la cual hay que ubicarlo para que realice una buena señal de la onda hacia el otro punto de recepción.

Monitoreo de enlaces en Vivo de Visualizadores por Workstation

En sala de Visualizadores están instaladas 24 Workstation netamente equipadas y orientadas a la actividad de visualización en vivo cada módulo tiene 2 pantallas con resolución Full HD, 1 joystick de mando para el manejo de las cámaras de forma libre, 1 headphone con salida a parlantes instalados cerca de las cámaras 1 anexo de comunicación y la Workstation con componentes robustas como tarjeta de video independiente con salida a puertos Display, para que puedan estar operativas 24/7 los 365 días del año. Parte de las actividades es que presente operatividad constante para su correcto funcionamiento revisando la conexión de las cámaras con la estación de trabajo, al igual con el funcionamiento de los headphone haciendo pruebas de sonido.

Si en el procedimiento de las pruebas de conexión hay alguna interferencia se procede a reiniciar los servicios de manera lógica en la estación de trabajo.

Revisión del Video Wall

Cerca de la sala de visualizadores se encuentra 16 pantallas de 50 pulgadas donde se pueden proyectar las cámaras de los Workstation que están asignadas para observar alguna incidencia en particular.

Cada pantalla conectada por puerto HDMI a dos Workstation cada una teniendo 8 pantallas conectadas por puerto display port usando un adaptador. Son los que van a interactuar para realizar diferentes proyecciones que se realicen durante todo el día.

3.3 Análisis de la Experiencia

Para colocar en contexto la experiencia de los procesos en la sede de Monitoreo y Video Vigilancia era el problema de los constantes apagones de energía que tenía la zona donde se ubicada la sede de Monitoreo y esto sumándole a que los equipos de monitoreo como las Workstations se apagaran y los visualizadores no puedan operar las cámaras que estaban asignadas, también en el data center fue implementado baterías de respaldo con el fin de

proporcionar continuidad de funcionamiento de los servidores, NVRs, switches y demás dispositivos pero que no sucedía con el aire acondicionado que fue instalado en el Data Center porque no estaba adicionado para que sea proveído de ellas, todo esto producía molestias, tanto en los ciudadanos como en la sede además del encargado de dicha sede; causando deterioro de los dispositivos informáticos, la visión para la captura de imágenes por parte de las cámaras instaladas por la zona, también producía momentos de ocio para el personal. Esto hacia que no se cumpliera parte de los objetivos para los que se tenía que cumplir tanto en el día a día como para la Entidad.

Dada esta eventualidad se mencionó como parte de solución adicionar al grupo de batería de respaldo al equipo de enfriamiento del Data Center, así como también los equipos informáticos del grupo de visualizadores, todo con el fin de que se pueda cumplir con los objetivos y se pueda llevar calidad de vida a la comunidad, que es al final es para el cual fue implementado la sede de Videovigilancia.

En cuanto a la conexión de las cámaras del tipo de radio enlace la cual son por antena tiene el problema de no captar bien la señal tanto en la recepción como el envió dejando sin captura en tiempo real a los visualizadores haciendo que el encargado de la sede de monitoreo se cuestione el porque la perdida de conexión, pero por desconocimiento las causas posibles son por clima, perdida de energía, rotación de la antena o talvez la realización de alguna obra por la zona esto hace que los visualizadores no cumplan con los reporte de incidencias y también cabe precisar que la perdida de conexión por las cámaras del tipo radio enlace podría darse en cualquier momento del día, así que como solución propuse tener un personal de soporte en cámaras y de la red que cubriera los turno de tarde y madrugada; así como también personal dedicado al trabajo de campo como es el de ir a revisar las cámaras físicamente si es que no s podía acceder por medio del software y tener como resultado no tener perdida de conexión de los dispositivos.

3.4 Aportes

En el transcurso de la solución ya implementada y en producción se fueron adicionando en las actividades laborales ciertos aportes para la mejora de la administración en la sede como son:

Se llevo un barrido de las cámaras instaladas de su operatividad ya que si bien es cierto hay un software al que podemos darle seguimiento a las configuraciones y conexión de las cámaras, pero esta aplicación no tenía la opción de sacar un reporte de las cámaras por ubicación física

así que se decidió hacer en una hoja de cálculo un registro de incidencias por cámaras en dicha ubicación.

