UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Modelo de defensa informático para la Protección de los datos en la empresa CGS MAXIMA S.A.C., Lima 2022

TESIS PARA OBTENER EL
TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORES:

Manihuari Arimuya, Luis Carlos (orcid.org/0000-0002-2336-9332)

Vergaray Pintado, Willy Frank (orcid.org/0000-0001-9568-115X)

ASESOR:

Dr. Agreda Gamboa, Everson David (orcid.org/0000-0003-1252-9692)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

TRUJILLO - PERÚ

2022

Dedicatoria

A mis padres Jorge y Mariela, quienes me dieron la fuerza para continuar, que desde pequeño me inculcaron la disciplina de estudiar y luchar por los sueños.

A mi abuela por enseñarme su paciencia y amor incondicional y a mi abuelo que creyó siempre en mí y guía desde el cielo.

Luis Carlos

A mis padres Víctor y Gladys quienes, con su apoyo desde el Colegio, Instituto y Universidad me brindaron su incondicional amor para sostenerme en el camino académico.

A mi hermana Katy y mi hermosa sobrina Valery, quien desde su llegada; su sonrisa resuena por toda la casa como la mejor composición musical jamás escrita.

A mi Papá abuelo Hugo quien, desde mi nacimiento nunca dejó de felicitarme cada 21 de septiembre y a mi abuelito Rodolfo.

A los amigos que nos reuníamos en el parque Canchis y a mis tíos Román, Marleny sus hijos Mercedes y Jesús.

A mis cantantes y actores que con su talento me hicieron una mejor persona, Chester Bennington, Chris Cornell; con sus prodigiosas voces, entonación y timbre vocal. A los actores Chadwick Boseman, Tommy Oliver; con su habilidad en la actuación me hicieron sentir y vivir la cercanía de sus personajes.

Willy Frank

Agradecimiento

A la Universidad César Vallejo por la oportunidad de ser profesionales de alta competitividad académica.

A la empresa CGS MAXIMA S.A.C. por su apoyo a lo largo de estos meses, por facilitarnos toda la información necesaria para la culminación exitosa del trabajo.

Nuestro profundo agradecimiento a la universidad, a los docentes y en especial a nuestro tutor de tesis por su confianza, colaboración, profesionalismo, que con su experiencia académica supo direccionar este trabajo de tesis.

Los autores

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

Esta investigación tuvo como objetivo incrementar la protección de datos en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022 mediante la propuesta de un modelo de defensa informático; el tipo es investigación fue aplicada y de diseño preexperimental. Se utilizó una muestra poblacional de 10 personas, además de la aplicación de la norma internacional ISO/IEC 27002:2013 para el desarrollo la solución tecnológica propuesta. Como resultados se tuvo que, para el primer indicador "Nivel de confidencialidad de la data" hubo un incremento de 3.03 puntos (60.60%), para el segundo indicador "Nivel de integridad de la data" hubo un incremento de 2.96 puntos (59.20%) y para el tercer indicador "Nivel de disponibilidad de la data" hubo un incremento de 3.23 puntos (64.60%), lo cual permitió un resultado favorable al implementar la solución propuesta. Como conclusión general se tuvo que, la propuesta de un modelo de defensa informático incrementó de forma trascendental la protección de la data de la empresa en estudio.

Palabras clave: *Modelo de defensa informático, Protección de datos, Norma internacional ISO/IEC 27002:2013, Empresa de seguridad.*

Abstract

The objective of this research was to increase data protection in the company CGS MAXIMA S.A.C. in the city of Lima in the year 2022 through the proposal of a computer defense model; the type of research was applied and pre-experimental design. A population sample of 10 people was used, in addition to the application of the international standard ISO/IEC 27002:2013 for the development of the proposed technological solution. As results, for the first indicator "Data confidentiality level" there was an increase of 3.03 points (60.60%), for the second indicator "Data integrity level" there was an increase of 2.96 points (59.20%) and for the third indicator "Data availability level" there was an increase of 3.23 points (64.60%), which allowed a favorable result when implementing the proposed solution. As a general conclusion, it was concluded that the proposal of an IT defense model significantly increased the protection of the data of the company under study.

Keywords: *IT defense model, Data protection, International standard ISO/ IEC 27002:2013, Security company.*

I. INTRODUCCIÓN

Según ISO-TI (2021) afirma que, la **protección de los datos** puede variar según las especificidades de cada compañía y la sección económica al que dedica su accionar operacional, entonces se habla de fines comunes compartidos por diversas compañías en el aspecto de la seguridad y protección de datos. Se puede encontrar esta información sobre seguridad en la normativa mundial ISO 27001/27002. Este estándar provee una guía para la implementación de la información segura, cuyo fin primordial es cuidar los recursos de datos; vale decir. terminales, usuarios y datos procesados. Hay tres cosas principales a considerar al crear este sistema de seguridad de datos ISO: integridad, confidencialidad y disponibilidad.

