UNIVERSIDAD PRIVADA ANTENOR ORREGO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

TESIS PARA OPTAR POR EL TÍTULO DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

"AUDITORÍA INFORMÁTICA A LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DE LA CENTRAL DE TRÁFICO, RIESGO Y MONITOREO DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DEL PERÍODO ENERO-MARZO DEL 2022"

LÍNEA DE INVESTIGACIÓN: PLATAFORMA TECNOLÓGICA

AUTOR:
Br. Sánchez Castro, Diego Alonso

Jurado Evaluador

Presidente: Ing. Gaytan Toledo Carlos
Secretario: Ing. Vidal Melgarejo Zoraida
Vocal: Ing. Alvarado Rodríguez, Luis

ASESOR:
Ing. Díaz Sanchez, Jaime Eduardo
Código ORCID 0000-0002-8652-0247

TRUJILLO-PERU
2022

Fecha de Sustentación: 2022/12/12

DEDICATATORIA

A dios, por darme la fortaleza y la salud
para continuar y poder permitirme llegar
a esta etapa en mi carrera profesional.

A mi familia, mi pequeño Ivanuel y mi esposa Olga
por acompañarme y brindarme un apoyo incondicional.

A mis padres, Andrés e Yrene, por su
apoyo y respaldo incondicional

A mis hermanos Flor, Giuli y Andrés
por el apoyo y su afecto constante

Y a memoria de mi querido abuelito Manuel
y mi querido Tío Julio que descansan en paz
en el cielo

AGRADECIMIENTO

Comenzando siempre el respectivo agradecimiento a Dios por permitirme tener vida, fuerza y salud y así lograr concluir uno de los mas grandes proyectos en mi carrera profesional el cual al día de hoy está siendo realidad.

A mi familia, mi hijito Ivanuel Sánchez Valdivieso y mi esposa Olga Valdivieso Rodríguez, que me acompañaron en todo momento y darme siempre su apoyo incondicional.

A mis padres Andrés Eleuterio Sánchez Esquivel e Yrene Castro Arica por brindarme su amor, apoyo, comprensión, consejos y educación; ya que nunca se han rendido conmigo y me han acompañado en esta etapa importante en mi vida profesional.

A mis hermanos Flore de María Sánchez Castro, Andrés Sánchez Castro y Giuliana Sánchez Castro, por ser ejemplos de formación profesional, ya que ellos siempre me aconsejaron que con trabajo y esfuerzo se logra el éxito profesional.

Y a mi asesor Ing Jaime Eduardo Diaz Sánchez por ser una guía y transmitirme sus conocimientos correspondientes a mi profesión, y sobre todo su apoyo y paciencia y la gran colaboración para poder realizar esta obra, ya que sin el apoyo correspondiente no hubiera sido posible realizarlo.

“AUDITORÍA INFORMÁTICA A LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DE LA CENTRAL DE TRÁFICO, RIESGO Y MONITOREO DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DEL PERÍODO ENERO-MARZO DEL 2022”

RESUMEN

Por: Br. Sánchez Castro, Diego Alonso

El presente trabajo de tesis es planteado para así poder identificar puntos fuertes y débiles en la gestión de las TI y así poder recomendar mejoras. La investigación surge debido al estado situacional de la CTRM, ya que es notoria la deficiente gestión de las tecnologías de información (TI) y el manejo de la información obtenida del sistema de videovigilancia, las cuales generan un continuo retraso en los procesos y el funcionamiento del área.

El plan de auditoria informática propuesto tiene como base a las Normas Técnica de Control de la Contraloría General de la República, la Directiva N.º 01-2022-JUS/DGTAIPD Tratamiento de Datos Personales Mediante Sistemas de Videovigilancia, la Norma Técnica Peruana ISO/IEC 27007:2015 y otros documentos normativos, con la finalidad de establecer los procedimientos de evaluación y control adecuados y pertinentes.

Luego aplicarse los instrumentos de auditoría se obtuvieron los siguientes puntos débiles de gestión: (1) Mala delegación de las funciones y los cargos que se desempeñan en el área, (2) Problemas en la asignación de acceso al sistema los cuales pueden conllevar a operaciones no autorizadas, (3) Inexistente control de los activos físicos e informáticos que puede conllevar a posibles sanciones legales, (4) Mala gestión del almacenamiento de videos, (5) Falta de mantenimiento preventivo y correctivo los equipos y (6) Incumplimiento de varios documentos normativos relacionados a la gestión de las TI.

En el mismo sentido, se identificaron aspectos positivos: (1) se cuenta con un criterio positivo en el desempeño de las actividades del personal, (2) No se ha logrado detectar un acceso indebido al sistema de cámaras actual ya que solo le es permitido al personal en turno el uso del mismo, (3) Se ah lograr cumplir el

acceso a los videos, en base a los requerimientos que llegan a la CTRM y (4) Se ha logrado tener un correcto control de los equipos evitando las fallas consecutivas.

Se concluye que la gestión de las TI de la CTRM se está ejecutando deficientemente, así mismo, se formulan las recomendaciones necesarias para que los procesos realizados en la CTRM, puedan alinearse de manera correcta y cumplan con las diferentes directivas y estatutos que se evalúan dentro de una unidad del Estado.

Palabras claves: Auditoría, gestión, instrumentos, normatividad, videovigilancia.

"COMPUTER AUDIT OF THE MANAGEMENT OF INFORMATION TECHNOLOGIES OF THE TRAFFIC, RISK AND MONITORING OF THE CENTRAL OFFICE OF THE MUNICIPALIDAD PROVINCIAL DE TRUJILLO, FOR THE PERIOD JANUARY - MARCH 2022"

ABSTRACT

By: Br. Sánchez Castro, Diego Alonso

This thesis work is proposed in order to identify strong and weak points in the management IT and try to recommend improvements. The investigation arises due to the situational state of the CTRM, due to is notorious the poor management of information technologies (IT) and the handling of information obtained from the video surveillance system, which generate a continuous delay in the processes and operation of the area.

This computer audit plan is based on the Technical Control Standards of the Comptroller General of the Republic, Directive N°. 01-2022-JUS/DGTAIPD Processing of Personal Data Through Video Surveillance Systems, the Peruvian Technical Standard ISO/ IEC 27007:2015 and other normative documents, in order to establish the pertinent procedures of evaluation and adequate control.

After applying the audit instruments, it was obtained the following management weaknesses: (1) Poor delegation of functions and positions performed in the area, (2) Problems in the assigning access to the system which can lead to operations unauthorized, (3) Non-existent control of physical and computer assets that can lead to possible legal sanctions, (4) Poor management of video storage, (5) Lack of preventive and corrective maintenance of equipment and (6) Non-compliance with several regulatory documents related to IT management.

In the same sense, it was identified positive aspects: (1) there is a positive criterion in the performance of personal activities, (2) It has not been possible to detect improper access to the camera system, because it is only allowed to the personal on shift the use of the same, (3) It has been possible to comply with the access to the videos, based on the requirements that reach the CTRM, (4) It has been possible to have a correct control of the equipment avoiding consecutive failures.

It is concluded that TI management of the CTRM is being poorly executed, and the necessary recommendations are formulated so that the processes carried out in the CTRM can be aligned correctly and comply with the different directives and statutes that are evaluated within a State.

Keywords: Audit, management, instruments, regulations, video surveillance.

PRESENTACION

SEÑORES MIENBROS DEL JURADO:

Dando cumplimiento al Reglamento de Grados y Titulo de la “Universidad Privada Antenor Orrego”, para optar el título Profesional de Ingeniero de Computación y Sistemas, es grato poner a vuestra consideración, la presenta tesis titulada: **AUDITORÍA INFORMÁTICA A LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DE LA CENTRAL DE TRÁFICO, RIESGO Y MONITOREO DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DEL PERÍODO ENERO-MARZO DEL 2022.**

Este trabajo de investigación es el resultado de esfuerzo, donde he plasmado todos los conocimientos y experiencias adquiridas a lo largo de mi formación profesional, complementando además la orientación y apoyo de mi asesor Ing. Jaime Eduardo Diaz Sánchez y todas aquellas personas que colaboraron durante el desarrollo de la misma.

Atentamente,

Br. Diego Alonso Sánchez Castro

Trujillo, noviembre del 2022

Contenido

I. INTRODUCCION

En el distrito de Trujillo desde aproximadamente el año 2015, hubo una reducción en el índice delictivo, esto es debido a la labor conjunta donde interviene la Municipalidad, la Policía Nacional del Perú, Ministerio Publico, Poder Judicial, Oficina defensorial de la Libertad y las Juntas Vecinales de Seguridad Ciudadana.

Para que se siga cumpliendo los objetivos trazados, es necesario reincidir en el trabajo preventivo que se está realizando por parte de la Municipalidad Provincial de Trujillo (MPT), gracia a la intervención de la Gerencia de Seguridad Ciudadana y Defensa Civil (GSCDC).

A pesar de todo aún existen actos que perjudican la seguridad ciudadana, así como la convivencia pacífica en el distrito de Trujillo, como en el caso de extorsiones, sicariato, como también hurtos y robos en diversas modalidades es por ello que es necesario el lograr fortalecer las acciones necesarias con el fin de poder combatirlos contando con el apoyo de las entidades ya mencionadas, es por ello que surgió e implemento la Central de Trafico, Riesgo y Monitoreo de Trujillo (CTRMT).

La Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo, fue inaugurada el 29 de Setiembre del 2017, con el objetivo de poder fortalecer la seguridad ciudadana en el distrito de Trujillo, mediante la implementación de 65 cámaras, la cuales se encuentran instaladas en puntos estratégicos para así poder ofrecer de manera rápida y eficaz la seguridad de la ciudad.

La CTRMT, cuenta con una completa infraestructura y con el apoyo de un equipo profesional para el uso y manejo de las Cámaras implementadas para así lograr ofrecer un funcionamiento óptimo las 24 horas del día.

Las cámaras implementadas tienen las siguientes características: ángulo de visión de 360 grados, visión nocturna e infrarroja que permite observar en detalle las imágenes nocturnas, al igual que un zoom que

amplifica a la imagen a 300 metros de distancia, permitiendo ubicar aspecto como números de placa, característica de vestimenta, rasgos faciales completos y características físicas, entre otros aspectos.

La CTRMT está conectada mediante fibra óptica instalada en una red de 37 kilómetros al largo de toda la ciudad, permitiendo una transmisión de datos en altas velocidades. Además, este compuesto por un video Wall de alta definición que muestra las imágenes en tiempo real y son almacenadas en el Data Center, el cual posee un sistema que mantiene encendidos los equipos pese a que existan cortos de fluido eléctrico, evitando así perder información importante.

La CTRMT, busca también el poder dar apoyo y tener el apoyo de otras áreas como Seguridad Ciudadana, Defensa Civil y la Central 105 de la Policía.

La situación actual en la CTRMT, es que está presentando un déficit en el funcionamiento tecnológico y el manejo de información, los cuales no permite el funcionamiento óptimo del área, lo cual conlleva a los siguientes problemas:

A nivel de sistema:

- No hay un uso óptimo de un software de grabación. (no es licenciado)
- El almacenamiento de la información se realiza mediante una computadora de escritorio como un servidor temporal
- Se utiliza un sistema gratuito de Hikvision, que no cubre los objetivos del área.

A nivel de usuario:

- Mala gestión de los usuarios para el registro de incidencias
- No se realizó una capacitación del sistema gratuito que se está utilizando actualmente.
- Actualización de cámaras no controlada.

En equipamiento:

- Mala gestión de mantenimiento de las cámaras, hay un promedio de 30 cámaras que se encuentran inoperativas.
- El Data Center no es utilizado adecuadamente para brindar los servicios de red necesarios.
- Hay un promedio de 18 estaciones de trabajo, de las cuales hay un promedio de 4 que no son utilizadas por fallas técnicas por falta de mantenimiento.

Lo descrito conlleva a formular el siguiente problema de estudio *¿Una auditoria informática a la gestión de las tecnologías de información de la Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo facilita la identificación de sus fortalezas y debilidades?*

En el mismo sentido, se formula como objetivo general *"Ejecutar una Auditoría Informática a la Gestión de la Tecnología de Información de la Central de Tráfico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo para identificar sus fortalezas y debilidades, basada en la Norma* NTP-ISO/IEC 27001:2014*".* Y como objetivos específicos:

- Evaluar la *NTP-ISO/IEC 27001:2014* para identificar las etapas y actividades correlacionadas con las Normas de Control Interno del CGR.
- Formular los objetivos de las etapas del modelo de auditoría.
- Formular instrumentos de auditoría acorde las Normas de Control Interno del CGR.
- Aplicar la auditoría para identificar las fortaleza y debilidades de la gestión de TI.

Esta investigación tiene como objetivo el poder planificar y ejecutar una Auditoria a la Gestión de las Tecnologías de Información de la Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo,

para lograr identificar las fortalezas y debilidades, y el nivel de cumplimiento de los objetivos y metas establecidos.
Los aspectos a considerar son:

- **Tecnológico,** se utilizarán herramientas informáticas gratuitas durante el proceso de auditoría.
- **Económico,** no se requiere la asignación de un presupuesto por parte de la MPT, este será asumido por el investigador.
- **Legal,** el modelo propuesto se basará en un estándar internacional ampliamente aceptado y será adoptado a la normativa peruana vigente para infringir la misma.
- **Académico,** el caso de estudio se encuentra dentro del campo de aplicación de los conocimientos teóricos – prácticos de la formación profesional del investigador

Para ello se seguirán los lineamientos establecidos en las Normas Técnicas de Control Interno de la CGR como un marco metodológico; con el apoyo de las Normas Técnicas de Control Interno, vamos a tener un análisis situacional del área, para poder determinar cuáles son los puntos quiebres que se presentan.

Con la información recolectada elaboraremos nuestro Plan de Auditoria, donde estableceremos el alcance, nuestros objetivos, procedimientos de evaluación y un cronograma para la ejecución del nuestro Plan de Auditoria
Como objetivo final presentaremos nuestro Informe Final de Auditoria, en el cual detallaremos todas nuestras observaciones en el proceso de auditoría y la redacción de un informe ejecutivo para la Central de Trafico, Riesgo y Monitoreo.

II. MARCO DE REFERENCIA

2.1. Antecedentes del estudio

- **Rivera & Zambrano** (2015)**,** en su tesis: “Auditoria al Control y Mantenimiento de la Infraestructura tecnológica del departamento tecnológico de la ESPAM MFL”, tiene como objetivo principal: “la evaluación del nivel de cumplimiento de aplicaciones de buenas prácticas, estándares y normas de control interno a nivel informático y tecnológico establecidos en la Contraloría General del Estado Ecuatoriano”. Se concluye que el departamento tecnológico incumple totalmente “con el uso de buenas prácticas, normas y los estándares que dispone la ley; en la aplicación de las técnicas se han identificado que los procesos que se manejan internamente no se encuentran documentados”, causando una gran desinformación en el personal del Departamento Tecnológico, detectando un nivel de riesgo extremadamente alto, es por ello que mediante la aplicación de “la matriz de Riesgo-Confianza del Manual de Contraloría del Estado se determinó que el nivel de riesgo de la Norma Control Interno de TI 410-09 Infraestructura Tecnológica es de 66.43% y el nivel de riesgo de la Norma ISO 27000 es de 65.42%, gracias a ello se han establecido las observaciones y recomendaciones para ser emitidas en el informe final”

- **Diaz & Enriquez**, (2006)**,** en su tesis “Aplicación de una Auditoria informática para la Empresa Comercial Almacenes Oña de la Ciudad de Latacunga”, tiene como objetivo principal “mejorar la eficiencia del servicio informático mediante la aplicación de una Auditoria Informática, utilizando la Metodología COBIT, que permita optimizar el control de servicio informático en los almacenes Oña”. La investigación que se ha realizado ha permitido conocer la situación actual de los recursos informáticos,

controles y el manejo del sistema AFCSYSCO implementado en la institución, gracias al apoyo de la Metodología COBIT. En la investigación realizada ha permitido identificar que en algunos casos los procesos no están debidamente documentados y que no se ha realizado de manera correcta la evaluación del rendimiento del sistema informático, además el sistema de respaldo de la información es deficiente; es por ello que en las observaciones y recomendaciones concluidas plantearemos todas las pautas necesarias para cubrir los problemas identificados, las cuales serán emitidas en el informe final.

- **Gavino Llagas**, (2018), en su tesis "Auditoria en Seguridad Informática y Gestión de Riesgo en el Hospital Regional de Huacho, 2018", tiene como objetivo analizar la auditoria en seguridad informática para determinar su relación con la gestión de riesgo en el Hospital Regional de Huacho, 2018.La Auditoría realizada alcanzo una calificación recomendable para la toma de conciencia sobre la administración de riesgos, como una parte fundamental de las operaciones del departamento, se ha concluido mediante la auditoria el poder definir políticas de evaluación y administración de riesgo, lograra identificar posibles eventos y sus respectivos impactos que puedan afectar el funcionamiento del departamento.