Tener un inventario de los equipos informáticos instalados y que son parte de la solución en la sede de Monitoreo y Video Vigilancia. Tanto un registro físico como también de los aplicativos que se instalaban a los equipos con sus respectivas credenciales si correspondía.

Se realizó un mapeo de las cámaras físicas distribuidas en el distrito por comisarias más cercanas todo esto con el fin de dar apoyo a la rápida respuesta por parte de los visualizadores y tener mejor panorama de las ubicaciones de los dispositivos.

Se procedió a habilitar y asignar una cantidad de espacio de disco en uno de los servidores para que puedan los visualizadores almacenar los distintos reportes diarios con imágenes para las actividades de monitoreo.

Capítulo IV: Propuestas

1. Propuse el de adquirir un software para el tipo de red topológica, esto con el fin de detectar las distintas incidencias que se presenten en la red así agilizar la pronta respuesta a la solución.

Se tendría como Objetivo un software para la gestión eficiente de una red topológica y mejorar la disponibilidad y el rendimiento de los servicios de red.

Alcance:

El proyecto incluirá la adquisición e implementación de un software especializado para la gestión de una red topológica y la configuración de la red para su óptimo funcionamiento. Además, se brindará capacitación al equipo encargado de la gestión de la red y se establecerán procedimientos para la monitorización y el mantenimiento de la red.

El proyecto se llevará a cabo siguiendo una metodología en fases, con una planificación y un cronograma detallados. La metodología incluirá:

Análisis de requisitos: Se realizará un análisis de los requisitos de la red topológica y se definirán las funcionalidades que el software debe tener para su gestión eficiente.

Selección del software: Se realizará una investigación de los diferentes softwares disponibles en el mercado y se seleccionará el que mejor se ajuste a los requisitos de la red topológica.

Implementación del software: Se procederá a la instalación y configuración del software seleccionado, se realizarán pruebas para asegurar su correcto funcionamiento.

Capacitación: Se brindará capacitación al equipo encargado de la gestión de la red para que puedan utilizar eficientemente el nuevo software.

Monitorización y mantenimiento: Se establecerán procedimientos para la monitorización y el mantenimiento de la red, de manera que se garantice su óptimo funcionamiento y disponibilidad.

Los entregables del proyecto serán:

- Informe de análisis de requisitos.
- Software de gestión de red instalado y configurado.
- Documentación de configuración y procedimientos de uso del software.
- Equipo capacitado en el uso del nuevo software.

- Procedimientos para la monitorización y mantenimiento de la red.

La adquisición e implementación de un software para la gestión de una red topológica traerá los siguientes beneficios:

- Mejora en la disponibilidad y el rendimiento de los servicios de red.
- Mayor eficiencia en la gestión de la red topológica.
- Mayor rapidez en la detección y resolución de problemas en la red.
- Reducción de los costos operativos asociados a la gestión de la red.
- Mayor satisfacción de los usuarios de la red.

2. Propuse implementar una solución a las incidencias que se daban durante los turnos ya que los visualizadores lo hacían en un documento Word para luego cargarlos en un compartido de esta manera tener todos los meses indicadores que puedan ayudar a determinar mejor respuesta de acción en las incidencias.

Tendría como Alcance la implementación del proyecto la identificación de las incidencias más comunes, el diseño y la implementación de una solución para su detección y resolución, y la capacitación del personal encargado de la visualización de las cámaras de video vigilancia.

Se llevará a cabo siguiendo una metodología en fases, con una planificación y un cronograma detallados que incluirá:

Identificación de incidencias: Se realizará un análisis de las incidencias que se presentan con mayor frecuencia durante los turnos de visualización de las cámaras de video vigilancia.

Diseño de la solución: Se diseñará una solución para la detección y resolución de las incidencias identificadas, que incluirá herramientas de monitoreo y alerta para el personal encargado de la visualización.

Implementación de la solución: Se procederá a la implementación de la solución diseñada, que incluirá la instalación de herramientas de monitoreo y alerta, así como la configuración de los procesos necesarios para su correcto funcionamiento.