De otra parte, LeyProteccionDatos (2019) sostiene que, los **modelos de defensa informáticos** deben garantizar la integridad; es decir. la presentación de los datos en la forma prevista, sin modificaciones o cambios no expresamente admitidos. El fin fundamental es asegurar la transferencia de la data en un ambiente de seguridad plena utilizando protocolos con seguridad incorporada (encriptación) y mecanismos para impedir peligros. La reserva de la data avala que únicamente los usuarios autorizados o las personas jurídicas tengan acceso a la información recopilada y que no se divulgue sin la debida autorización. Los sistemas seguros de la data deben asegurar que su reserva no se vea afectada. El aspecto de usabilidad garantiza que la data esté continuamente a disposición para aquellos usuarios o entidades con autorización para controlarlo y entenderlo. De esta forma, es importante disponer de mecanismos de apoyo y aseguramiento para el acceso a la data datos cuando sea imprescindible y, así impedir dificultades en la atención.

En este contexto, actualmente se tiene a la **empresa CGS MAXIMA S.A.C** de la ciudad de Lima, la cual es una empresa peruana localizada en Pueblo Libre, Lima. Inició sus actividades económicas el 03/11/2008. Esta empresa fue inscrita el 20/08/2008 como una Sociedad Anónima Cerrada. Es una empresa especializada en brindar soluciones globales de impresión, contando para ello con un equipo (CGS MAXIMA, 2018).

La empresa en estudio actualmente no cuenta con un modelo de defensa informático, encontrándose los datos desprotegidos, identificándose los siguientes **problemas específicos**: poco control en el acceso de usuarios; alto riesgo del manejo de los datos a cargo de trabajadores o de terceros; políticas de seguridad incompletas; datos disponibles a trabajadores que cambian a otras unidades organizacionales, lo cual provoca un riesgo de circulación de los datos; retraso en generar solicitudes de acceso a los datos al no estar a disposición y, además inexacto sin contar con directivas de protección de datos (CGS MAXIMA, 2018).

Para hacer frente a las deficiencias descritas en el párrafo anterior, fue ineludible plantear un **modelo de defensa informático**, lo cual fomenta un visionamiento adecuado de las indicaciones y pasos fundamentales para identificar y examinar peligros latentes e intimidaciones a la data con miras a adaptarlos a un modelo que levante las especificaciones requeridas.

Se consideró el **enunciado del problema**: *General:* ¿En qué condición un modelo de defensa informático impacta en la protección de los datos en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022?; *Específicos: Deficiencia concreta 1* - ¿En qué condición un modelo de defensa informático impacta en la confidencialidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022?; Deficiencia concreta 2 - ¿En qué condición un modelo de defensa informático impacta en la integridad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022?; Deficiencia concreta 3 - ¿En qué condición un modelo de defensa informático impacta en la disponibilidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022?

Se consideró la **justificación de la investigación**: *Conveniencia*, puesto que fortalece la reputación e imagen empresarial como una compañía segura; *Relevancia social*, puesto que beneficia a la comunidad con trabajadores más tranquilos y seguros en su trabajo diario; *Utilidad metodológica*, puesto que es el sustento para próximas investigaciones respecto a modelos de seguridad de la data; *Implicancias prácticas*, puesto que mejora el cuidado de la data; *Valor teórico*, puesto que se comprendió

correctamente el modelo de protección informática y las teorías subyacentes de cuidado de la data.

Se consideró los **objetivos**: *General*: Incrementar la protección de datos de la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022 mediante la propuesta de un modelo de defensa informático; *Específicos*: Fin concreto 1 - Incrementar la confidencialidad de la data de la empresa; Fin concreto 2 - Incrementar la integridad de la data de la empresa; Fin concreto 3 - Incrementar la disponibilidad de la data de la empresa.

Se consideró las **hipótesis:** *General:* "El modelo de defensa informático incrementa de manera significativa la protección de datos en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022"; *Específicas: Supuesto concreto 1* - "El modelo de defensa informático incrementa la confidencialidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022"; Supuesto concreto 2 - "El modelo de defensa informático incrementa la integridad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022"; Supuesto concreto 3 - "El modelo de defensa informático incrementa la disponibilidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022".