- **Mendoza & Zavaleta** (2015)**,** en su tesis: “Auditoria Informática al Departamento de Informática del Hospital Belén de Trujillo”, tiene como objetivo aplicar una Auditoria Informática a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos en la organización. Se concluyó mediante el desarrollo de la auditoria una desactualización en la documentación disponible así como también la inexistencias de documentos importantes para el desarrollo de las actividades; se detectó la falta de un plan de contingencias que les permita evitar

efectos generados por la ocurrencias de emergencias; a su vez no cuentan con un plan de mantenimiento en el Departamento de informática; mediante todos estos puntos detectados se elevó el Informe de Auditoría a la Gerencia, dando a conocer los resultados de la evaluación de cada uno de los procesos, dejando en claro cómo se encuentra actualmente la entidad en la gestión de TI.

2.2. Marco Teórico

2.2.1. Auditoria

a. Concepto

Según Muñoz (2002, pág. 11), “es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización, y con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y cumplimiento de sus operaciones”.

Piattini Velthuis & Navarro (2000, pág. 4), “indican que la Auditoria es toda, es la actividad que consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple con las condiciones que le han sido prescritas”.

Para Heredero, y otros (2006, pág. 258) establece que es la “revisión, verificación y evaluación con un conjunto de métodos, técnicas y herramientas de los sistemas de información de una organización, de forma discontinua y a petición de su Dirección y con el fin de mejorar su rentabilidad, seguridad y eficacia”.

b. Objetivos Generales de la Auditoria

Para Muñoz (2002, pág. 29), señala los siguientes objetivos que se desarrollan en una Auditoria:

- “Realizar una revisión independiente de las actividades, áreas o funciones específicas de la organización a fin de proporcionar una opinión profesional sobre la solidez de las actividades y resultados.
- Realizar evaluaciones profesionales e independientes de los aspectos contables, financieros y operativos de la empresa.
- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que rigen las actividades de los empleados y funcionarios de la organización, y evaluar las actividades realizadas en sus unidades administrativas.
- Dirigir el desempeño y las operaciones de la empresa con profesionalidad e independencia, así como el desarrollo de las funciones de la empresa y el logro de las metas y operaciones de la empresa.

c. Clasificación de la Auditoría

1. Auditoría Externa

“Definido como una revisión independiente realizada por un profesional de auditoría, con plena discreción y criterio y sin ninguna influencia, para evaluar la eficacia de las actividades, operaciones y funciones realizadas en la empresa que lo contrata, así como la validez de sus estados financieros. La relación laboral del auditor es ajena de la organización donde se realizará la auditoría, lo que permite emitir una opinión libre e independiente”. Muñoz, (2002, pág. 13)

2. **Auditoría Interna**

   “Es la revisión que realiza un profesional de la auditoría, cuya relación de trabajo es directa y subordinada a la institución donde se aplicara la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de sus resultados financieros. El objetivo final es contar con un dictamen interno sobre las actividades de toda la empresa, que permita diagnosticar la actuación administrativa, operacional y funcional de empleados, funcionarios de las áreas que se auditan”. Muñoz (2002, pág. 14)

d. Metodología

Tomando en cuenta la propuesta de Muñoz (2002, pág. 185), la manera genérica los pasos y las fases que se tienen que considerar para la realización del proceso de auditoria:

1. **Planeación**

   Se establecen los siguientes puntos:

   - “Identificar la fuente de la auditoría.
   - La vista previa del área a evaluar.
   - Establecer los objetivos de auditoría.
   - Especificar los puntos a evaluar durante la auditoría.
   - Preparar el plan, programa y presupuesto para la auditoría
   - Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.
   - Especificar los recursos y sistemas informáticos para la auditoría”.

2. **Ejecución**

Se establece lo siguiente:

- “Realizar las acciones programadas para la auditoría.
- Aplicar los instrumentos y herramientas para la auditoría.
- Identificar y elaborar los documentos de desviaciones encontradas.
- Elaborar el dictamen preliminar y presentarlo en discusión.
- Integrar el legajo de papeles de trabajo de la auditoría”.

3. **Dictamen**

Se establece los siguientes puntos:

- “Analizar la información y elaborar un informe de situaciones detectadas.
- Elaborar el dictamen final.
- Presentar el informe de auditoría”.

En la Familia ISO/IEC 27000 relacionada a la Seguridad de la Información se cuenta con la ISO/IEC27007, que “incluye:

- **Gestión del programa de auditoría del SGSI**, en el que se determinar que, cuándo y cómo auditar, gestionar el riesgo de auditoría, nombrar a los auditores adecuados, mejorar continuamente del proceso, etc.
- **Realización de la auditoria relativa al SGSI**, esta incluye la planificación, el proceso de auditoría, la realización de actividades clave, análisis, trabajo de campo, presentación de informes y seguimiento.
- **Gestión de los auditores del SGSI**, las cuales son las competencias, evaluaciones, atributos, etc.”.

El estándar “tiene las siguientes finalidades:

- Corroborar la mitigación realizada por los controles de seguridad de la información sobre los riesgos de la organización.
- que es correcta la relación de los controles de seguridad con la contabilidad general o de los sistemas y procesos de contratación para que los auditores verifiquen los datos.
- Comprobar que las obligaciones contractuales con los proveedores son satisfactorias.
- Realizar una revisión y control por la dirección.
- Operaciones rutinarias del SGSI de una organización para garantizar la buena marcha de la organización.
- Auditar después de producirse incidentes en la seguridad de la información como parte del análisis.
- Generar acciones correctivas".

Publicado en ISOTools (2014)

2.2.2. Gestión

a. Concepto

Según Cansino Muñoz-Repiso (2001, pág. 57), "está basada en la construcción y el asesoramiento específicos, en tratar al público como clientes, motivas la competitividad entre proveedores de servicio, en la descentralización de la toma de decisiones, en mejorar las técnicas de gestión e introducir indicadores eficientes y técnicas de plan corporativista y explotar las practicas gerenciales de recursos humanos privados y los servicios de información".

b. Gestión Pública en el Perú

Encontrado en Gómez (2020), se define "como la comunidad social jurídicamente organizada. Estado es

un concepto político que se refiere a una forma de organización social, económica, política soberana y coercitiva, formada por un conjunto de instituciones que tiene el poder de regular la vida nacional".

Según el Instituto De Ciencias HEGEL (2021), la define "como el conjunto de procesos y acciones que los funcionarios llevan a cabo para administrar adecuadamente los recursos públicos de la entidad en la que laboran y de ese modo puedan cumplir con las metas institucionales. Para ello se debe hacer un uso adecuado, eficiente y óptimo de los recursos económicos, logísticos, físicos, etc., de la entidad. En resumidas cuentas, la Gestión Publica en el Perú es el cómo se manejan los recursos de una entidad pública para cumplir sus objetivos".

2.2.3. Tecnologías de la Información

a. Concepto

Según Heredero, Hermoso Agius, Romo Romero, & Medina Salgado (2019, pág. 22), la define como "un conjunto de dispositivos, soluciones y elementos de tipo hardware, software y de comunicaciones aplicados al tratamiento automático de la información y de la difusión de esta para satisfacer las necesidades de información".

Baca Urbina, Acosta Gonzaga, & Solares Soto (2014, pág. 38), indican que las tecnologías de información se relacionan con el conjunto de funciones de información que son requeridas por las actividades de un proceso de negocio. Los procesos de negocio requieren funciones de información, y la tecnología de información realiza funciones operativas, que apoyan las actividades de los procesos.

b. Características de las Tecnologías de Información

Olmedo Canchola (2017), nos indica las siguientes características fundamentales:

- **"Inmaterialidad,** su materia prima es su información en múltiples códigos y formas.
- **Interconexión,** aunque se presentan por separado, se pueden combinar para expandir sus conexiones.
- **Interactividad,** permite la interacción del sujeto con la maquina y, adaptarse a los diferentes dominios educativos y cognitivos del ser humano.
- **Instantaneidad,** contribuyendo a la velocidad de acceso e intercambio de información.
- **Calidad de imagen y/o sonido,** otorga credibilidad y autenticidad a la información brindad".

c. Clasificación

Encontrado en Rodríguez (2017), las clasifica "desde 2 puntos de vista:

1. Clasificación según un enfoque tecnológico

- **Equipos:** Son recursos de tipo electrónico a los que se les atribuye la adquisición, almacenamiento y exposición de la información, así como también la transmisión o comunicación de la misma.

- **Servicios:** Se refiere a prestaciones cuya base radica en el campo de la electrónica, y las cuales facilitan la adquisición, almacenamiento, tratamiento y exposición de la información, al igual que la transmisión o comunicación de la misma.

2. **Clasificación según el mercado económico de bienes y servicio de la información y comunicaciones**
    - **Mercado de las Telecomunicaciones:** Aquí encontraremos los respectivos mercados de comunicaciones fijas y móviles.
    - **Mercado audiovisual:** Incluye la televisión y la radio.
    - **Mercado de servicios informáticos:** Engloba los ordenadores personales, así como las redes de comunicaciones de datos (internet) y los servidores de mensajería (correo electrónico o email)".

2.3. Marco Conceptual

- **Auditor,** personas que tiene como cargo revisar, examinar, evaluar los resultados de la gestión administrativa y financiera de una dependencia o entidad.
- **Dictamen o Informe de Auditoría,** son las conclusiones del auditor, en la cual se encarga de resaltar las situaciones más relevantes, aquellas que afecten el significativamente al sistema o el entorno físico de una respectiva entidad.
- **Herramientas de Auditoría,** es el conjunto de programas y ayudas que dan asistencia a los auditores de sistemas. Analistas, ingenieros de software, desarrolladores.
- **Procedimientos de Auditoría,** es el conjunto de métodos y técnicas de investigación aplicables a hechos o circunstancias para describir los mismos, así como sus causas y efectos.
- **Seguridad de la Información,** son las medidas, procedimientos y técnicas definidas y aplicadas para controlar y salvaguardar los datos de una organización, ya sean de acceso interno o externo.

- **Plan-Do-Check-Act,** es una técnica de autoevaluación para controlar el buen desenvolvimiento de los procesos y procedimientos implementados en una organización.

2.4. Sistema de Hipótesis

2.4.1. Variable Independiente

Auditoria informática de la Gestión de Tecnología de la Información de la Central de Tráfico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo basada de la ISO/IEC 27007:2015.

2.4.2. Variable Dependiente

La Gestión de las Tecnología de Información de la Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo.

III. METODOLOGIA EMPLEADA

3.1. Tipo y nivel de Investigación

3.1.1. Tipo de Investigación

- Aplicada

3.1.2. Nivel de Investigación

- Descriptiva y documental.

3.2. Población y muestra de estudio

3.2.1. Población

Los procesos de gestión de la Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo.

3.2.2. Muestra

Los procesos de gestión de TI de la Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo.

3.3. Diseño de investigación

El diseño de Investigación será descriptivo y documental.

3.4. Procesamiento y análisis de datos

- Se realizará una encuesta a los Operadores de Cámaras para evaluar si el área les otorga las herramientas necesarias para el desempeño de sus funciones y a su verificar que problemas podemos detectar en la interacción del área con el Operador de Cámaras.
- Se realizará una entrevista a los Encargados de la Central de Trafico, Riesgo y Monitoreo, con el objetivo de comprobar si se cumplen todos los objetivos y metas del área y sus lineamientos establecidos.
- Se realizará una entrevista a el personal que este encargado como Soporte Técnicos en los diferentes

turnos, para obtener información detallada sobre el estado de los equipos informáticos, el sistema y el funcionamiento en conjunto de la Central de Trafico, Riesgo y Monitoreo

- Mediante la Técnica de Observación, se registrará el estado del área competiendo sus equipos, el sistema o software utilizado, papeles de trabajo, etc.
- La información recopilada será clasificada en cuadros y tablas para su mejor comprensión y manejo.
- Se procederá a analizar e interpretar aquellos datos para poder entender plenamente la información y mejorar la investigación.
- Se aplicará estadística descriptiva en la cuantificación de los resultados.

IV. PRESENTACION DE RESULTADOS

4.1. La Central de Trafico, Riesgo y Monitoreo de la MPT

4.1.1. Generalidades o Descripción General

La Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo, fue inaugurada el 29 de Setiembre del 2017, con el objetivo de poder fortalecer la seguridad ciudadana en el distrito de Trujillo, mediante la implementación de 65 cámaras, la cuales se encuentran instaladas en puntos estratégicos para así poder ofrecer de manera rápida y eficaz la seguridad de la ciudad.

La CTRMT, cuenta con una completa infraestructura y con el apoyo de un equipo profesional para el uso y manejo de las Cámaras implementadas para así lograr ofrecer un funcionamiento óptimo las 24 horas del día.

Las cámaras que tiene habilitadas cuentan con un ángulo de visión de 360 grados, visión nocturna e infrarroja que permite observar en detalle las imágenes nocturnas, al igual que un zoom que amplifica a la imagen a 300 metros de distancia, permitiendo ubicar aspecto como números de placa, característica de vestimenta, rasgos faciales completos y características físicas, entre otros aspectos.

El sistema de Monitoreo de Trujillo, está basado en instalaciones tecnológicas con múltiples equipos con terminales GPON y redes LAN, video wall y posiciones de monitoreo, cableado estructurado con tecnología IP, cuyo medio de transmisión son según los lotes de cámara de radio enlace y de fibra óptica.

La mayoría de esta plataforma de comunicaciones está en fibra óptica micro canalizada de tecnología GEPON. La cual asegura el ancho de banda necesario para la transmisión de video en resolución HD sin interrupciones de señal, ya que no se ve afectada ante interferencias radio eléctrica.

4.1.2. Organigrama u Organización

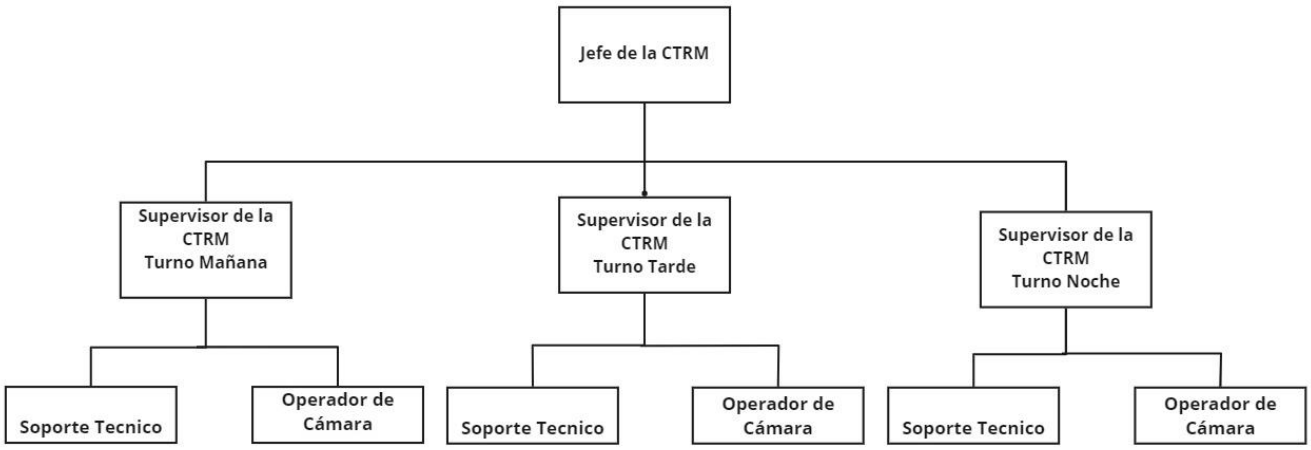


Figura N° 1: Organigrama de la CTRM (no aprobado oficialmente)

4.1.3. Funciones

1. Jefe de la CTRM

- Encargado de dirigir, supervisar y controlar las acciones de la Central de tráfico, riesgo y monitoreo.
- Apoyar en el seguimiento de la ejecución de las metas, fines y objetivos de la Gerencia.
- Controla el cumplimiento de las directivas de carácter interno.
- Participar en los procesos de toma de decisiones en cuanto a Tecnologías de la información de la GSC.

- Participar en la organización y difusión de actividades de la GSC.
- Contribuir en la formulación de planes y su ejecución en la búsqueda de cumplimiento de la misión de Seguridad Ciudadana.
- Proponer proyectos para mejorar la gestión operativa y administrativa de la Gerencia
- Supervisar personal a Cargo.
- Las demás funciones que les corresponden de acuerdo a ley o le asignen sus superiores jerárquicos.