Capacitación: Se brindará capacitación al personal encargado de la visualización de las cámaras de video vigilancia para que puedan utilizar eficientemente la nueva solución implementada.

Monitorización y mejora continua: Se establecerán procedimientos para la monitorización y el seguimiento continuo de la solución implementada, de manera que se puedan detectar y corregir posibles problemas o deficiencias.

Los entregables del proyecto serán:

- Informe de análisis de incidencias.
- Diseño de la solución para la detección y resolución de incidencias.
- Solución implementada y funcionando correctamente.
- Personal capacitado en el uso de la nueva solución.
- Procedimientos para la monitorización y mejora continua de la solución.

La implementación de una solución para la detección y resolución de incidencias en la visualización de cámaras de video vigilancia traerá los siguientes beneficios:

- Reducción de las incidencias en la visualización de las cámaras de video vigilancia.
- Mayor eficiencia en la detección y resolución de las incidencias.
- Mayor seguridad y protección de la población.
- Mayor satisfacción de los usuarios de los servicios de video vigilancia.
- Mejora de la imagen y reputación de la institución encargada de la seguridad.

También propuse tener personal de informática que cubrieran turno por las 24 horas ya que se presentaban incidencias no solo en determinado horario si no en todo el día y así poder tener pronta respuesta a ellos.

Conclusiones

Con la implementación de la solución ya expuesta en capitulo anterior se puede llegar a concluir que se obtuvieron más punto de visión y cobertura en el Distrito cumpliendo con el objetivo de mejorar la colaboración en los sectores y organismos en el Distrito de Comas, reduciendo la inseguridad percibida por la ciudadanía y cooperación activa en las instituciones.

Con la implementación de las cámaras de video vigilancia y el software implementado, se cumple con el objetivo de detectar y prevenir delitos y actividades peligrosas en diferentes puntos y así dar aviso a las autoridades, teniendo la mejora en la seguridad de la población y fortaleciendo a la institución.

En conclusión, el uso de cámaras de seguridad y análisis de datos se ha convertido en una herramienta valiosa para garantizar la seguridad de la población y mejorar las fuerzas de seguridad en la prevención y resolución de delitos. Las cámaras de seguridad pueden ser utilizadas para monitorear áreas críticas y proporcionar una vista en tiempo real de las actividades sospechosas, mientras que el análisis de datos puede ayudar a identificar patrones y tendencias que pueden ser útiles en la planificación de estrategias de seguridad.

Recomendaciones

Para los barridos o reporte de conexión de las cámaras en los diferentes puntos se recomienda obtener una aplicación con más prestaciones de apoyo a la configuración de los dispositivos para que se pueda tener una mejor administración de las cámaras, la red de datos y conexiones que se tiene de forma online (en vivo).

Es recomendable utilizar una herramienta de monitoreo de red en cualquier momento en el que desee asegurarse de que su red está funcionando de manera óptima y no hay problemas que afecten su rendimiento. Esto puede incluir momentos como:

Cuando experimenta problemas de conectividad o velocidad de red.

Cuando necesite asegurarse de que la red cumpla con los requisitos de disponibilidad y rendimiento establecido en su SLA.

Cuando se desee monitorear el uso de ancho de banda y los recursos de red para identificar cuellos de botella y optimizar el rendimiento.

Cuando desee detectar y resolver problemas de seguridad de red, como intrusiones o vulnerabilidades de dispositivos.

Cuando se necesite recopilar información sobre el tráfico de red y los patrones de uso para fines de análisis o planificación de capacidad.

Referencias Bibliográficas

ANSI/BICSI 002-2011. (Marzo de 2011). *Data center design and implementation best practices.* (2. BICSI, Ed.) Committee Approval-January 2011 First Published.