II. MARCO TEÓRICO

Se examinó un grupo de **antecedentes** que ayudaron a conocer las investigaciones que se realizaron previo al presente estudio:

Como **estudios previos internacionales**, se asumió:

Larco (2017) en su investigación asumió como intención crear un piloto de administración de información segura para cuidar y asegurar la data básica de las entidades. De esta forma, se inició un diagnóstico y estudio de vulnerabilidad de la data en dicha entidad, que mediante sus departamentos jurídicos brindaba servicios legales en el contexto territorial dirigido al pueblo ecuatoriano; en este sentido, el propósito del presente informe fue desarrollar un modelo de administración que permita cristalizar el plan estratégico de la institución, los atributos y productos relacionados con la información segura basado con la regulación completa de la administración organizacional basada en operaciones del directorio institucional y el sistema legal de forma centralizada y descentralizada.

Cáceres (2017) en su investigación asumió como intención administrar, monitorear, evidenciar y optimizar permanentemente la información segura. El mecanismo empleado en la investigación se basó en períodos de conformidad que permitían el consenso y la mediación de puntos de vista sobre la base de un amplio sentido de colaboración para fomentar el despliegue de directivas y pasos a seguir para la información segura. En esta investigación, se plantea que el método de despliegue del SGSI se base en la administración de peligros empleando las líneas guía y sugerencias de la normativa ISO 31000. Las actividades de dirección de la Subsecretaría se clasifican en orden de prioridad por posición de riesgo e impacto optimizando la designación de recursos a programas de información segura, promoviendo el amaestramiento y la formación de grupos colaborativos en base a fines principales, sin perder el enfoque de grupo y fin último. Se llevaron a cabo dos supervisiones, una al interior y otra al exterior, para examinar el despliegue del SGSI y los principios y pasos de la información segura. Las dos supervisiones fueron absolutamente individuales del grupo que propuso y desplegó el SGSI, así como las directivas y pasos de información segura. Las dos supervisiones concluyeron

que la situación vigente de la data segura se encuentra en un estatus intermedio. Este paso adelante es clave puesto que al inicio de la investigación existía ausencia de un SGSI o líneas guía y pasos reales para cuidar el aseguramiento de los datos.

Hernández (2015) en su investigación asumió como intención analizar la gestión de la información segura del banco con los recursos, estructuras organizacionales, marcos regulatorios y otros elementos vigentes durante el período de evaluación, teniendo en cuenta los habilitadores del proceso APO13 7 COBIT 5 y sus dimensiones comunes, es decir, objetivos, stakeholders, ciclo de vida y beneficio aplicado. prácticas En base a los logros conseguidos, se pudo determinar que, fue necesario definir y actualizar periódicamente el perfil de peligro de información segura, el cual se utiliza como herramienta básica para orientar estrategias e iniciativas sobre seguridad de la información y para estudiar las estructuras organizacionales necesarias, liderar la estrategia y actividades administrativas y de administración de información segura que actualmente no son lo suficientemente visibles en la creación de valor y, así promover el cuidado de los bienes de información del banco.

González (2015) en su investigación asumió como intención sostener la probidad, disposición y reserva de los recursos de datos de la organización que almacenan información, donde se llevó a cabo un diagnóstico de los mecanismos fundamentales incorporados en la normativa ISO/IEC 27002 para consumar con el rubro de la gestión de bienes.

Triguero (2015) en su investigación tuvo como intención proporcionar privacidad y seguridad de los datos almacenados en aplicaciones gratuitas de servicios en la nube. Para lograr este objetivo, primero identificamos los riesgos lógicos, las amenazas y las vulnerabilidades que pueden afectar el almacenamiento de datos en la nube. Se estudiaron diferentes mecanismos de seguridad que pudieran reducir o eliminar riesgos y asegurar los lugares más vulnerables, que sería la solución propuesta en este trabajo. Estas opciones fueron probadas para seleccionar mecanismos que podrían ser otras soluciones. Esta tesis presenta los resultados de los experimentos y su análisis. Con base en este análisis, se identificaron varios mecanismos que

deberían incluirse en el prototipo. En conclusión, se concluyó que los protocolos de encriptación Ipsec VPN, AES y RSA eran necesarios a fin de asegurar el cuidado de la data (supuesta seguridad de datos) y privacidad del usuario para minimizar los efectos negativos del uso de aplicaciones gratuitas.