2. Supervisor de la CTRM

- Supervisar al personal asignado al área para el cumplimiento de funciones.
- Supervisar el cumplimiento de los protocolos establecidos para la CTRM.
- Velar por todo el material logístico este en buen estado.
- Verificar el funcionamiento de todos los sistemas existentes de la CTRM.
- Documentar, mediante informes diarios, las actividades realizadas durante la jornada de trabajo.
- Controlar que el personal de la Central acceda la información específica, según el caso.
- Coordinar con las diferentes áreas involucradas.
- Supervisar emergencias monitoreadas por el sistema de videovigilancia
- Supervisar y controlar el buen desempeño de las funciones de los operadores de atención al vecino y monitoreo de video vigilancia.

3. Soporte Técnico

- Realizar inventario de todo el material logístico asignado a la CTRM.
- Verificar y evaluar el cumplimiento de los protocolos de acceso a información necesaria del personal
- Realizar coordinaciones para que el personal acceda a información necesaria para el cumplimiento de labores.
- Coordinar con las áreas competentes para el mantenimiento de limpieza preventivo y correctivo de las cámaras de video vigilancia.
- Identificar oportunamente las posibles fallas en los equipos logísticos (cámaras, teléfonos, radios, etc.) con el fin de efectuar las coordinaciones oportunas
- Verificar que la transmisión de datos en los equipos de cómputo este en buen estado.
- Verificar constantemente el buen estado y funcionamiento del equipamiento de emergencia en las instalaciones de la CTRM.
- Reportar al jefe inmediato las observaciones realizadas por el incumplimiento de protocolos
- Realizar el seguimiento de las unidades mediante el sistema GPS de las radios Tetra.

4. Operador de Videovigilancia

- Conocer las calles avenidas del distrito de Trujillo, así como la ubicación y teléfonos de las instituciones públicas y privadas al servicio de la comunidad.
- Visualizar mediante el monitoreo de las cámaras de videovigilancia en base a los diferentes hechos que puedan ocurrir.
- Realizar consultas mediante internet para la obtención de datos de vehículos y/u personas

sospechosas (Intrasat, SATT, Papeletas, Reniec, etc.)

- Grabar los sucesos importantes y archivarlos en el disco duro de la computadora asignada.
- Comunicar al supervisor las novedades del servicio a fin de que este disponga de las medidas.
- Comunicación constante con los puestos fijos de las novedades que se observan a través de las cámaras de videovigilancia.
- Otras actividades que asigne el jefe inmediato.

4.1.4. Equipamiento Tecnológico

a. Hardware

Actualmente la CTRM cuenta con los siguientes equipos:

- Cuenta con 18 unidades de CPUs Marca DELL color negro.
- Con 1 unidad de CPU HP Z240 SFF WORKSTATION (Servidor).
- Con 3 unidades CPU WORK STATION LENOVO THINKSTATION P340.
- Con 14 Monitores LCD de marca Asus de 23 pulgadas.
- Un Monitor HP, SERIE CN45120LZ1.
- Un Monitor HP, SERIE V6PD678.
- Un Monitor HP SERIE CN45120M9K.
- Un Monitor LED Marca Lenovo de 19 pulgadas.
- Dos Monitores LED Marca Lenovo de 19.5 pulgadas.
- Dos Monitores LED Marca HP Elite Display 19.5 pulgadas.

- Con 20 Teclados USB Color Negro marca DELL.
- Con 3 teclados USB Color Negro marca Lenovo
- Con 21 unidades de Mouse variados.
- Con 1 Modem Movistar color blanco
- Tiene 9 Estabilizadores de voltaje.
- Con 1 Memoria Kingston de 16 GB.
- Una Impresora Multifuncional Ricoh MP 501.

b. Software

Actualmente la CTRM utiliza el programa iVMS-4200 el cual es un software gratuito no licenciado de la marca Hikvision

c. Adicionales

Actualmente cuenta también con los siguientes equipos adicionales:

- Tiene 3 Radios Portátiles de la marca Hytera.
- Un Celular Motorola.
- Tiene 17 Teléfonos IP de marca Grandstream.
- Cuenta con 4 televisores de marca Samsung de 55" UHD.
- Cuenta con 4 equipos de aire acondicionado.
- Tiene 2 Extintores de Gas Carbónico (CO2) de 15 libras.
- Tiene 21 sillas de plástico color blanco.
- Tiene 5 sillas cromadas con forro de tela color negro

4.2. Correlación de las Normas de Control Interno con ISO/IEC 27001:2014 y la Directiva de Videovigilancia

En esta sección se realiza una correlación de los Controles para las Tecnologías de la Información y Comunicaciones de las Normas de Control Interno (Contraloría General de la

República, 2006) con los controles de la Norma Técnica Peruana ISO/IEC 27001:2014 (PERÚ, 2016) y la Directiva de Tratamiento de datos personales mediante sistemas de videovigilancia (Autoridad Nacional de Protección de Datos Personales, 2020).

Los Controles de Tecnología de Información y Comunicaciones establecen que “la información de una organización es proporcionada mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC incluyen datos, sistemas de información, tecnología relacionada, instalaciones y el personal. Las actividades de control de las TIC incluyen controles que aseguran el procesamiento de información para el cumplimiento misional y de los objetivos de la entidad, debiendo diseñarse para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas”.

Al respecto se han formulado 8 comentarios para un mejor entendimiento y son estos lo que son usados para la correlación. En la tabla Nº 1: Correlación de documentos, se muestra la correlación de los tres documentos mencionados anteriormente:

Tabla Nº 1: Correlación de documentos

COMENTARIO DE LAS NORMAS DE CONTROL INTERNO	**NTP/ISO IEC 27001:2014**	**DIRECTIVA DE VIDEOGILANCIA**
1. Los controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad.	A.6.1.1 Funciones y responsabilidades de la seguridad de la información. A.6.1.2 Segregación de tareas.	6.23 Para efectos de un cumplimiento adecuado de las medidas de seguridad dentro del sistema de videovigilancia, es necesaria la implementación de los perfiles definidos en el glosario de la presente directiva, a fin de limitar accesos y gestión de privilegios de los usuarios. 6.26 Las personas que operan o tienen acceso a cualquier sistema de

Tabla Nº 1: Correlación de documentos

COMENTARIO DE LAS NORMAS DE CONTROL INTERNO	NTP/ISO IEC 27001:2014	DIRECTIVA DE VIDEOGILANCIA
		videovigilancia, en razón de sus funciones, son responsables de la facilitación, comercialización, difusión, copia o entrega no autorizadas del contenido de las grabaciones. 6.19 El encargado del tratamiento debe garantizar al responsable que el acceso a los datos sólo se realizará por personas debidamente autorizadas debiendo adoptar las medidas de seguridad necesarias para asegurar el adecuado uso del sistema y tratamiento de los datos personales.
2. Para la puesta en funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas: (i) Definición de los recursos (ii) Planificación y organización (iii) Requerimiento y salida de datos o información (iv) Adquisición e implementación (v) Servicios y soporte (vi) Seguimiento y monitoreo.	A.8.1.1 Inventario de activos A.12.1.1 Documentación de los procedimientos operacionales A.14.1.1 Análisis y especificaciones de los requisitos de la seguridad de la información	6.22.3 Contar con un inventario documentado de las cámaras u otros dispositivos de videovigilancia 6.18 contrato, convenio o documento similar atiende a las circunstancias concretas de la prestación del servicio. El encargado está obligado, en mérito de él, a cumplir con las condiciones técnicas y organizativas necesarias para respetar las obligaciones establecidas en la LPDP; a observar los requisitos legales que lo habilitan para prestar el servicio; a seguir las instrucciones del responsable del tratamiento o del titular del banco de datos; a realizar las acciones necesarias para asistir al responsable o titular del banco de datos en el cumplimiento de su deber de responder frente el ejercicio de los derechos señalados en la LPDP; y, en general, de colaborar en el cumplimiento de las obligaciones del titular del banco de datos.

Tabla Nº 1: Correlación de documentos

COMENTARIO DE LAS NORMAS DE CONTROL INTERNO	NTP/ISO IEC 27001:2014	DIRECTIVA DE VIDEOGILANCIA
		6.22.1 Tener procedimientos de identificación y autentificación de usuarios que den cuenta del funcionamiento del centro de control y monitoreo del sistema de cámaras o videocámaras de videovigilancia, de las partes que lo componen y los equipos.
3. La segregación de funciones implica que las políticas, procedimientos y estructura organizacional estén establecidos para prevenir que una persona controle los aspectos clave de las operaciones de los sistemas, pudiendo así conducir a acciones no autorizadas u obtener acceso indebido a los recursos de información	A.7.2.1 Responsabilidades de la Gerencia A.9.1.1 Política de control de acceso A.9.1.2 Acceso a las redes y a los servicios de las redes	6.23 Para efectos de un cumplimiento adecuado de las medidas de seguridad dentro del sistema de videovigilancia, es necesaria la implementación de los perfiles definidos en el glosario de la presente directiva, a fin de limitar accesos y gestión de privilegios de los usuarios. En el caso de personas jurídicas o naturales que cuenten con un número no superior de ocho cámaras y dos operadores de las mismas, sólo será necesario la determinación del perfil administrador y habilitarse un ambiente aislado o apropiado con mecanismo de control de acceso asignado para el mismo.
4. El control del desarrollo y mantenimiento de los sistemas de información provee la estructura para el desarrollo seguro de nuevos sistemas y la modificación de los existentes, incluyendo las carpetas de documentación de estos. Se requiere definir mecanismos de autorización para la realización de proyectos, revisiones, pruebas y aprobaciones para actividades de desarrollo y modificaciones previas a la puesta en operación de los sistemas. Las decisiones sobre desarrollo propio o adquisición de software deben considerar la satisfacción de las	A.14.1.1 Análisis y especificaciones de los requisitos de la seguridad de la información A.14.2.2 Procedimiento de control de los cambios de sistemas A.14.2.3 Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional A.14.2.9 Revisión de la aceptación del sistema	6.17 Cuando una persona natural, jurídica o entidad pública ha instalado o pretende instalar un sistema de cámaras de videovigilancia, pero encarga a otra la gestión del sistema con utilización de los equipos o acceso a las imágenes o voces, debe de suscribirse un contrato, convenio o documento similar en el que se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos y categorías de interesados, las obligaciones y derechos que correspondan, así como el destino de los datos al finalizar la prestación.

Tabla Nº 1: Correlación de documentos

COMENTARIO DE LAS NORMAS DE CONTROL INTERNO	NTP/ISO IEC 27001:2014	DIRECTIVA DE VIDEOGILANCIA
necesidades y requerimientos de los usuarios, así como el aseguramiento de su operabilidad		
4. Los controles de aplicación incluyen la implementación de controles para el ingreso de datos, proceso de transformación y salida de información, ya sea por medios físicos o electrónicos.	A.8.1.1 Inventario de activos A.9.1.1 Política de control de acceso A.9.4.1 Restricción del acceso a la información A.11.1.3 Seguridad de las oficinas, salas e instalaciones A.12.1.1 Backup de la información A.14.2.2 Procedimiento de control de los cambios de sistemas A.14.2.3 Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional	6.17 Formalidades que debe seguir el encargado del tratamiento 6.19 El encargado del tratamiento debe garantizar al responsable que el acceso a los datos sólo se realizará por personas debidamente autorizadas debiendo adoptar las medidas de seguridad necesarias para asegurar el adecuado uso del sistema y tratamiento de los datos personales.
5. El control específico de las actividades incluye el cambio frecuente de contraseñas y demás mecanismos de acceso que deben limitarse según niveles predeterminados de autorización en función de las responsabilidades de los usuarios. Es importante el control sobre el uso de contraseñas, cuidando la anulación de las asignadas a personal que se desvincule de las funciones	A.9.4.2 Procedimiento seguro de logeo. A.9.4.3 Sistema de gestión de la clave.	6.23 Para efectos de un cumplimiento adecuado de las medidas de seguridad dentro del sistema de videovigilancia, es necesaria la implementación de los perfiles definidos en el glosario de la presente directiva, a fin de limitar accesos y gestión de privilegios de los usuarios.
6. Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con	A.17.1.1 Continuidad de los planes de seguridad de la información A.17.1.2 lmplementación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	6.18 El contrato, convenio o documento similar atiende a las circunstancias concretas de la prestación del servicio. El encargado está obligado, en mérito de él, a cumplir con las condiciones técnicas y organizativas necesarias para respetar las obligaciones establecidas en la LPDP; a observar los requisitos legales que lo habilitan para prestar el servicio; a seguir las instrucciones del responsable del tratamiento o del titular del banco de datos; a realizar las acciones

Tabla Nº 1: Correlación de documentos

COMENTARIO DE LAS NORMAS DE CONTROL INTERNO	NTP/ISO IEC 27001:2014	DIRECTIVA DE VIDEOGILANCIA
el fin de afrontar situaciones de emergencia		necesarias para asistir al responsable o titular del banco de datos en el cumplimiento de su deber de responder frente el ejercicio de los derechos señalados en la LPDP; y, en general, de colaborar en el cumplimiento de las obligaciones del titular del banco de datos
7.El programa de planificación y administración de seguridad provee el marco y establece el ciclo continuo de la administración de riesgos para las TIC, desarrollando políticas de seguridad, asignando responsabilidades y realizando el seguimiento de la correcta operación de los controles	A.5.1.1 Políticas de la seguridad de la información A.5.1.2 Revisión de las políticas de seguridad de la información	6.9 Registro de banco de datos de videovigilancia. La persona natural, jurídica o entidad pública que utilice un sistema de videovigilancia o cualquier dispositivo que permita el tratamiento de datos para dicho fin, debe solicitar la inscripción del banco de datos personales respectivo a la Dirección de Protección de Datos Personales, unidad orgánica de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, encargada de la administración del Registro Nacional de Protección de Datos Personales

4.3. Plan de Auditoria

Todo proceso de auditoria debe estar limitado por su alcance y los objetivos de evaluación de la misma, así como del conjunto de procedimientos y técnicas que se aplicaran. En esta sección se formula este plan para el caso de estudio

4.3.1. Alcance de la Auditoria

De acuerdo a la ISO 19011:2018 se formula el siguiente alcance:

La auditoría se ejecutará en la Central de Trafico, Riesgo y Monitoreo de la MPT abarcando los procesos de Gestión de TI, Servicios de Comunicación y Seguridad de la Información, Servicios de Mantenimiento; para así conocer el cumplimiento de los Controles de Tecnología de Información y Comunicaciones de las Normas de Control Interno de la Contraloría Gerencial de la Republica y su relación con la Norma Técnica Peruana ISO/IEC 27001:2014y la Directiva de Videovigilancia.

4.3.2. Objetivos de la Auditoria

- Evaluar el cumplimiento de la normativa y la directiva vigente en la CTRM.
- Evaluar la disponibilidad de los servicios de comunicación.
- Evaluar las medidas de seguridad que se emplea para mantener la integridad de la información.
- Evaluar el plan de mantenimiento preventivo de la CTRM.
- Evaluar el plan de prevención de daños y perdidas de los activos y equipos de cómputo dentro de la CTRM.
- Evaluar la confidencialidad en los sistemas de la CTRM.

4.3.3. Procedimientos y Evaluación

Se realizará los procedimientos de acuerdo a cada objetivo de Auditoria:

Objetivo 1: Evaluar el cumplimiento de la normativa y directiva vigente en la CTRM.

Procedimientos de Auditoria:

1. Se realizará una entrevista al jefe de la CTRM con el fin de corroborar de que en la actualidad se cumpla con las disposiciones establecidas en la directiva de videovigilancia.
2. Se revisará la documentación elaborada para su cumplimiento y gestión.

Objetivo 2: Evaluar la disponibilidad de los servicios de comunicación.

Procedimientos de Auditoria:

1. Se verificará la existencia de un plan de contingencia en la CTRM y si se ejecuta cuando se necesita.
2. Se verificará si cuenta con un sistema eléctrico de respaldo.
3. Se revisará si cuenta con un sistema de comunicaciones y equipos de respaldo

Objetivo 3: Evaluar las medidas de seguridad que se emplea para mantener la integridad de la información.

Procedimientos de Auditoria:

1. Se verificará si tienen un procedimiento para realizar la copia de seguridad de las bases de datos y archivos.
2. Se realizará pruebas de contenido de los registros desde los sistemas de información y consultado las tablas.

Objetivo 4: Evaluar el plan de mantenimiento preventivo de la CTRM.

Procedimientos de Auditoria:

1. Verificar si existe un plan de mantenimiento preventivo en la CTRM y si es ejecutado cuando es necesario.

2. Solicitar la documentación pertinente para evaluar el grado de eficiencia en la ejecución del mismo.

Objetivo 5: Evaluar el plan de prevención de daños y pérdidas de los activos y equipos de cómputo dentro de la CTRM.