ANSI/BICSI 002-2019. (1 de Mayo de 2019). *ANSI/BICSI.* Obtenido de bicsi.org: https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-2019-data-center-design

Beltran Rondon, G. Y., & Montealegre Cabrera, J. E. (2018). *Implementación de un Sistema de Video Vigilancia bajo el protocolo TCP/IP V4 a traves de redes inalambricas utilizando el estandar 802.11g en el Municipio de Yaguará en el Departamento del Huila.* [Titulo de Especialista]. https://repository.ucc.edu.co/server/api/core/bitstreams/f21bc15b-72d8-45e4-85d8-dbd93ac17e65/content

Booba, B., & Gopal, T. V. (2015). Efficient scheduling of packets in wireless sensor networks using priority based scheduling approach. *Journal of Computer Science*, 137-144. doi:https://doi.org/10.3844/jcssp.2015.137.144

Carmona, D. H. (2011). *Teoria General de Sistemas.* Obtenido de https://books.google.es/books?hl=es&lr=&id=Ww41AwAAQBAJ&oi=fnd&pg=PP16&dq=teoria+de+sistemas+informaticos&ots=Nc0WIG06A_&sig=_JYhEJU4pBgVVGddXdGLk8nCTGs#v=onepage&q=teoria%20de%20sistemas%20informaticos&f=false

Carrión Bravo, M. Á. (2019). *Diseño de una Solución DCIM, basada en herramientas open source para un Centro de Datos experimental.* https://dspace.udla.edu.ec/jspui/bitstream/33000/11388/4/UDLA-EC-TIRT-2019-07.pdf

Castro Castillo, F. E. (2018). *Propuesta de Mejoramiento del Sistema de Video Vigilancia en la Seguridad Ciudadana distrito de la Esperanza 2018.* [Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31223/castro_cf.pdf?sequence=1&isAllowed=y

Chaglla Toaquiza, J. G., Villa Romero, L. M., & Caicedo Altamirano, F. S. (2021). *Estudio técnico de implementación de un sistema de video vigilancia IP para el control de la seguridad de las áreas administrativas, aulas, talleres, laboratorios, etc. En los Campus Centro y Belisario Quevedo de la Universidad De Las Fuerzas Armadas ESPE*. [Informe Monográfico]. http://repositorio.espe.edu.ec/handle/21000/25383

Cooper, M. D. (2018). The Safety Culture Construct: Theory and Practice. En *SpringerBriefs in Applied Sciences and Technology* (págs. 47-61). Springer Nature. doi:https://doi.org/10.1007/978-3-319-95129-4_5

Corzo Quintana, L. J. (2019). *Implementación de una infraestructura tecnológica para servicios de seguridad ciudadana en el distrito de Santiago de Cusco.* [Suficiencia Profesinal]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/2260/Luis%20Corzo_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20PRofesional_2019.pdf?sequence=1

Cui, M., Duan, X., Lu, J., Liu, Y., & Li, Z. (2020). High-speed real-time machine vision detection system based on a tunable pulsed fiber laser. *Optics and Lasers in Engineering*. doi:https://doi.org/10.1016/j.optlaseng.2020.106029

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. E. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers and Security*. doi:https://doi.org/10.1016/j.cose.2020.101713.

Desongles Corrales, J., Ponce Cifredo, E. A., Garzon Villar, L., & Sampalo de la Torre, D. (2006). *Tecnico de Soporte Informatico.* Sevilla: MAD. https://books.google.com.pe/books?id=vbXYgr3AdAkC&pg=PA11&dq=sistema+informatico++teoria+de+sistemas&hl=es419&sa=X&ved=0ahUKEwjMlNiIjMXPAhVGGR4KHRtfCK0Q6AEIHjAB#v=onepage&q=sistema%20informatico%20%20teoria%20de%20sistemas&f=false

Diaz Huarancca, I. A. (2018). *Implementación del Sistema Videovigilancia IP para Mejorar la Seguridad de Activos en una Universidad Pública.* [Informe de Tesis]. https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/831/DIAZ%20HUARANCCA%20Igor%20Alexi.pdf?sequence=1&isAllowed=y

Ding, F., Lv, L., Pan, J., Wan, X., & Jin, X.-B. (2020). Two-stage Gradient-based Iterative Estimation Methods for Controlled Autoregressive Systems Using the Measurement Data. *International Journal of Control, Automation and Systems*. doi:https://doi.org/10.1007/s12555-019-0140-3

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 92-100. doi:https://doi.org/10.1016/j.comcom.2013.11.005.

Dovgyi, S., & Kopiika, O. (2023). Standard Model of System Architecture of Enterprise IT Infrastructure: Lecture Notes in Networks and Systems.

Fatorachian, H., & Kazemi, H. (2021). Impact of Industry 4.0 on supply chain performance. *Journal*. doi:10.1080/09537287.2020.1712487

Ghaemi, M., Hamzeh, A., Ghorbani, A. A., & Menhaj, M. B. (2020). Joint optimization of intrusion detection and traffic engineering in software defined networks. *Journal of Network and Computer Applications*, 166. doi:https://doi.org/10.1016/j.jnca.2020.102678

Gupta, S., & Sharma, K. (2019). Dynamic multilevel priority packet scheduling using hybrid seec. *International Journal of Scientific and Technology Research*, 1149-1154. https://www.scopus.com/record/display.uri?eid=2-s2.0-85075079597&origin=resultslist&sort=r-f&src=s&mltEid=2-s2.0-85032303614&mltType=ref&mltAll=t&imp=t&sid=e3a1bee2f75fa4425da5a3afe2536e39&sot=mlt&sdt=mlt&sl=686&s=REFEID%28%28%222-s2.0-85027561259%22%29+O

Hammadi, A., & Mhamdi, L. (2014). *A survey on architectures and energy efficiency in Data Center Networks.* doi:https://doi.org/10.1016/j.comcom.2013.11.005

Hydeman, M. M., & Swenson, D. E. (2010). Humidity controls for data centers are they necessary. *ASHRAE Journal*. https://www.scopus.com/record/display.uri?eid=2-s2.0-77950659463&origin=resultslist&sort=r-f&src=s&mltEid=2-s2.0-85021800213&mltType=ref&mltAll=t&imp=t&sid=4c3031438d2c5370d6957789eda3de17&sot=mlt&sdt=mlt&sl=244&s=REFEID%28%28%222-s2.0-0003955218%22%29+OR

Hydeman, M., & Swenson, D. E. (2010). Humidity controls for data centers are they necessary. *ASHRAE*, 48-55.

Javed, F., & Akhund, , A. (2021). A novel hybrid machine learning and statistical approach for anomaly detection in software defined networks. *Computers & Security*. doi:https://doi.org/10.1016/j.cose.2021.102231

Jemmali, M., Denden, M., Boulila, W., Jhaveri, R. H., & Gadekallu, T. R. (2022). A Novel Model Based on Window-Pass Preferences for Data Emergency Aware Scheduling in Computer Networks. *IEEE Transactions on Industrial Informatics*, 7880-7888. doi:10.1109/TII.2022.3149896

Manual de Organización y Funciones - MOF. (04 de Febrero de 2009). *Municomas.gob.pe*. Obtenido de Municomas: https://www.municomas.gob.pe/resources/upload/paginas/instrumentos-de-gestion/mof_2009.pdf

Medina Garzón, M. A., & Vásquez Rodríguez, Y. (2020). *Repositorio Institucional*. Obtenido de Diseño de un modelo y sistema que permite determinar el aseguramiento de la información bajo el estándar ISO 27000 en empresas financieras: http://hdl.handle.net/11349/29845

Mokrani Gallego, O. (2021). *Diseño y manejo de infraestructuras de red cumpliendo con los estándares de ciberseguridad.* Obtenido de https://oa.upm.es/66341/

Montero Lopez, G. (2016). *Implementación de un Sistema de Video Vigilancia con Cámaras IP*. [Informe de Actividades Profesionales]. http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/14877/1/Informe.pdf

New Jersey, M. (2018). *Manual de redes Heterogéneas.*

Niles, S. (2015). Standardization and modularity in data center physical infrastructure. *Whitepaper 116, Schneider Electric*. https://em360tech.com/sites/default/files/migration_image/ID%2094%20Schneider%20Electric%201437145595Schneiderwp3.pdf

Normas Legales. (2003, 27 de mayo). *Ley Orgánica de Municipalidades.* Lima: Diario Oficial el Peruano. Obtenido de https://diariooficial.elperuano.pe/pdf/0015/3-ley-organica-de-municipalidades-1.pdf