Procedimientos de Auditoria:

1. Verificar que en el Centro de Operaciones y Monitoreo cuenten con la tecnología y los equipos necesarios (cableado, hardware, software) para el funcionamiento continuo y el óptimo proceso de información.
2. Verificar la correcta distribución de los equipos de cómputo dentro del Centro de Operación y Monitoreo.
3. Verificar si cuenta con un generador de respaldo ante cualquier falla prolongada de energía.
4. Verificar si las luces de emergencia se encuentran en funcionamiento.
5. Corroborar si se cuenta con el inventario de los activos y equipos de cómputo dentro del área.
6. Verificar si cuentan con un registro de la salida de equipos en la CTRM.
7. Solicitar el cronograma de mantenimiento preventivo y el informe de ejecución.
8. Verificar si cuenta con un procedimiento de adquisición (activos, equipos de cómputo, software, etc.).

Objetivo 6: Evaluar la confidencialidad de los sistemas de la CTRM.

Procedimientos de Auditoria:

1. Solicitar la documentación de los perfiles de usuarios de los sistemas de información en la CTRM.
2. Verificar el control de acceso de los usuarios a los sistemas de información de la CTRM.

4.3.4. Cronograma de Auditoria

Se realiza en función a los procedimientos y evaluación de cada objetivo, el cual se distribuye en la tabla N.º 2: Cronograma de Actividades de Auditoria que se muestra a continuación:

Tabla N. º 2: Cronograma de Procedimientos de Auditoria

ETAPAS	DESCRIPCION	PROCEDIMIENTOS	INICIO	TERMINO
1	**Requerimiento para el acceso a la información en la CTRM**	Presentar la Carta Nº1-2022-DASC, donde se solicitará la información pertinente con la debida autorización del Gerente de Seguridad Ciudadana.	05.08.2022	05.08.2022
2	**Evaluar el cumplimiento de la normativa y directiva vigente en la CTRM**	Se realizará una entrevista al jefe de la CTRM con el fin de corroborar de que en la actualidad se cumpla con las disposiciones establecidas en la directiva de videovigilancia.	08.08.2022	08.08.2022
		Solicitar la documentación pertinente para evaluar el grado de eficiencia en la ejecución del mismo	10.08.2022	11.08.2022
3	**Evaluar las medidas de seguridad que se emplea para mantener la**	Se verificará si tienen un procedimiento para realizar la copia de seguridad de las bases de datos y archivos.	12.08.2022	12.08.2022

Tabla N. º 2: Cronograma de Procedimientos de Auditoria

ETAPAS	DESCRIPCION	PROCEDIMIENTOS	INICIO	TERMINO
	integridad de la información.	Se realizará pruebas de contenido de los registros desde los sistemas de información y consultado las tablas.	15.08.2022	15.08.2022
4	**Evaluar el plan de mantenimiento preventivo de la CTRM.**	Verificar si existe un plan de mantenimiento preventivo en la CTRM y si es ejecutado cuando es necesario.	16.08.2022	17.08.2022
		Solicitar la documentación pertinente para evaluar el grado de eficiencia en la ejecución del mismo.	17.08.2022	18.08.2022
5	**Evaluar el plan de prevención de daños y perdidas de los activos y equipos de cómputo dentro de la CTRM**	Verificar que en el Centro de Operaciones y Monitoreo cuenten con la tecnología y los equipos necesarios (cableado, hardware, software) para el funcionamiento continuo y el óptimo proceso de información.	19.08.2022	19.08.2022
		Verificar la correcta distribución de los equipos de cómputo dentro del Centro de Operación y Monitoreo.	22.08.2022	22.08.2022
		Verificar si cuenta con un generador de respaldo ante cualquier falla prolongada de energía.	23.08.2022	23.08.2022
		Verificar si las luces de emergencia se encuentran en funcionamiento.	24.08.2022	24.08.2022
		Corroborar si se cuenta con el inventario de los activos y equipos de cómputo dentro del área.	25.08.2022	25.08.2022
		Verificar si cuentan con un registro de la salida de equipos en la CTRM.	26.08.2022	26.08.2022
		Solicitar el cronograma de mantenimiento preventivo y el informe de ejecución.	29.08.2022	29.08.2022

Tabla N. º 2: Cronograma de Procedimientos de Auditoria

ETAPAS	DESCRIPCION	PROCEDIMIENTOS	INICIO	TERMINO
		Verificar si cuenta con un procedimiento de adquisición (activos, equipos de cómputo, software, etc).	31.08.2022	31.08.2022
6	**Evaluar la confidencialidad de los sistemas de la CTRM**	Solicitar la documentación de los perfiles de usuarios de los sistemas de información en la CTRM.	01.09.2022	01.09.2022
		Verificar el control de acceso de los usuarios a los sistemas de información de la CTRM.	02.09.2022	02.09.2022
7	**Redacción del Informe de Auditoria**	Redacción de observaciones	05.09.2022	07.09.2022
		Redacción del informe ejecutivo.	08.09.2022	12.09.2022
		Informe Final del Proceso de Auditoria.	13.09.2022	23.09.2022

4.4. Ejecución del Plan de Auditoria

Tabla N. º 3: Ejecución

FASE	ACTIVIDADES DE AUDITORIA	FECHA DE EJECUCIÓN
1. Levantamiento de información	• Se realizó una entrevista no documentada al Jefe de la CTRM donde se le solicito el poder facilitar algunos documentos para el estudio de los mismos • Se realizo un Check list para la evaluación de la Gestión de Redes y Servidores	05.09.2022
2. Selección de controles	• Análisis de las Normas de Control Interno. • Selección de los controles específicos.	11.10.2022
3. Plan de auditoría	Informe de Plan de Auditoria	14.10.2022

4. Ejecución de la auditoría	Informe de Análisis de Resultados	21.10.2022
5. Elaboración del informe de auditoria	Informe Final del Proceso de Auditoria	28.10.2022

4.4.2. Aplicación de los Procedimientos

En base al Plan de Auditoria, se consideró la ejecución de los procedimientos de la siguiente forma:

1. Se procedió presentar la a Carta N° 01-2022-DASC dirigida al Gerente de Seguridad Ciudadana el Crnl. Alejandro Leoncio Mazuelo Ramos, en la cual se le solicitaba el permiso respectivo para poder ejecutar la Auditoria Informática dentro de la CTRM, en la cual **se recibió de manera aprobatoria las facilidades de acceso a la información y a su vez se llegó en mutuo acuerdo la Confidencialidad de la CTRM a la no publicación de imágenes.**
2. Se realizo un levantamiento de información, en la cual se ejecutó un Check list: “Evaluación de la Gestión Redes y Servidores” y también se realizó una entrevista no documentada al Jefe de la CTRM, donde también nos facilitó la documentación necesaria; adicionalmente se realizó la recopilación de fotos y video para el estudio de la Auditoria Informática que se efectuará en la CTRM.
3. Posterior a la recopilación de la información requerida se procedió con la Selección de los controles reguladores de la Auditoria Informática las cuales son: Las Normas Técnica de Control de la Contraloría General de la República, la Directiva N.º 01-2022-JUS/DGTAIPD Tratamiento de Datos Personales Mediante Sistemas de Videovigilancia, la Norma Técnica Peruana ISO/IEC 27007:2015 y otros documentos normativos.
4. Considerando el punto 2 y 3, se procedió a elaborar el Plan de Auditoria Informática que se ejecutara dónde: Se formulo el alcance, objetivos, procedimientos de evaluación y el cronograma

de ejecución con el objetivo de construir el Informe de Plan de Auditoria.

5. Una vez constituido el informe se ejecutará el Plan de Auditoria donde se aplicará los procedimientos ya establecidos, el acopio de resultados y evidencias y la identificación de puntos fuertes y débiles con el objetivo de realizar el Informe de Análisis y Resultados.
6. En base a todos los procedimientos ya ejecutados se procede con la elaboración del Informe de Auditoría, donde se redactarán las observaciones y la redacción del informe ejecutivo para así obtener el Informe Final de Auditoria.

4.4.3. Acopio de Evidencias y Resultados

En base a la información recolectada se han detectado las siguientes observaciones:

1. **<u>NO SE CUENTA UN MANUAL DE ORGANIZACIÒN Y FUNCIONES APROBADO REALIZÁNDOSE LAS MISMAS DE MANERA EXTRAOFICIAL Y CON RIESGOS DE TRASGEDIR LAS RESPONSABILIDADES O DELEGACIÓN DE FUNCIONES</u>**

   De la revisión de la información requerida mediante la Carta N° 01-2022-DASC, se verifica que se no cuenta un el Manual de Organización y Funciones (MOF) debidamente aprobado por la Municipalidad Provincial de Trujillo.

   Durante la entrevistada realizada el día 01.OCT.2022 al Jefe de la CTRM, este manifiesta que su despacho presentó una propuesta de MOF pero que a la fecha no obtiene la aprobación, tampoco le han hecho de conocimiento si tiene observaciones o sugerido recomendaciones. También que al personal le asignan funciones de dicha propuesta. Finalmente indica que se han formulado funciones para los siguientes puestos jefe, supervisor, operador y soporte

técnico para contribuir en la reducción de riesgos en los procesos, actividades o tareas técnicas especializadas.

Los hechos revelados demuestran que no se cumple con:

- El *control "El titular o funcionario designado debe desarrollar, aprobar y actualizar la estructura organizativa en el marco de eficiencia y eficacia que mejor contribuya al cumplimiento de sus objetivos y a la consecución de su misión"* del punto ***"1.4. Estructura Organizacional"*** que en su *Comentario 3* dice *"Las entidades públicas, de acuerdo con la normativa vigente emitida por los organismos competentes, deben diseñar su estructura orgánica, la misma que no solo debe contener unidades sino también considerar los procesos, operaciones, tipo y grado de autoridad en relación con los niveles jerárquicos, canales y medios de comunicación, así como las instancias de coordinación interna e interinstitucional que resulten apropiadas. El resultado de toda esta labor debe formalizarse en manuales de procesos, de organización y funciones y organigramas"* de las **Normas Técnica de Control** de la **Contraloría General de la República**.
- *El control* ***"A.12.1.1 Documentación de procedimientos operativos"*** *que indica "Se debería documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requirieran"* del *Objetivo de control* ***"A.12.1 Procedimientos y responsabilidades de operación: Asegurar la operación correcta y segura de los recursos de procesamiento de información"***; de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 EDI "Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Información. 2a. edición".

Este incumplimiento generar la existencia de dualidades jerárquicas, el cumplimiento de las funciones, la organización interna del área, la segregación de funciones y la incertidumbre si el número de puestos de trabajos es el adecuado.

Se recomienda reiterar la revisión y aprobación de la propuesta de MOF para la formalización de las funciones y responsabilidades, de esa manera se fortalece y posiciona la Oficina de CTRM al interior de la MPT.

2. **NO SE CUENTA CON DOCUMENTOS DE GESTIÓN (PLANES, PROCEDIMIENTOS Y DIRECTIVAS) NECESARIOS PARA SU CORRECTA GESTIÓN GENERANDO EL RIESGO DE DESGOBIERNO Y DESORDEN DE SUS ACTIVIDADES**

De la revisión de la información requerida mediante la Carta N° 01-2022-DASC, se comprueba que se no cuenta con los siguientes documentos:

- Plan Operativo anual.
- Plan de Continuidad.
- Políticas, normas y directivas de seguridad de la información.
- Plan de Seguridad física y lógica de los equipos e instalaciones.
- Plan de Gestión de Riesgos de Tecnología de la Información.

En la entrevistada realizada el día 01.OCT.2022 al Jefe de la CTRM, este manifiesta que:

- Se desconoce si la Gerencia de Tecnologías de Información de la Municipalidad Provincial de Trujillo ha considerado al área para el cumplimiento del **Decreto Supremo N° 081-2017-PCM** del 08.AGO.2017, denominado “Plan de Transición al Protocolo IPV6” y que debió ser elaborado y puesto en ejecución en el 2018.
- Se carece de personal calificado para la elaboración de dichos documentos y que el personal designado a la oficina se encuentra ocupado en sus funciones, no siendo posible asignarles nuevas.

- Se adolece de un mecanismo de comunicación de la oficina responsable del cumplimiento legal de la MPT para tomar conocimiento de la normatividad vigente que involucre a la Gerencia de Seguridad Ciudadana.

Los hechos revelados demuestran que no se cumple con:

- El control *"Los procesos, actividades y tareas deben estar debidamente documentados para asegurar su adecuado desarrollo de acuerdo con los estándares establecidos, facilitar la correcta revisión de los mismos y garantizar la trazabilidad de los productos o servicios generados"*, del punto ***"3.8. Documentación de procesos, actividades y tareas"***, *y los "Controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad"*, del punto ***"3.10. Controles para las Tecnologías de la Información y Comunicaciones"*** de las **Normas Técnica de Control** de la **Contraloría General de la República**.
- *El control* ***"A.5.1.1 Políticas de la seguridad de la información"*** *que indica "La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información"* del *Objetivo* del control ***"A.5.1 Gestión de la Gerencia para la seguridad de la información: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requisitos del negocio, las leyes y las regulaciones"***, de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 EDI "Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Información. 2a. edición".
- Lo dispuesto en el **Decreto Supremo N° 081-2017-PCM** del 08.AGO.2017, denominado ***"Plan de Transición al Protocolo IPV6"*** que establece un plazo máximo de un (01) año, desde su entrada en vigencia, para la elaboración y aprobación de los respectivos Planes de Transición.

Este incumplimiento genera un escenario de gestión deficiente y errónea del área, en particular, y de la Gerencia de Seguridad Ciudadana, en general.

Se recomendación contratar a personas o empresas especializadas para la elaboración de los documentos de gestión pertinentes, que luego de ser revisados y aprobados por el jefe del área de CTRM, ser presentados a las autoridades correspondientes para su aprobación institucional y posterior implementación.

3. <u>NO SE CUENTA CON UN ADECUADO PROCEDIMIENTO PARA LA GESTIÓN DE USUARIOS, CONTRASEÑAS, ACCESOS A LOS SERVICIOS INFORMÁTICOS, PERFILES DE USUARIO Y NIVELES DE ACCESO GENERANDO EL RIESGO DE ACCESOS Y OPERACIONES NO AUTORIZADAS</u>

De la revisión de la información requerida mediante la Carta N° 01-2022-DASC se verifica que no se cuenta con los siguientes documentos:

- Procedimiento para la Gestión de Usuarios.
- Procedimiento para la Gestión de Contraseñas.
- Procedimiento para la Gestión de Perfiles de Usuarios.
- Procedimiento para la Gestión de Acceso.
- Procedimiento para la Gestión de Privilegios.
- Procedimiento para la Verificación periódica de privilegios.
- Matriz de acceso de usuarios a los recursos y servicios informáticos.
- Registro de operaciones de los procedimientos anteriores.
- Informes de ejecución de operaciones.

En la entrevistada realizada el día 01.OCT.2022 al Jefe de la CTRM, este manifiesta que “un usuario administrador es el responsable de distribuir un usuario en común para cada estación de trabajo, existiendo la posibilidad de asignar a más de una persona si la

computadora es compartida entre ellas". Es decir, un usuario puede ser compartido entre varias personas.

Los hechos revelados demuestran que no se cumple con los Objetivos de Control:

- Con el comentario *"06. El control específico de las actividades incluye el cambio frecuente de contraseñas y demás mecanismos de acceso que deben limitarse según niveles predeterminados de autorización en función de las responsabilidades de los usuarios. Es importante el control sobre el uso de contraseñas, cuidando la anulación de las asignadas a personal que se desvincule de las funciones"* de relacionado a *"Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas"*, del punto ***"3.10. Controles para las Tecnologías de la Información y Comunicaciones"*** de las **Normas Técnica de Control** de la **Contraloría General de la República**.
- Los controles la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 EDI "Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Información. 2a. edición":
  - ***"A.9.1.1 Política de control de acceso"*** y ***"A.9.1.2 Acceso a las redes y servicios de red"*** que indican *"Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información"* y *"Los usuarios deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar",* respectivamente, del *Objetivo de control* ***"A.9.1 Requisitos del negocio sobre control del acceso: Controlar los accesos a la información"***;

- ***"A.9.2.2 Aprovisionamiento de acceso a usuario"*** *y* ***"A.9.2.4 Gestión de información de autenticación secreta de usuarios"***, que indican *"Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios"* y *"Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal",* respectivamente, del *Objetivo de control* ***"A.9.2 Gestión del acceso al usuario: Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios"*** y
- ***"A.10.1.2 Gestión de las claves"*** *que indica "Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida"*, del control ***"A.10.1 Controles de la criptografía: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información"***.

- La **Directiva N° 01-2020-JUS/DGTAIPD**, denominada "Tratamiento de datos personales mediante sistemas de videovigilancia" en los siguientes títulos:
  - ***"Principio de seguridad"*** que en la ***cláusula 6.5*** establece *"El responsable del tratamiento debe adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado"*.
  - ***"Principales obligaciones sobre medidas de seguridad"*** que en la ***cláusula 6.22.1*** establece *"El responsable del tratamiento debe adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida,*

tratamiento o acceso no autorizado", de igual manera en la ***cláusula 6.23*** establece *"Para efectos de un cumplimiento adecuado de las medidas de seguridad dentro del sistema de videovigilancia, es necesaria la implementación de los perfiles definidos en el glosario de la presente directiva, a fin de limitar accesos y gestión de privilegios de los usuarios"*.

Este incumplimiento pone en alto riesgo el contenido de la información pudiendo causar la paralización de las actividades de la CTRM, pérdida, manipulación y acceso indebido a los datos almacenados. También, en sanciones y penalidades de las entidades reguladoras y/o supervisoras.

Se recomiendo al jefe de la CTRM debe presentar un informe detallando la necesidad de contar con los procedimientos mencionados y a la vez, solicitar la contratación de personas o empresas especializadas para la elaboración de los documentos de pertinentes.

4. <u>NO SE CUENTA CON UNA ADECUADA GESTIÓN DEL INVENTARIO DE SOFTWARE DESCONOCIÉNDOSE EL TIPO Y LA CANTIDAD DE CADA UNO DE ELLOS GENERANDO LA POSIBILIDAD DE SANCIONES ECONÓMICAS Y PENALES POR SU USO NO LEGAL</u>

De la revisión de la información requerida mediante la Carta N° 01-2022-DASC no se encuentra el Inventario de Software que es utilizado en el área de CTRM y de la entrevistada realizada el día 01.OCT.2022 al Jefe de la CTRM, este manifiesta que no se cuenta con un uno porque no se les comunica de su adquisición. Al revisar las computadoras se identifica al software iVMS-4200 de Hikvision que es utilizado para conectarse a las cámaras de videovigilancia y son utilizadas por ser gratuitas.

Los hechos revelados demuestran que no se cumple con:

- La ***Resolución Ministerial Nº 073-2004-PCM*** del 14.MAR.2004 denominada ***"Guía para la Administración***

Eficiente del Software Legal en la Administración Pública" que establece:

- ***Artículo 1*** *"Aprobar la Guía para la Administración Eficiente del Software Legal en la Administración Pública elaborada coordinadamente por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI y la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI, que forma parte de la presente resolución",*
- ***Artículo 2*** *"Las entidades de la Administración Pública, integrantes del Sistema Nacional de Informática, deberán aplicar lo establecido en el artículo 1º, siendo responsabilidad de las áreas de informática o de las que hagan sus veces, la implementación y aplicación de la presente norma"*.
- ***Artículo 3*** *"Las áreas de informática, o las que hagan sus veces, desarrollarán acciones informativas y de capacitación dirigidas al personal de cada institución, con el objeto de asegurar la correcta aplicación de lo establecido en el artículo 1º. Para tal efecto, realizarán las coordinaciones correspondientes con las áreas de personal o las que hagan sus veces en la entidad".*

- El control ***"A.8.1.1 Inventario de activos"*** que dice *"Se debe identificar los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos"* del ***Objetivo de Control "A.8.1 Responsabilidad sobre los activos: Identificar los activos de la organización y definir las responsabilidades adecuadas de protección"*** de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 EDI "Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Información. 2a. edición".

La carencia de un Inventario de Software con datos exactos y actualizados debido a una mala Administración de este y la carencia

de un Procedimiento para su Registro como un Activo Intangible de la Municipalidad produce el descontroló de sus instalaciones y versiones y el riesgo de sanciones económicas y penales por su uso no autorizado ni legal.

Se recomienda las siguientes acciones:

- Designar a un Responsable de los Activos Informáticos de la Municipalidad según lo establece la **Norma Técnica Peruana ISO/IEC 27001:2008 "EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos"**.
- Elaborar un Procedimiento para el Registro de Software de la Municipalidad siguiendo la Guía de la **Resolución Ministerial N° 073-2004-PCM del 14.MAR.2004** y tomando en cuenta el **Catálogo de la Superintendencia Nacional de Bienes Estatales**.
- Elaborar un reporte acorde a lo recomendado por la ONGEI.

5. <u>NO SE CUENTA CON UNA ADECUADO PROCEDIMIENTO PARA EL RESPALDO DE LOS VIDEOS GENERANDO LA POSIBILIDAD DE SU PÉRDIDA O DETERIORO Y ALTERACIÓN DE SU CONTENIDO</u>

De la revisión de la información requerida mediante la Carta N° 01-2022-DASC no se encuentra el Procedimiento de Respaldo de los videos obtenidos del Sistema de Videovigilancia.

En la entrevistada realizada el día 01.OCT.2022 al Jefe de la CTRM, este manifiesta que se realiza el siguiente procedimiento:

- Los videos diarios se almacenan en la computadora donde se encuentra instalada la aplicación iVMS-4200 de Hikvision, esta hace la función de servidor.
- Se almacenan en carpetas identificadas por la fecha de grabación y dentro de ella por el número de la cámara.
- Se eliminan cada CUARENTICINCO (45) días para liberar el espacio ocupado y por no haber sido solicitados.

- El acceso a la carpeta de los videos es permitido a todos los usuarios del sistema de videovigilancia.
- Los videos donde se visualizan robos, accidentes u otros eventos son mantenidos hasta que se reciba la orden de eliminación. Esta orden debe ser brindada por el Gerente de Seguridad Ciudadana.

Los hechos revelados demuestran que no se cumple con:

- *El comentario "05. Para el área de producción: En la seguridad física, por medio de restricciones de acceso a la sala de cómputo y procesamiento de datos, a las redes instaladas, así como al respaldo de la información (backup)"*, del Control ***"3.10. Controles para las Tecnologías de la Información y Comunicaciones"*** de las **Normas Técnica de Control de la Contraloría General de la República**.
- *El control "A.12.3.1 Backup de la información"* que dice *"Se debe tomar y poner a prueba de manera regular, el back up de: copias de la información, software e imágenes del sistema, de acuerdo a la política de backup de la organización"*, del *Objetivo de control* ***"A.12.3 Backup: Proteger la información contra la pérdida"***, de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 EDI "Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Información. 2a. edición".
- La **Directiva N° 01-2020-JUS/DGTAIPD**, denominada ***"Tratamiento de datos personales mediante sistemas de videovigilancia***" en el título ***"6.22.6 Principales obligaciones sobre medidas de seguridad"*** que establece *"Cuando corresponda, contar con mecanismos de respaldo de seguridad de la información de carácter personal obtenida a través de sistemas de videovigilancia, así como con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo"*.

Almacenar los videos originales y sus copias de resguardo en un mismo equipo y ambiente es un hecho que podría causar la pérdida

de evidencias importantes requeridas por el Ministerio Público, Poder Judicial y Policía Nacional del Perú, desacreditando el sistema de videovigilancia como medio para hacer frente a la delincuencia y mejora de la seguridad ciudadana.

El jefe de la CTRM debe presentar un informe detallado del actual procedimiento de las Copias de Respaldo (Backups) para solicitar se le asigne los recursos necesarios para realizar las mejoras de seguridad pertinentes y garantizar la protección de los videos y su copia de respaldo. También, solicitar la adquisición del Servicio de Salvaguarda Externa de los mismos para evitar la pérdida de originales y copias.

6. **NO SE CUENTA CON PLANES MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA LOS EQUIPOS DE CÓMPUTO Y CÁMARAS DEL SISTEMA DE VIDEOVIGILANCIA GENERANDO LA POSIBILIDAD DEL DETERIORO DE SU RENDIMIENTO, CALIDAD DE IMAGEN Y SONIDO O PÉRDIDA TOTAL DEL ACTIVO.**

   De la revisión de la información requerida mediante la Carta N° 01-2022-DASC se verifica que el último mantenimiento realizado a un equipo de cómputo se realizó en el 2019, incluso que este no devino de un plan sino de un requerimiento efectuado por un usuario. No se evidencia la formulación de un Plan de Mantenimiento para el Sistema de Videovigilancia, que incluya cámaras, cableado y otros equipos.

   En la entrevistada realizada el día 01.OCT.2022 al Jefe de la CTRM, este manifiesta que:

   - No se cuenta con personal especializado para realizar las actividades de mantenimiento de los equipos de cómputo y al ocurrir una incidencia, se solicita el apoyo de la Gerencia de Tecnología de la Información de la MPT.
   - Para el mantenimiento de las cámaras se contará a un proveedor de servicio, pero que no se cuenta con un calendario o plan de mantenimientos.

Los hechos revelados demuestran que no se cumple con:

- *El comentario "05. Controles para el área de soporte técnico, en el mantenimiento de máquinas (hardware), licencias (software), sistemas operativos, utilitarios (antivirus) y bases de datos. Los controles de seguridad deben proteger al sistema en general y las comunicaciones cuando aplique, como por ejemplo redes instaladas, intranet y correos electrónicos."*, del punto ***"3.10. Controles para las Tecnologías de la Información y Comunicaciones"*** de las **Normas Técnica de Control de la Contraloría General de la República**.
- *El control "A.11.2.4 Mantenimiento de los equipos"* que dice *"Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas"*, del *Objetivo de control* ***"A.11.2 Equipos: Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización"***, de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 EDI "Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Información. 2a. edición".

No brindar mantenimiento a los equipos de cómputo y las cámaras del sistema de videovigilancia generan el riesgo de deterioro o pérdidas de los activos, la baja calidad de los vídeos (imágenes y sonido), también la inoperatividad de los equipos y pérdida de confiabilidad del sistema de seguridad ciudadana.

El jefe de la CTRM debe presentar un informe detallado del actual estado de los equipos de cómputo y las cámaras del sistema de videovigilancia para solicitar se le asigne los recursos necesarios y de esa manera contratar los servicios especializados de mantenimientos de todos esos activos.

4.4.4. Identificación de Puntos Fuertes y débiles

a. Puntos Fuertes

- La CTRM se mantiene operativa a pesar de las deficiencias detectadas, el personal se identifica con la entidad y realiza sus actividades en pro de ella.
- Los requerimientos son atendidos pro activamente por el personal a pesar de sus limitaciones y logrando la disponibilidad de los equipos, así como brindando apoyo en el uso de las aplicaciones.
- El personal cumple con las tareas designadas de manera oportuna y con responsabilidad, a pesar que no se cuenta con un MOF autorizado y vigente. Esto demuestra su compromiso en el cumplimiento de sus labores cotidianas.
- El buen uso y manejo de los equipos del sistema de videovigilancia ha permitido que se mantengan operativos hasta el momento, lográndose todo ello por la capacidad técnica del personal que tiene a su cargo al mismo y al proceso de selección y capacitación que se le brindó al momento de su contratación.

b. Puntos Débiles

- No se cumple con la directiva de videovigilancia N° 01-2020-JUS/DGTAIPD, denominada “Tratamiento de datos personales mediante sistemas de videovigilancia.
- No cuentan con planes de contingencia documentados para las posibles fallas dentro de la CTRM.
- Carece de una designación adecuado con las funciones ejecutadas dentro del área.
- No hay una correcta administración de la plataforma informática dentro del área
- No hay un conocimiento en concreto de la Gestión de los Servicios dentro de la CTRM.
- No se encuentra establecido un control interno de los activos informáticos dentro del área.
- No se gestiona de manera correcta el mantenimiento del equipamiento de la CTRM.

- No se efectúa de manera correcta el resguardo de la información de la CTRM.
- Se corrobora una dependencia total del área de Sistemas de la Municipalidad.

V. DISCUSION DE LOS RESULTADOS

Conforme a las evidencias y resultados obtenidos en la auditoria y luego de haber ejecutado los procedimientos y evaluaciones (Checklist, entrevistas, revisión de documentos, imágenes y videos recopilados), se puede llegar a las siguientes conclusiones de la misma:

- No cumple la normativa y directivas vigentes como: La Directiva N° 01-2020-JUS/DGTAIPD, denominada “Tratamiento de datos personales mediante sistemas de videovigilancia, los Controles para las Tecnologías de la Información y Comunicaciones de las Normas Técnica de Control de la Contraloría General de la República y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, debido que se adolece de comunicación por parte de la MPT, en términos de responsabilidades legales de la CTRM.
- Existe una deficiencia en la disponibilidad de los servicios de comunicación debido al poco respaldo de la MPT en aspecto presupuestales y logísticos.
- La integridad de la información tiene el riesgo de perderse debido a que tanto los datos fuentes como los de respaldo se encuentran en el mismo ambiente. También, porque no se cuenta un procedimiento normalizado para la ejecución de las actividades de copia de respaldo (backups) y restauración (restore).
- El plan de mantenimiento preventivo no está actualizado debido que no se le asigna el debido presupuesto desde la MPT, a pesar de la importancia del sistema de videovigilancia para su gestión e imagen.
- No se cuenta con un plan de prevención de daños y perdidas de los activos y equipos de cómputo, debido que no se le asigna el debido presupuesto desde la MPT.
- Se carece de confidencialidad en los sistemas, debido a que no cuenta con una gestión de acceso para los usuarios y un control de acceso a los sistemas y aplicaciones utilizados en la CTRM

CONCLUSIONES

1. Las Normas de Control Interno de la CGR relacionadas a tecnologías de información y comunicaciones formulan 7 comentarios que han facilitado de manera practica y directa la identificación de 19 controles de la NPT ISO/IEC 27001:2014 y 13 disposiciones de la Directiva de Videovigilancia.

2. Se formularon 6 objetivos de auditoría con la finalidad de evaluar los procesos críticos de la CTRM: cumplimiento de la normativa y directivas vigentes, la disponibilidad de los servicios de comunicación, integridad de la información, confidencialidad de los sistemas, plan de mantenimiento preventivo y el plan de la prevención de daños, con el propósito de establecer una correcta Gestión de TI.

3. Se han elaborado 7 artefactos de auditoria para facilitar la evaluación y el acopio de información de la gestión de TI, estando todos enmarcados en la Directiva N° 01-2020-JUS/DGTAIPD, denominada “Tratamiento de datos personales mediante sistemas de videovigilancia, la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 y las Normas de Control de la CGR.

4. Se han identificado 4 puntos fuertes y 8 débiles lo cual permite afirmar que la Gestión de TI de la CTRM, puede calificarse como deficiente al carecer de apoyo de la MPT, tanto de manera organizacional, legal, presupuestal y operativa.

RECOMENDACIONES

1. Las dependencias u órgano con estructuras y funciones aparentemente descentralizadas, como este caso de la CTRM, no deben carecer del apoyo y gestión de la entidad pública (MPT) por ser parte de su estructura y requiere siempre su supervisión y control.

2. La Gestión de TI de la CTRM, debe estar debidamente alineadas en base a la normativa y directrices vigentes: Directiva N° 01-2020-JUS/DGTAIPD, denominada “Tratamiento de datos personales mediante sistemas de videovigilancia, la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 y las Normas de Control de la CGR, si la CTRM ni cuenta con el personal calificado para la elaboración de los procedimientos y directivas es recomendable la contratación de una persona o empresa para tal efecto.

3. Los planes de mantenimiento preventivo y el plan de prevención de daños y perdidas de activos de cómputo deben encontrarse debidamente actualizados y respectivamente ejecutados, para ello se recomienda la comunicación reiterativa hacia la MPT solicitando el presupuesto adecuado.

4. Fortalecer la integración de la información, mediante la formalización del debido procedimiento para la ejecución de las actividades de copia de respaldo (backups) y restauración (restore); así como también el poder reforzar la confidencialidad de los sistemas de información implementando el debido proceso de gestión de acceso para los usuarios y un control de acceso a los sistemas y aplicaciones utilizados por la CTRM

REFERENCIAS BIBLIOGRAFICAS

Bibliografía

Albi, E., & Onrubia, J. (2015). *ECONOMÍA DE LA GESTION PUBLICA, Cuestiones fundamentales.* Madrid: Ramòn Areces.

Baca Urbina, G., Acosta Gonzaga, E., & Solares Soto, P. F. (2014). *Administracion Informatica I. Análisi y evaluación de tecnologias de información.* Mexico: Grupo Editorial Patria.

Cansino Muñoz-Repiso, J. M. (2001). *Evaluar al Sector Publico Español.* Cadiz: Servicio de Publicaciones de la Universidad de Cadiz.

Colaborador de DocuSign. (2021 de Mayo de 19). *https://www.docusign.mx*. Obtenido de https://www.docusign.mx: https://www.docusign.mx/blog/TICs

CONTRALORIA GENERAL DE LA REPUBLICA. (2006, 03 de Octubre). *NORMAS DE CONTROL INTERNO.* LIMA. Obtenido de www.contraloria.gob.pe

Cronicaglobal. (20 de 03 de 2021). *https://cronicaglobal.elespanol.com*. Obtenido de https://cronicaglobal.elespanol.com: https://cronicaglobal.elespanol.com/business/todo-necesitas-saber-sobre-tecnologia-informacion-ti-nprs_485346_102.html

Diaz, F. M., & Enriquez, D. S. (2006). *AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL.* Latacunga.

Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales . (2020). *DIRECTIVA N° 01-2020-JUS/DGTAIPD TRATAMIENTO DE DATOS PERSONALES MEDIANTE SISTEMAS DE VIDEOVIGILANCIA.*

Garcia, J. (2011). *Videovigilancia: CCTV usando video IP.* España: PUBLICACIONES VÉRTICE S.L.

Gavino Llagas, A. (2018). *AUDITORIA EN SEGURIDAD INFORMÁTICA Y GESTION DE RIESGO EN EL HOSPITAL REGIONAL DE HUACHO, 2018.* Huacho: Universidad Nacional Jose Faustino Sanchez Carrion de Huacho.

Gomez, A. (2011). *Enciclopedia de la Seguridad Informatica.* España: RA-MA S.A. Editorial y Publicaciones.

Gómez, S. (07 de Marzo de 2020). *conociendonuestroderecho.blogspot.com/*. Obtenido de conociendonuestroderecho.blogspot.com/: http://conociendonuestroderecho.blogspot.com/2015/07/estado-concepto-y-elementos.html

Guzmán, C. (s.f.). *blogposgrado.ucontinental.edu.pe*. Obtenido de blogposgrado.ucontinental.edu.pe: https://blogposgrado.ucontinental.edu.pe/el-concepto-de-estado-y-su-evolucion

Heredero, C. D., Hermoso Agius, J. J., Romo Romero, S. M., & Medina Salgado, S. (2019). *Organizacion y transformacion de los sistemas de Informacion en la empresa.* Madrid: ESIC.

Heredero, C., Lopez-Hermoso Agius, J. J., Romo Romero, S. M., Medina Salgado, S., Montero Navarro, A., & Najera Sanchez, J. J. (2006). *Direccion y gestion de los sistemas de informacion en la empresa.* Madrid: ESIC EDITORIAL.

Instituto De Ciencias HEGEL. (11 de Enero de 2021). *hegel.edu.pe*. Obtenido de hegel.edu.pe: https://hegel.edu.pe/blog/gestion-publica-en-peru-que-es-como-se-compone-importancia-etc/

INTPLUS. (19 de Abril de 2017). *http://www.videovigilancia.com/*. Obtenido de http://www.videovigilancia.com/respvideovigilancia.htm

ISOTools. (25 de Junio de 2014). *ISOTools*. Obtenido de ISOTools: https://www.isotools.cl/isoiec-27007/

Mendoza, S., & Zavaleta, F. (2015). *AUDITORIA INFORMATICA AL DEPARTAMENTO DE INFORMATICA DEL HOSPITAL BELEN DE TRUJILLO.* Trujillo.

Muñoz, C. (2002). *Auditoría en sistemas computacionales.* Mexico: Pearson Educacíon.

NORMA INTERNACIONAL ISO/lEC 27001. (2007). *Tecnología de la Información - Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información – Requisitos.* ISO/lEC 27001:2013 (E).

Olmedo Canchola, V. H. (09 de 03 de 2017). *http://www.scielo.org.mx*. Obtenido de http://www.scielo.org.mx: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-72032017000200150#:~:text=Existen%20m%C3%BAltiples%20ejemplos%20de%20TIC,las%20sociedades%20es%20el%20internet.

Piattini Velthuis, M. G., & Navarro, E. d. (2000). *INFORMATICA, un enfoque practico.* España: Ra-Ma.

Rivera, M. V., & Zambrano , M. (2015). *AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL.* Manabi.

Rodriguez, M. (14 de Enero de 2017). *https://tugimnasiacerebral.com*. Obtenido de https://tugimnasiacerebral.com: https://tugimnasiacerebral.com/herramientas-de-estudio/que-son-las-tics-tic-o-tecnologias-de-la-informacion-y-la-comunicacion

Suarez y Alonso, R. C. (2010). *Tecnologías de la Informacion Y la Comunicación.* España: Ideaspropias.

Tamayo, A. (2001). *AUDITORÍA DE SISTEMAS, una visión práctica.* COLOMBIA: UNIVERSIDAD NACIONAL SEDE MANIZALES.

ANEXOS

ANEXO N.º 1: CARTA N.º 01-2022-DASC

CARTA N.º 01-2022-DASC

Trujillo, 05 de agosto de 2022

Señor:

[ ]

Presente. -

Asunto: Requerimiento para el Área de la Central de Trafico, Riesgo y Monitoreo de la Municipalidad Provincial de Trujillo.

De nuestra consideración:

En relación a la Tesis de "**AUDITORIA INFORMÁTICA A LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DE LA CENTRAL DE TRÁFICO, RIESGO Y MONITOREO DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO",** del período enero-marzo 2022, se requiere sirva proporcionar la siguiente información:

1. Inventario de equipos de cómputo especificando características técnicas, usuario y ubicación.
2. Inventario de software indicando licencias, instalaciones y versión.
3. Cronograma de mantenimiento preventivo y el informe de ejecución.
4. Procedimiento de backups. Resguardo Interno y/o Externo, etc.
5. Relación de procesos realizados por el área.
6. Procedimiento de atención de Requerimientos y asignación de activos informáticos.
7. Procedimiento y mecanismos de control en la transmisión de datos.
8. Perfiles de usuario y niveles de acceso.
9. Relación de contratos de adquisición de equipos de cómputo, comunicaciones y software (operativo, de base, aplicativo y utilitario), así como servicio tercerizado.
10. Relación de últimas adquisiciones por software y el destino de los mismos.
11. Relación de Documentación Técnica por sistema (Usuario, Sistemas, Diccionarios, etc.) indicando fecha de actualización.

Agradecemos la atención a la presente, y solicitamos se sirva hacernos llegar a la brevedad posible dicha información.

Atentamente,

MUNICIPALIDAD PROVINCIAL DE TRUJILLO
GERENCIA DE SEGURIDAD CIUDADANA
05 AGO. 2022
Reg.: Folios: 01
Hora: 08.43 Firma:

Diego Alonso Sánchez Castro
DNI: 47049444

ANEXO N.º 2: ACTA DE RELEVO DE LA CTRM

ACTA DE RELEVO DE BIENES Y ENSERES DE LA CENTRAL DE TRÁFICO, RIESGO Y MONITOREO DE SEGURIDAD CIUDADANA - VIDEO CÁMARAS

FECHA: Trujillo, LUNES 01 de AGOSTO del 2022 TURNO: 14:00 - 22:00 HRS.

N° ORD	ARTICULO	MODELO	CODIGO PATRIMONIAL	N° DE SERIE	OBSERVACIONES
01	RADIO PORTÁTIL HANDIE, MARCA HYTERA	PT-580H PLUS	95226965 - 0451	17411A0652	CODIGO 4336158
02	RADIO PORTÁTIL HANDIE, MARCA HYTERA	PT-580H PLUS	95226965 - 0447	17411A0660	CODIGO 4336159
03	CARGADOR DE RADIO PORTATIL HYTERA		SIN CODIGO PAT	17113G2318	
04	CELULAR MARCA MOTOROLA	MOTO E6S	SIN CODIGO PAT		IMEI 355549115786888
05	CARGADOR DE CELULAR MARCA MOTOROLA	USB MICRO	SIN CODIGO PAT		
06	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1572	BN6MF73	ESTACION DE MONITOREO 01
07	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1573	CN6MF73	ESTACION DE MONITOREO 02
08	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1574	JM6MF73	ESTACION DE MONITOREO 03
09	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1575	2N6MF73	ESTACION DE MONITOREO 04
10	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1571	DM6MF73	ESTACION DE MONITOREO 05
11	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1570	7N6MF73	ESTACION DE MONITOREO 06
12	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1569	GM6MF73	ESTACION DE MONITOREO 07
13	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1568	9N6MF73	ESTACION DE MONITOREO 08
14	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1567	HM6MF73	ESTACION DE MONITOREO 09
15	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1566	1P6MF73	ESTACION DE MONITOREO 10
16	CPU HP Z240 SFF WORKSTATION (Servidor)	HP Z240 SFF	74089200 - 0010	2UA5451PLS	ESTACION DE MONITOREO 11
17	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1563	HN6MF73	ESTACION DE MONITOREO 12
18	CPU WORKSTATION LENOVO THINKSTATION P340	P340	74089950 - 1559	MJ0ECA9Z	ESTACIÓN DE MONITOREO 13
19	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1564	6N6MF73	ESTACION DE MONITOREO 14
20	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1565	GN6MF73	ESTACION DE MONITOREO 15
21	CPU MARCA DELL, COLOR NEGRO	OPTIPLEX 3080 SFF	74089950 - 1562	9M6MF73	DEMITRIADES
22	CPU WORKSTATION LENOVO THINKSTATION P340	P340	74089950 - 1560	MJ0ECAA1	SUPERVISIÓN
23	CPU WORKSTATION LENOVO THINKSTATION P340	P340	74089950 - 1561	MJ0ECAA2	USO MY BOY
24	CPU LENOVO THINK CENTRE M9205	M9205	74089950 - 1355		MONITOREO SIPCOP
25	CPU MARCA DELL, DE COLOR NEGRO	OPTIPLEX 3046 MT	74089950 - 1176	6S584J2	DIGITACION SIPCOP
26	CPU MARCA DELL, DE COLOR NEGRO	OPTIPLEX 3046 MT	74089950 - 1180	652G4J2	DIGITACION CMT
27	CPU MARCA DELL, DE COLOR NEGRO	OPTIPLEX 3046 MT	74089950 - 1523		DIGITACION SATURNO
28	CPU MARCA DELL, DE COLOR NEGRO	OPTIPLEX 3046 MT	74089950 - 1177	6S3D4J2	APP BOTON DE PÁNICO
29	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0016	G7LMTJ009996	ESTACION DE MONITOREO 01
30	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0005	G7LMTJ002486	ESTACION DE MONITOREO 02
31	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0010	G7LMTJ009985	ESTACION DE MONITOREO 03
32	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0004	G7LMTJ009999	ESTACION DE MONITOREO 04
33	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0001	G7LMTJ009997	ESTACION DE MONITOREO 05
34	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0013	G7LMTJ009983	ESTACION DE MONITOREO 06
35	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0003	G7LMTJ009984	ESTACION DE MONITOREO 07
36	MONITOR HP, SERIE CN45120LZ1		74088037 - 0094	CN45120LZ1	ESTACION DE MONITOREO 08
37	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0014	G7LMTJ010000	ESTACION DE MONITOREO 09
38	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0012	G7LMTJ010006	ESTACION DE MONITOREO 10
39	MONITOR LENOVO, SERIE V6PD678	TINKVISION	74087700 - 0560	V6PD678	ESTACION DE MONITOREO 11
40	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0008	G7LMTJ009998	ESTACION DE MONITOREO 12
41	MONITOR LED, MARCA HP ELITE DISPLAY, DE 23 PULGADAS	E233	74088037 - 0537	CNCO2319CC	ESTACIÓN DE MONITOREO 13
42	MONITOR LED, MARCA HP ELITE DISPLAY, DE 23 PULGADAS	E233	74088037 - 0536	CNCO2319CG	ESTACIÓN DE MONITOREO 13
43	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0009	G7LMTJ009995	ESTACIÓN DE MONITOREO 14
44	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0015	G7LMTJ010011	ESTACION DE MONITOREO 15
45	MONITOR W-LED MARCA HP, DE 24 PULGADAS	ELITEDISPLAY E241I	74088037 - 0100	CN45120LZ2	DIGITACION SIPCOP
46	MONITOR W-LED MARCA HP, DE 24 PULGADAS	ELITEDISPLAY E241I	74088037 - 0092	CN4512L1Z13	MONITOREO SIPCOP
47	MONITOR LCD, MARCA LENOVO, 19 PULGADAS	L197WA	74087700 - 0376	V1AK178	DIGITACION CMT
48	MONITOR LCD, MARACA LENOVO, DE 19.5 PULGADAS	LT20135WA	74088037 - 0103	V5A48423	DIGITACIÓN CMT
49	MONITOR LED, MARCA LENOVO, DE 19.5 PULGADAS	E2054A	74088037 - 0363	VKW03739	DIGITACIÓN SATURNO
50	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0011	G7LMTJ010008	DEMITRIADES
51	MONITOR LED, MARCA HP ELITE DISPLAY, DE 23"	E233	74088037 - 0535	CNCO2319CB	SUPERVISIÓN
52	MONITOR LED, MARCA HP ELITE DISPLAY, DE 23"	E233	74088037 - 0534	CNCO2319CW	SUPERVISIÓN
53	MONITOR LCD, MARCA ASUS DE 23 PULGADAS	MX239H	95225835 - 0006	G7LMTJ009987	APP BOTON DE PÁNICO
54	MONITOR HP, SERIE CN45120M9K		74088037 - 0046	CN45120M9K	USO MY BOY
55	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1624		APP BOTON DE PÁNICO
56	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1676	0AD-01FH-A04	ESTACIÓN DE MONITOREO 01
57	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1671	0AD-01F5-A04	ESTACIÓN DE MONITOREO 02
58	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1673	0AD-01FN-A04	ESTACIÓN DE MONITOREO 03
59	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1672	0AD-01FO-A04	ESTACIÓN DE MONITOREO 04
60	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1674	0AD-00I7-A04	ESTACIÓN DE MONITOREO 05
61	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1675	0AD-01FL-A04	ESTACIÓN DE MONITOREO 06
62	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1677	0AD-01FG-A04	ESTACIÓN DE MONITOREO 07
63	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1678	0AD-00IA-A04	ESTACIÓN DE MONITOREO 08
64	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1679	0AD-00YH-A04	ESTACIÓN DE MONITOREO 09
65	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1680	0AD-00YJ-A04	ESTACIÓN DE MONITOREO 10

ANEXO N.º 3: ACTA DE RELEVO DE LA CTRM

N° ORD.	ARTICULO	MODELO	CODIGO PATRIMONIAL	N° DE SERIE	OBSERVACIONES
66	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1684	0AD-00JX-A04	ESTACIÓN DE MONITOREO 11
67	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1625		ESTACIÓN DE MONITOREO 12
68	TECLADO USB COLOR NEGRO, MARCA LENOVO		74089500 - 1669	00FD	ESTACIÓN DE MONITOREO 13
69	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1623		ESTACIÓN DE MONITOREO 14
70	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1681	0AD-00I4-A04	ESTACIÓN DE MONITOREO 15
71	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1619		MONITOREO SIPCOP
72	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1682	0AD-01GL-A04	DIGITACIÓN SIPCOP
73	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1621		DIGITACION SATURNO
74	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1631		DIGITACION CMT
75	TECLADO USB COLOR NEGRO, MARCA DELL		74089500 - 1683	0AD-01FK-A04	DEMITRIADES
76	TECLADO USB COLOR NEGRO, MARCA LENOVO		74089500 - 1670	00CX	SUPERVICIÓN
77	TECLADO USB COLOR NEGRO, MARCA LENOVO		74089500 - 1668	00BT	USO MY BOY
78	21 MOUSE VARIOS		SIN CODIGO PAT		DISTRIBUIDO EN CADA ESTACION
79	01 MODEM MOVISTAR, COLOR BLANCO		SIN CODIGO PAT	252184065320	"OJOS DE TRUJILLO"
80	ESTABILIZADOR DE VOLTAJE, EIDA POWER		46225215 - 0843		DATA CENTER
81	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1411	214715801992	ESTACIÓN 02
82	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1410	214715801987	ESTACIÓN 03
83	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1409	214715801991	ESTACIÓN 04
84	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1408	214715777227	ESTACIÓN 05
85	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1415	214715801990	ESTACIÓN 07
86	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1412	214715777225	ESTACIÓN 11
87	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1413	214715777228	ESTACIÓN 13
88	ESTABILIZADOR DE VOLTAJE, FORZA POWER TECHNOLOGIES	FVR-2202	46225215 - 1414	214715801989	ESTACIÓN 15
89	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0357	20EZOXWN1082D1F5	ESTACIÓN 01
90	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0347	20EZOXWN1082D1F7	ESTACIÓN 02
91	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0343	20EZOXWN1082D254	ESTACIÓN 03
92	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0354	20EZOXWN1082D103	ESTACIÓN 04
93	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0358	20EZOXWN1082D1FF	ESTACIÓN 05
94	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0342	20EZOXWN1082D1F8	ESTACIÓN 06
95	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0350	20EZOXWN1082D1EF	ESTACIÓN 07
96	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0346	20EZOXWN1082D267	ESTACIÓN 08
97	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0345	20EZOXWN1082D26C	ESTACIÓN 09
98	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0341	20EZOXWN1082D258	ESTACIÓN 10
99	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0359	20EZOXWN1082D1EC	ESTACIÓN 11
100	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0352	20EZOXWN1082D1FD	ESTACIÓN 12
101	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0356	20EZOXWN1082D1FO	ESTACIÓN 13
102	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0344	20EZOXWN1082D1E6	ESTACIÓN 14
103	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0360	20EZOXWN1082D1F9	ESTACIÓN 15
104	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0349	20EZOXWN1082D1F3	DIGITACIÓN CMT
105	TELEFONO IP, MARCA GRANDSTREAM	GXP1630	95228287 - 0351	20EZOXWN1082D1F1	MY. BOY
106	IMPRESORA MULTIFUNCIONAL, RICOH MP 501	MP 501	74222358 - 0093	G988X582815	
107	MEMORIA USB KINGSTON (metalica) DE 16 GB.			04854-316 A01LF	
108	EXTINTOR DE GAS CORBONICO (CO2), DE 15 LIBRAS		88222525-0278		1RA COLUMNA SALA MONITOREO
109	EXTINTOR DE GAS CORBONICO (CO2), DE 15 LIBRAS		88222525-0090		3RA COLUMNA SALA MONITOREO
110	21 SILLAS DE PLÁSTICO DE COLOR BLANCO		SIN CODIGO PAT		
111	02 ENGRAMPADORAS TIPO ALICATE, DE METAL		SIN CODIGO PAT		01 grande y 01 pequeño - MALOS
112	02 PERFORADORAS DE METAL				01 grande y 01 pequeño
113	01 LINTERNA LED RECARGABLE PALUX DE 2 W				
114	01 BANDEJA DE METAL CON GRASS SINTÉTICO				para desinfección del personal
115	01 TAPIZÓN COLOR NEGRO				para limpieza de los zapatos
116	05 SILLAS FIJAS DE METAL, CROMADAS CON FORRO DE TELA COLOR NEGRO				SILLAS REPARADAS (02 MALA)
117	04 EQUIPOS DE AIRE ACONDICONADO, MARCA MCQUAY.				Instalados en la sala de monitoreo
118	TELEVISOR MARCA SAMSUNG, SMART TV DE 55" UHD	UN55KU6000G	95228586 - 0009		EN RACK DE TV WALL
119	TELEVISOR MARCA SAMSUNG, SMART TV DE 55" UHD	UN55KU6000G	95228586 - 0010		EN RACK DE TV WALL
120	TELEVISOR MARCA SAMSUNG, SMART TV DE 55" UHD	UN55KU6000G	95228586 - 0011		EN RACK DE TV WALL
121	TELEVISOR MARCA SAMSUNG, SMART TV DE 55" UHD	UN55KU6000G	95228586 - 0012		EN RACK DE TV WALL