Normas Legales. (2010, 09 de Noviembre). *faculta a los gobiernos regionales y gobiernos locales a disponer recursos a favor de la Policía Nacional del Perú.* Lima: Diario Oficial el Peruano. https://www.leyes.congreso.gob.pe/Documentos//2006_2011/ADLP/Normas_Legales/29611-LEY.pdf

Normas Legales. (2013, 11 de Febrero). *Ley del Sistema Nacional de Seguridad Ciudadana y su Reglamento.* Lima: Diario Oficial el Peruano. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/331205-27933

Panduit. (2019). *Optimice su Infraestructura. Recuperado el 31 de marzo 2019.* http://www.panduit.com/es/solutions/data-center-solutions/offerings/physical-infrastructure-foundation

PNUD. (10 de Diciembre de 2020). Análisis sobre innovación en seguridad ciudadana y derechos humanos en América Latina y el Caribe. Una perspectiva desde las políticas públicas y la gestión institucional. Ciudad del saber, Panamá, República de Panamá. https://www.undp.org/es/latin-america/publications/an%C3%A1lisis-sobre-innovaci%C3%B3n-en-seguridad-ciudadana-y-derechos-humanos-en-am%C3%A9rica-latina-y-el-caribe

Qiu, T., Zheng, K., Han, M., Philip Chen, C. L., & Xu, M. (Mayo de 2018). *A Data-Emergency-Aware Scheduling Scheme for Internet of Things in Smart Cities.* doi:doi: 10.1109/TII.2017.2763971

Riffan, F., Teguh Kurniawan, M., & Septo Hediyanto, U. Y. (2018). Analisis Cabling Design Consideration Building Automation System Di Data Center Dinas Komunikasi, Informatika Dan Statistik Pemerintah Kabupaten Bandung Menggunakan Standar Ansi/bicsi 002 Dengan Metode Ppdioo. *eProceedings of Engineering, 5(2).*, 3076.

Ruldeviyani, Y., Hadiyanti, R. D., & Sucahyo, Y. G. (2017). Development of data center management evaluation guideline: Case study of BPS-statistics Indonesia. *Journal of Engineering and Applied Sciences*, 2175-2180.

Shekhar, S., Ayyappan, S., Singh, D., Kumar, S., & Kumar, S. (2020). Performance analysis of free space optical communication link under turbulence and pointing errors. *Journal of Optical Communications and Networking*. doi:https://doi.org/10.1364/JOCN.382537

Temoche Vera, A. E. (2019). *Propuesta de Implementación de Data Center en Presta Sullana - Sullana:2019.* [Informe de Tesis]. https://repositorio.uladech.edu.pe/handle/20.500.13032/18478

Trang, S. T., & Brendel, B. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers*, 1265-1284. doi:https://doi.org/10.1007/s10796-019-09956-4

Uptime Institute. (2018). *Infraestructura para Centros de Datos Tier Standard: Topología.* https://es.uptimeinstitute.com/resources/asset/tier-standard-topology-es

Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. *International Journal of Information Management*, 387-394. https://www.sciencedirect.com/science/article/pii/S0268401218302603?via%3Dihub#section-cited-by

Wu, L., & Liu, J. (2021). Multimodal video summarization for IP camera networks. *Journal of Visual Communication and Image Representation*. doi:https://doi.org/10.1016/j.jvcir.2021.103023

Wu, T., Zhang, Z., Sun, M., Chen, X., & Xia, Z. (2021). An improved pre-processing method for IP camera images. *Journal of Physics: Conference Series*. doi:https://doi.org/10.1088/1742-6596/1851/1/012051

Zhang, Y., Ma, S., Wang, X., Wang, Y., & Gao, R. (2021). Fiber optic sensing technology for structural health monitoring of wind turbine blades. *Renewable and Sustainable Energy Reviews*. doi:https://doi.org/10.1016/j.rser.2021.111323

Zhu, Y., & Zheng, W. (29 de Agosto de 2019). Multiple Lyapunov Functions Analysis Approach for Discrete-Time-Switched Piecewise-Affine Systems Under Dwell-Time

Constraints. *IEEE Transactions on Automatic Control*, 2177-2184. doi:10.1109/TAC.2019.2938302