ENTREGA CONFORME

RECIBE CONFORME

ANEXO N.º 3: CONTRATACION DE BIENES

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

RUC N° 20175639391

Jr. Diego de Almagro N° 525, La Libertad

ADENDA N.° 01 AL CONTRATO N. ° 44-2021/MPT-SGA.

CONTRATACION DE BIENES "ADQUISICION DE EQUIPOS DE VIDEO VIGILANCIA, EN LA GERENCIA DE SEGURIDAD CIUDADANA DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DISTRITO DE TRUJILLO - PROVINCIA DE TRUJILLO - LA LIBERTAD" CON CODIGO UNICO DE INVERSIONES N° 2501568.

LICITACION PUBLICA N. ° 001-2021-MPT-1

Conste por el presente documento la Adenda N.° 01 al Contrato N. ° 44-2021/MPT-SGA que celebran de una parte **LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO**, con RUC N° 20175639391, con domicilio legal en Jr. Diego de Almagro N.° 525 del distrito y provincia de Trujillo, departamento de La Libertad, representada por el Gerente Municipal **PEREZ TAVERA DANIEL SEGUNDO**, identificado con DNI n.° 19238117, debidamente facultado con Decreto de Alcaldía n.° 001-2019-MPT de fecha 01 de febrero del 2019 modificado por el Decreto de Alcaldía n.° 032-2019-MPT de fecha 04 de octubre del 2019, a quien en adelante se le denominará **"LA ENTIDAD"** y de la otra parte **HARDTECH SOLUTIONS S.A.C.**, con RUC n. ° 20481066094, con domicilio legal en Jr. San Martin n.° 426, distrito y provincia de Trujillo, departamento de La Libertad, debidamente representada por su Gerente General **CARLOS TITO CASTILLO SEVILLA**, identificado con DNI n.° 18225733, con poder inscrito en el Asiento n.° A00001 de la Partida Electrónica n.° 11036415 del Registro de Personas Jurídicas de la Zona Registral n.° V — Sede Trujillo; a quien en adelante se le denominara EL CONTRATISTA. La adenda se suscribe en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES.

El 24 de mayo del 2021 LA ENTIDAD y EL CONTRATISTA suscriben el contrato n.° 44-2021/MPT-SGA derivado de la LICITACIÓN PÚBLICA N. ° 001-2021-MPT-1 el que tiene por objeto la CONTRATACION DE BIENES "ADQUISICION DE EQUIPOS DE VIDEO VIGILANCIA, EN LA GERENCIA DE SEGURIDAD CIUDADANA DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DISTRITO DE TRUJILLO - PROVINCIA DE TRUJILLO - LA LIBERTAD" CON CODIGO UNICO DE INVERSIONES N° 2501568.

El monto total del referido contrato asciende a S/ 1'767,000.00 (Un Millón setecientos sesenta y siete mil con 00/100 Soles), que incluye todos los impuestos de ley.

CANTIDAD	DESCRIPCION	UNIDAD DE MEDIDA	PRECIO UNITARIO S/ INC IGV	PRECIO TOTAL S/ INC IGV
61	CAMARA DE VIDEO VIGILANCIA PTZ INCLUYE INSTALACION, GRUA Y ACCESORIOS HIKVISION DS-2DF9C4415HS-DLW(T2)/GI0	UNIDAD	S/ 24,995.00	S/ 1,524,695.00
1	MONITOR LED 46" HIKVISION DS-D2046NH-E INCLUYE INSTALACION	UNIDAD	S/ 23,395.00	S/ 23,395.00
1	DECODIFICADOR DE VIDEO CON TARJETAS DE SALIDA DVI Y ENTRADA DVI HIKVISION DS-6916UDI INCLUYE INSTALACION	UNIDAD	S/ 22,300.00	S/ 22,300.00
3	CPU INCLUYE INSTALACION	UNIDAD	S/ 18,300.00	S/ 54,900.00
4	MONITOR 23.8" HP Z24nf G2 INCLUYE INSTALACION	UNIDAD	S/ 3,610.00	S/ 14,440.00
13	ACUMULADOR DE ENERGIA -EQUIPOS DE UPS 2KVA APC STM2200I INCL.INSTALACION	UNIDAD	S/ 3,780.00	S/ 49,140.00
15	ACUMULADOR DE ENERGIA -EQUIPOS DE UPS 1.5 KVA APC STM1500I INCL. INSTALACION	UNIDAD	S/ 3,510.00	S/ 52,650.00

ANEXO N.º 4

MUNICIPALIDAD PROVINCIAL DE TRUJILLO
RUC N° 20175639391
Jr. Diego de Almagro N° 525, La Libertad

14	TARJETA DE VIDEO EXPRESS X 8GB INCLUYE INSTALACION	UNIDAD	S/ 1,820.00	S/ 25,480.00
			TOTAL S/ INCL IGV	S/ 1'767,000.00

Con Acta de conformidad de bienes n.° 656-2021 y n.° 657-2021, el responsable de Almacén General otorga Conformidad a la recepción de los bienes.

Con Acta de conformidad de bienes de fecha 07 de junio del 2021, el área técnica y el ingeniero supervisor concluyen que los bienes entregados por HARDTECH SOLUTIONS SAC y revisados por la supervisión cumplen con las especificaciones técnicas de los términos de referencia.

Con informe de fecha 09 de junio del 2021, el que tiene por objetivo la verificación de la instalación del equipo de video vigilancia in situ, el ingeniero supervisor referente al suministro de tarjeta de video PCI EXPRESS X 4GB DRR3 precisa que las tarjetas de video no son compatibles con las computadoras del centro de monitoreo por lo que se recomienda coordinar el área usuaria una solución alternativa. Adicionalmente concluye:

- "La supervisión concluye que la empresa ejecutora ha cumplido con la entrega de los bienes según contrato.
- La supervisión concluye que la empresa ejecutora ha cumplido con el servicio de instalación de los bienes según contrato".

Con Acta de recepción de proyecto de fecha 18 de junio del 2021, el ingeniero supervisor, el área técnica y el área usuaria concluyen, entre otros aspectos, que las 14 tarjetas de video corresponden a los bienes solicitados en el proceso, sin embargo, al verificar su funcionamiento se advierte que las tarjetas de video no son compatibles con las computadoras de la entidad lo que impide su buen funcionamiento. Adicionalmente precisan que la incompatibilidad de las 14 tarjetas de video no es atribuible ni responsabilidad de la empresa ejecutora, sin embargo, se recomienda a la ejecutora plantear una alternativa de solución la misma que sería remitida a la entidad.

Con carta n.° 22-2021 de fecha 08 de julio del 2021, HARDTECH SOLUTIONS SAC presenta popuesta para las 14 tarjetas de video que resultan incompatibles con los equipos existentes en la central de monitoreo y propone reemplazar las 14 tarjetas de video por 14 CPU nuevos con las siguientes caracteristicas:

- Workstation marca DELL.
- Procesador Core I5 de 10ma generación.
- Disco duro 1 Tb de capacidad.
- Disco de estado sólido de 240 Gb de capacidad.
- Tarjeta de video de 2 Gb.
- Memoria RAM de 16 Gb de velocidad.

En el citado documento HARDTECH SOLUTIONS SAC precisa además lo siguiente: "Las computadoras ofertadas poseen vigencia tecnológica y garantía de 1 año ofrecida por el fabricante, además de un óptimo rendimiento y mejores condiciones de operatividad con el sistema de videovigilancia de la MPT. El plazo para efectuar el referido cambio es de 10 días calendarios desde el día de siguiente de suscrita la adenda respectiva. El cambio se realizará ser sin perjuicio de la conformidad a la que tenemos derecho por haber cumplido con el proyecto en los plazos establecidos, tampoco se generará costo adicional a la entidad".

Con informe de fecha 09 de julio del 2021, el ingeniero supervisor efectúa la verificación de la propuesta efectuada por HARDTECH SOLUTIONS SAC concluyendo que las computadoras propuestas (Workstation) poseen vigencia tecnológica y pueden ser integradas al sistema de la central de monitoreo cumpliendo con las especificaciones técnicas mínimas requeridas para el trabajo

ANEXO N.º 5

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

RUC N° 20175639391
Jr. Diego de Almagro Nº 525, La Libertad.

CONTRATO N.° 44-2021-MPT-SGA.

CONTRATACIÓN DE BIENES "ADQUISICIÓN DE EQUIPOS DE VÍDEO VIGILANCIA, EN LA GERENCIA DE SEGURIDAD CIUDADANA DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DISTRITO DE TRUJILLO - PROVINCIA DE TRUJILLO - LA LIBERTAD" CON CÓDIGO ÚNICO DE INVERSIONES N° 2501568.

LICITACIÓN PÚBLICA N. ° 001-2021-MPT-1

Conste por el presente documento el contrato para la **CONTRATACIÓN DE BIENES "ADQUISICIÓN DE EQUIPOS DE VÍDEO VIGILANCIA, EN LA GERENCIA DE SEGURIDAD CIUDADANA DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DISTRITO DE TRUJILLO - PROVINCIA DE TRUJILLO - LA LIBERTAD" CON CÓDIGO ÚNICO DE INVERSIONES N° 2501568**, que celebran de una parte **LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO**, con RUC n. ° 20175639391, con domicilio legal en Jr. Diego de Almagro n.° 525 del distrito y provincia de Trujillo, departamento de La Libertad, representada por el Gerente Municipal **DANIEL SEGUNDO PEREZ TAVERA**, identificado con **DNI n.° 19238117**, debidamente facultado con Decreto de Alcaldía N° 001-2019-MPT de fecha 01 de febrero del 2019 modificado por el Decreto de Alcaldía N.° 032-2019-MPT de fecha 04 de octubre del 2019, a quien en adelante se le denominará **"LA ENTIDAD"**, y de la otra parte la Empresa **HARDTECH SOLUTIONS S.A.C.**, con RUC n. ° 20481066094, con domicilio legal en Jr. San Martín n.° 426, distrito y provincia de Trujillo, región La Libertad, debidamente representada por su Gerente General **CARLOS TITO CASTILLO SEVILLA**, identificado con DNI n.° 18225733, con poder inscrito en el Asiento n.° A00001 de la Partida Electrónica n.° 11036415 del Registro de Personas Jurídicas de la Zona Registral n.° V – Sede Trujillo; a quien en adelante se le denominará **EL CONTRATISTA**. El contrato se suscribe en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

El 29 de abril del 2021, a través del Sistema Electrónico de Contrataciones del Estado – SEACE, la ENTIDAD efectuó la publicación del otorgamiento de la buena pro de la **LICITACIÓN PÚBLICA N. ° 001-2021-MPT** para la **CONTRATACIÓN DE BIENES "ADQUISICIÓN DE EQUIPOS DE VÍDEO VIGILANCIA, EN LA GERENCIA DE SEGURIDAD CIUDADANA DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DISTRITO DE TRUJILLO - PROVINCIA DE TRUJILLO - LA LIBERTAD" CON CÓDIGO ÚNICO DE INVERSIONES N° 2501568**, a favor de la Empresa **HARDTECH SOLUTIONS S.A.C.**, cuyos detalles e importe constan en los documentos integrantes del presente contrato.

El 30 de abril del 2021, a través del Sistema Electrónico de Contrataciones del Estado – SEACE, LA ENTIDAD realizó el registro del consentimiento de la Buena Pro del procedimiento de selección referido en el párrafo precedente.

El 12 de Mayo del 2021, la Empresa **HARDTECH SOLUTIONS S.A.C.** remite documentación para suscripción del contrato.

El 14 de Mayo del 2021, con carta n.° 051-2021-MPT/GAF-SGA, LA ENTIDAD formula observaciones a la información remitida por **HARDTECH SOLUTIONS S.A.C** otorgando el plazo máximo de cuatro (04) días hábiles para la subsanación de las observaciones.

El 20 de mayo del 2020, la Empresa **HARDTECH SOLUTIONS S.A.C.** subsana observaciones.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la **CONTRATACIÓN DE BIENES "ADQUISICIÓN DE EQUIPOS DE VÍDEO VIGILANCIA, EN LA GERENCIA DE SEGURIDAD CIUDADANA DE LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, DISTRITO DE TRUJILLO - PROVINCIA DE TRUJILLO - LA LIBERTAD, CON CÓDIGO ÚNICO DE INVERSIONES N° 2501568.**

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a S/ 1'767,000.00 (Un Millón Setecientos Sesenta y siete Mil con 00/100 Soles), que incluye todos los impuestos de ley.

Recibo 1 mayo / 2021

ANEXO N.º 6

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

RUC N° 20175639391
Jr. Diego de Almagro N° 525, La Libertad.

CANTIDAD	DESCRIPCIÓN	UNIDAD DE MEDIDA	PRECIO UNITARIO S/ INC IGV	PRECIO TOTAL S/ INC IGV
61	CÁMARA DE VIDEO VIGILANCIA PTZ INCLUYE INSTALACIÓN, GRUA Y ACCESORIOS HIKVISION DS-2DF9C44I5HS-DLW(T2)/GIO	UNIDAD	S/24,995.00	S/ 1,524,695.00
1	MONITOR LED 46" HIKVISION DS-D2046NH-E INCLUYE INSTALAICON	UNIDAD	S/23,395.00	S/23,395.00
1	DECODIFICADOR DE VIDEO CON TARJETAS DE SALIDA DVI Y ENTRADA DVI HIKVISION DS-6916UDI INCLUYE INSTALACION	UNIDAD	S/22,300.00	S/22,300.00
3	CPU INCLUYE INSTALACION	UNIDAD	S/18,300.00	S/54,900.00
4	MONITOR 23.8" HP Z24nf G2 INCLUYE INSTALACIÓN	UNIDAD	S/3,610.00	S/14,440.00
13	ACUMULADOR DE ENERGÍA -EQUIPOS DE UPS 2KVA APC STM2200I INCL. INSTALACIÓN	UNIDAD	S/3,780.00	S/49,140.00
15	ACUMULADOR DE ENERGÍA -EQUIPOS DE UPS 1.5 KVA APC STM1500I INCL. INSTALACIÓN	UNIDAD	S/3,510.00	S/52,650.00
14	TARJETA DE VIDEO EXPRESS X 8GB INCLUYE INSTALACIÓN	UNIDAD	S/1,820.00	S/25,480.00
			TOTAL S/ INCL IGV	S/ 1´767,000.00

Este monto comprende el costo de los bienes, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente; así como cualquier otro concepto que pueda tener incidencia sobre la ejecución de la prestación materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en soles, en PAGOS PERIÓDICOS, previa conformidad por parte del área usuaria, luego de haber recepcionado el informe favorable del SUPERVISOR asignado por la Municipalidad, el cual se remitirá a la Sub Gerencia de Abastecimiento de la Municipalidad Provincial de Trujillo, para los trámites y acciones correspondientes y será de la siguiente manera:

- 1er Pago 80%, a la entrega de los bienes.
- 2do Pago 20%, luego de la firma de Acta de Instalación, configuración, capacitación y puesta en marcha de la Adquisición de Equipamiento de Video vigilancia, en la Gerencia de Seguridad Ciudadana y Defensa Civil de la Municipalidad Provincial de Trujillo.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Recepción de Almacén General.
- Informe del SUPERVISOR designado por la entidad con el aval de la Gerencia de Sistemas y conformidad de la prestación efectuada por la Gerencia de Obras Públicas.
- Comprobante de pago.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá el de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emitirá en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

ANEXO N.º 7

LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendarios siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

En caso de retraso en el pago por parte de LA ENTIDAD, salvo caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado en concordancia con el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

LA ENTIDAD se obliga a pagar la contraprestación al CONTRATISTA en soles el monto total del precio convenido. El depósito correspondiente deberá efectuarse en la cuenta proporcionada con Código de Cuenta Interbancario (CCI) n.° **011-250-000100036614-84** del BANCO CONTINENTAL BBVA, a nombre de **HARDTECH SOLUTIONS S.A.C.**

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de veinticinco (25) días calendarios, contabilizados a partir del día siguiente de la firma de contrato, los que comprenden:

Entrega del equipamiento tecnológico:	**Hasta 10 días calendarios.**
Instalación y configuración de equipamiento tecnológico:	**Hasta 15 días calendarios.**
Plazo de entrega total:	**25 días calendarios.**

La entrega de los bienes se efectuará en el Almacén General de la Municipalidad Provincial de Trujillo, ubicado en la Av. España n.° 742, distrito y provincia de Trujillo, en el horario de 7:30 a 15:00 horas y la instalación de cámaras de video vigilancia, se realizará, según el punto de ubicación detallado en el Anexo 1 (ubicaciones de cámaras de video vigilancia) de las Bases Integradas y los demás equipos tecnológicos, serán instalados y configurados en la central de Tráfico, Riesgo y Monitoreo.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA SÉTIMA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

- De Fiel Cumplimiento del Contrato: **S/176,700.00 (CIENTO SETENTA Y SEIS MIL SETECIENTOS CON 00/100 SOLES)**, a través de la Carta Fianza N°0011-0280-9800095116-54 emitida por **BBVA**, monto que es equivalente al diez por ciento (10%) del monto total del contrato, que regirá desde el 04 de mayo de 2021 hasta el 10 de Julio de 2021, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto en el literal a) del numeral 1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA NOVENA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción es responsabilidad del área de almacén y la conformidad de las Especificaciones

ANEXO N.º 8: MANTENIMIENTO PREVENTIVO

MUNICIPALIDAD PROVINCIAL DE TRUJILLO
SUB GERENCIA DE SEGURIDAD CIUDADANA
17 MAYO 2019
Reg.: 1160 Folios: 4
Hora:

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

CARGO

INFORME Nro. 487-2019-MPT/GSCyDC/SGSC/CTRM

SEÑOR : CAP ® PNP EDUARDO MOLERO OYOLA
SUB GERENTE DE SEGURIDAD CIUDADANA-MPT

ASUNTO : Solicita mantenimiento preventivo, correctivo y de limpieza de los Equipos de Computo de la Central de Monitoreo, por motivo que se indica.

REF. : Informe Nro. 019-2019-CMT-GSCDC del 17MAY2019

Me dirijo a Ud. con la finalidad de informar lo siguiente:

1. El día de la fecha se recepcionó por parte del responsable de Soporte Técnico de la Central de Tráfico, Riesgo y Monitoreo **Ing. LUIS ALBERTO ZAMORA HERNANDEZ,** el documento de la referencia, haciendo de conocimiento que se viene reportando problemas por fallas en los ordenadores (CPU) de la central de monitoreo; toda vez que trabajan ininterrumpidamente las 24 horas los 365 dias del año (inoperativos CPU HP 74089950-0952 y CPU DELL 74089950-1174), solicitando el mantenimiento preventivo, correctivo y de limpieza de los equipos de computo de la Central de Monitoreo y Central de Radio Comunicaciones que se indican:

EQUIPOS DE COMPUTO CENTRAL MONITOREO (ORION 1)

N°	ARTICULO	COD. PATRIMONIAL	UBICACIÓN
01	CPU HP, SERIE 2UA5451PLH	74089200 - 0011	ESTACION N° 18
02	CPU HP, SERIE 2UA5451PLS	74089200 - 0010	ESTACION N° 08
03	CPU HP, SERIE MXL50711KP	74089950 - 0956	ESTACION N° 03
04	**CPU HP, SERIE MXL50711MC**	**74089950 - 0952**	**INF. Nro.999 del 06DIC2018**
05	CPU LENOVO	74089950 - 0988	USO DEL RESPONSABLE CMT
06	CPU DELL OPTIPLEX 7010, SERIE 7RQ6LY1	74089950- 0874	DIGITACION CMT

EQUIPOS DE COMPUTO CENTRAL MONITOREO (ORION 2)

N°	ARTICULO	COD. PATRIMONIAL	UBICACIÓN
01	CPU DELL OPTIPLEX 3046 MT, SERIE 6S584J2	74089950 - 1176	ESTACION 01
02	CPU DELL OPTIPLEX 3046 MT, SERIE 6S1H4J2	74089950 - 1175	ESTACION 02

ANEXO N.º 9

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

RUC N° 20175639391
Jr. Diego de Almagro N° 525, La Libertad.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 21 del artículo 45 de la Ley de Contrataciones del Estado.

CLÁUSULA DÈCIMO OCTAVA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA DÉCIMO NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: Jr. Diego de Almagro n.° 525 del distrito y provincia de Trujillo, departamento de La Libertad

DOMICILIO DEL CONTRATISTA: Jr. San Martín n.° 426, distrito y provincia de Trujillo, región La Libertad.

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por triplicado en señal de conformidad en la ciudad de Trujillo el 24 de mayo del 2021.

"LA ENTIDAD"

"EL CONTRATISTA"

ANEXO N.º 10

MUNICIPALIDAD PROVINCIAL
DE TRUJILLO

CARGO

INFORME Nro. 116 -2022-MPT/GSC/SGSCyCCI/CTRM

SEÑOR : CMDTE PNP ® WILLIAM RODRIGUEZ VILCHEZ
SUB GERENTE DE SEGURIDAD CIUDADANA-MPT

ASUNTO : Solicita mantenimiento técnico de CPU por motivo que se indica.

REF. : Informe Nro. 008-2022-CTRM/ST/JCRU

Es grato dirigirme a Ud. con la finalidad de informar lo siguiente:

1. El día de la fecha el Sr. JUAN CARLOS ROSARIO ULCO (OC-24) operador responsable soporte técnico de la Central de Tráfico, Riesgo y Monitoreo da cuenta mediante el documento de la referencia sobre las fallas técnicas que presenta el CPU marca Dell modelo Optiplex 7010 con código patrimonial 74089950-0874.

2. Hace conocer que desde el 20MAY20202 viene constantemente presentando fallas (el equipo se reinicia y apaga), dificultando el trabajo diario en la digitación de incidencias.

3. Por lo antes expuesto se remite Un (01) CPU marca Dell modelo Optiplex 7010 con código patrimonial 74089950-0874 a fin de ser trasladado al Area de Soporte Técnico de la Gerencia de Sistemas para su revisión, diagnóstico y reparación.

Trujillo, 21 de mayo del 2022

[redacted]

MUNICIPALIDAD PROVINCIAL DE TRUJILLO
SUB GERENCIA DE SEGURIDAD CIUDADANA
23 MAYO 2022
Reg.: ..... Folios: .....
Hora: 09:15 Firma: .....

ANEXO N.º 11

Este tipo de penalidad puede alcanzar un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora, LA ENTIDAD puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMO TERCERA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMO CUARTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMO QUINTA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, no haber ofrecido, negociado o efectuado cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, EL CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a: i) Comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) Adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

CLÁUSULA DÈCIMO SEXTA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÈCIMO SÉTIMA: SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

ANEXO N.º 12

03	**CPU DELL OPTIPLEX 3046 MT, SERIE 6S094J2**	**74089950 - 1174**	**INF. Nro. 486 16MAY2019**
04	CPU DELL OPTIPLEX 3046 MT, SERIE 6S6B4J2	MPT/UOCP-0042-18	ESTACION 05
05	CPU DELL OPTIPLEX 3046 MT, SERIE 6S0J4J2	74089950 - 1178	ESTACION 06
06	CPU DELL OPTIPLEX 3046 MT, SERIE 6S3D4J2	74089950 - 1177	ESTACION 07
07	CPU DELL OPTIPLEX 3046 MT, SERIE 6S4B4J2	74089950 - 1179	ESTACION 09
08	CPU DELL OPTIPLEX 3046 MT, SERIE 6S2G4J2	74089950 - 1180	ESTACION 10
09	CPU DELL OPTIPLEX 3046 MT, SERIE HTNQRG2	74089950 - 1183	ESTACION 11
10	CPU DELL OPTIPLEX 3046 MT, SERIE HTNKHG2	74089950 - 1181	ESTACION 12
11	CPU DELL OPTIPLEX 3046 MT, SERIE HTNTLG2	74089950 - 1182	ESTACION 13
12	CPU DELL OPTIPLEX 3046 MT, SERIE HTP1KG2	74089950 - 1184	ESTACION 14
13	CPU DELL OPTIPLEX 3046 MT, SERIE 2R1TRG2	MPT/UOCP-0076-18	ESTACION 15
14	CPU DELL OPTIPLEX 3046 MT, SERIE HTNZJG2	74089950 - 1185	ESTACION 16

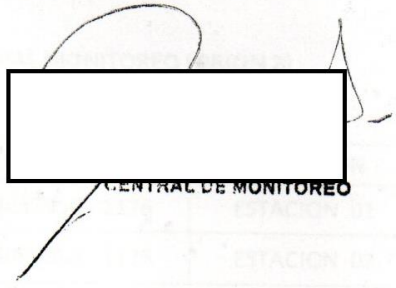
EQUIPO DE COMPUTO CENTRAL DE RADIO COMUNICACIONES (SATURNO)

CPU	COD. PATRIMONIAL	MARCA	MODELO	SERIE
CORE I3, Color negro	MPT/UCP - 0790	XTECH	C8500GD857	1206081207

2. Por lo antes expuesto y luego del diagnostico efectuado por el personal de soporte técnico se determino la necesidad de solicitar a través de la Gerencia de Sistemas MPT la programación de un Plan de Mantenimiento preventivo, correctivo y de limpieza de los equipos de computo antes indicados por el uso continuo, a fin de mantener la continuidad y operatividad de la Central de Monitoreo.

Lo que se cumple con informar a Ud. para los fines del caso

Trujillo, 17 de mayo del 2019



ANEXO N.º 14: CHECK List “Evaluación de la Gestión Redes y Servidores”

Evaluación de la Gestión Redes y Servidores

PREGUNTAS	Respuesta		
	SI	NO	N/A
1. ¿Es responsable de la administración de la plataforma informática?		X	
2. ¿Se cuenta con alojamiento propio?	X		
3. ¿Se cuenta con un diagrama de red?		X	
4. ¿Se cuenta con manuales y procedimientos para la gestión de los servicios?		X	
5. ¿Se cuenta con un inventario de los equipos de la infraestructura de red?		X	
a) ¿Se cuenta con un procedimiento aprobado? Indicar documento y fecha:			
b) ¿Se realiza periódicamente?			
c) ¿Se informa?			
6. ¿Se monitorea el sistema de comunicaciones?	X		
a) ¿Se cuenta con un procedimiento aprobado? Indicar documento y fecha:		X	
b) ¿Se registran las incidencias?	X		
c) ¿Se informa?	X		
7. ¿Se cuenta con políticas de acceso?	X		
a) ¿Se cuenta con un procedimiento aprobado? Indicar documento y fecha:		X	
b) ¿Se actualizó?		X	
8. ¿Se establecieron políticas que definan las claves de acceso?		X	
a) ¿Definidas por el área?	X		
b) ¿Fueron oficializadas? (Indicar Doc. y Fecha)		X	
c) ¿Se actualizaron?		X	
9. Las claves de acceso se asignan a los usuarios:		X	
a) ¿Directamente?			
b) ¿Sobre cerrado?			
c) ¿Correo electrónico?			
d) ¿Se comparten?	X	X	
10. ¿Se cuenta con software de gestión de accesos?	X		
a) ¿Se cuenta con un procedimiento aprobado? Indicar documento y fecha:		X	
b) ¿Se designó a un responsable? Indicar documento y fecha:	X		
c) ¿Se registran las ejecuciones?		X	
d) ¿Se registran las incidencias?		X	
e) ¿Se informa?			
11. ¿Se cuenta con cortafuegos? (hardware/software)		X	
a) ¿Se designó a un responsable de su operación y gestión? Indicar documento y fecha:			
b) ¿Se registran las configuraciones?			
c) ¿Se registran las actualizaciones?			
d) ¿Se registran las incidencias?			
e) ¿Se informa?			
12. Se implementaron los siguientes medios de control lógico:			
a) ¿Protectores de pantalla con contraseña?		X	
b) ¿Mantienen antivirus actualizados?		X	
c) ¿No se permite la instalación de software gratuitos?			
d) ¿No se cuenta con acceso a Internet?		X	
e) ¿No se permiten programas de mensajería instantánea?		X	
f) ¿Solo se usa correo interno?		X	
g) ¿Se cuenta con cortafuegos interno?		X	
h) ¿En cuanto a otras circunstancias que hacían peligrar el funcionamiento del sistema (Especificar):		X	

Municipalidad Provincial de Trujillo
Jefe(a) Área Gerencia de Seguridad Ciudadana

ANEXO N.º 14

PREGUNTAS	Respuesta		
	SI	NO	N/A
13. Se implementaron los siguientes medios de Control Físico en la Sala de Servidores:			
a) ¿Prohibición del acceso?	X		
b) ¿Registro de visitantes'		X	
c) ¿Mecanismos de Control Electrónico de Acceso?	X		
d) ¿Piso técnico (falso piso)?	X		
e) ¿Paredes de concreto?	X		
f) ¿Puertas de metálica o vidrio?	X		
g) ¿Ventanas protegidas?		X	
h) ¿Aire acondicionado?	X		
i) ¿Extintores?	X		
j) ¿Sensores de humo?	X		
k) ¿Sensores de movimiento?		X	
l) ¿Contingencias respecto a falta de fluido eléctrico?			
– Pozo a tierra independiente	X		
– Circuito eléctrico independiente	X		
– Llave cuchilla independiente	X		
– Llave cuchilla termosensible	X		
m) ¿Protectores de pared y/o piso para Gabinetes de Comunicación?	X		
n) ¿Canaletas y ductos de cableado?	X		
o) ¿Contingencias respecto a desperfecto?		X	
p) ¿Contingencias respectos a accidentes?		X	
q) ¿Evaluación de Especialistas Externos?	X		
14. Se implementaron los siguientes medios de control físico en las estaciones de trabajo:			
a) ¿Asignación documentada de Activos?		X	
b) ¿Asignación documentada de responsabilidades del uso incorrecto de activos?		X	
c) ¿Des habilitación de Unidades de Almacenamiento Removibles?	X		
d) ¿Des habilitación de Puertos (Serial/Paralelo/USB/Infrarrojo)?	X		
e) ¿Contingencias respecto a falta de fluido eléctrico?	X		
f) ¿Contingencias respecto a desperfecto en los equipos?		X	
g) ¿Contingencias respectos a accidentes?		X	
h) ¿Contingencias respecto a Incendios? (Sensores de Humo y Extintores)	X		
i) ¿Separación de los cables de energía de los de comunicaciones para evitar interferencias?	X		
j) ¿Protectores de caja toma datos?		X	
k) ¿Canaletas y Ductos de Cableado?	X		
l) ¿Política sobre fumar, beber y comer cerca de los equipos?		X	
m) ¿En cuanto a otras circunstancias que hacían peligrar el funcionamiento del Sistema (Especificar): Como circuito, se realizó un cambio a todos ellos.			

Observaciones y/o Comentarios Finales:

- No se cuenta con planes de Contingencia de comunicación
- No tienen manuales y procedimientos para la gestión de los servicios

Municipalidad Provincial de Trujillo
Sub Gerencia de Seguridad Ciudadana

Trujillo, 28 de octubre del 2022