Como **estudios previos nacionales**, se asumió:

Bustinza (2022) en su investigación asumió como intención determinar el afecto de la propuesta de información segura sostenido en la normatividad ISO/IEC 27001:2013 para la reducción de peligros de los bienes informáticos en una compañía particular de la ciudad arequipeña en el año 2021. El estudio realizado consideró a 32 empleados, cuyo supuesto de investigación fue crear una propuesta de información segura sostenido en esta normativa, que contuvo un impacto trascendental en la reducción de peligros de los bienes de información. Se pudo argumentar que la investigación consiguió evidencia que el despliegue de una propuesta de información segura sostenida en la normativa ISO/IEC 27001:2013 logró una afectación positiva en la reducción de peligros de los bienes de información de la compañía arequipeña.

Quispe (2021) en su investigación asumió como intención determinar un programa administrativo que cumpla con la normatividad ISO/IEC 27001:2013 con miras a fijar el impacto en la seguridad de la información de la entidad crediticia. A fin de lograr dicho triunfo, se empleó un método cuantitativo aplicado en un tipo de estudio de corte preexperimental. Asimismo, se trabajó con una muestra de 24 búsquedas por cada medición. Posteriormente, se logró una puntuación favorable de confidencialidad de datos de 75,52% a 87,36%, rendimiento de integridad de datos de 50,83% a 76,32% y un aumento significativo en la disponibilidad de datos de 96,81% a 99,93%. Al final, se destaca que un programa de administración que cumpla con la normatividad ISO/IEC 27001:2013 tendrá un impacto significativo en la información segura de una entidad crediticia.

Bonilla (2021) en su investigación asumió como intención estudiar los efectos del despliegue de las normativas ISO 27001 y 27002 acopladas a la información segura en una Secretaría Ejecutiva Policial Peruana. El estudio

realizado tuvo un diseño cuasiexperimental, puesto que la investigación se realizó con dos conjuntos, el primero en un pretest y el segundo es un postest.

Prado y Roman (2021) en su investigación asumió como intención estudiar la influencia de emplear un programa de red sostenido en la normativa administrativa de información segura con la ISO/IEC 27001 en una compañía. La investigación realizada fue de corte aplicativa y diseño preexperimental. La posición generó 30 comunicaciones repetidas durante el mes. A la encuesta se le aplicó un medio de recopilación de la data y empleando un formulario para el llenado de la misma. Los logros de esta prueba confirman la implementación del programa de red consiguiendo un logro verdadero en la gestión de información segura; asimismo, los índices de los reportes mostrados en el tiempo determinado, los reportes integrales logrados y los reportes confidenciales mostrados de manera imperceptible. Se concuerda que la “cantidad de recados privados entregados con cuidado” aumentó, con un promedio de 71,89% sin el programa y 96,89% con el programa, un incremento de 25% en la complacencia de los reportes privados. Se obtuvo que, la "cantidad de reportes conseguidos" sin el programa tenía una media del 69,11%, pero con el programa la media llegaba a 96,4%, evidenciando una subida del 27,33% en la complacencia del operador con los reportes cumplidos. Se obtuvo que, la “cantidad de reportes enviados en el tiempo señalado” incrementó con una media de 79,4% sin el programa y 96,00% con el programa, obteniendo así un progreso satisfactorio de únicamente 16,56% en los operadores.

Villarreal (2021) en su investigación asumió como intención identificar el impacto del programa de administración de información segura de una compañía constructora basado en la normativa ISO 270001:2013, debido a que contenía debilidades en diversos procesos de negocio y ponía en riesgo los bienes de información de la compañía. Fue un estudio aplicado, con diseño preexperimental. Además, se trabajó con una muestra de 20 exploraciones por cada medición para conseguir un logro positivo en las dimensiones de información segura, el 68.85% de vulnerabilidad de la confidencialidad de la data disminuyó a 15.40%, de integridad de la data

disminuyó en vulnerabilidad de 52.60% a 11.40% y, finalmente en disposición de la data se consiguió reducir la debilidad en las tres dimensiones de 47.15% a 11.95%, se consiguió incrementar la información segura a 90%.

Moran (2021) en su investigación asumió como intención estudiar los componentes claves de triunfo en el despliegue del programa de administración de información segura en una compañía de inversiones de Sechura utilizando el método descriptivo. A fin de conocer los componentes claves de éxito de la compañía, se realizó una entrevista a los directivos regionales y entregándose un checklist para el equipo de personas conformado por el inspector y la administración envuelta en la disposición. Respecto a los logros obtenidos se estableció que, en la compañía se identificaran 5 factores: responsabilidad de la dirección, sabiduría de la organización, grado de información segura, examinación del ejercicio, conciencia. Luego del estudio de los logros obtenidos se puede deducir que, cada componente debe producir tácticas a fin de obtener el despliegue del programa administrativo de información segura en tal compañía; adicionalmente, se deduce que, el componente más relevante es la conciencia, la cual tiene una afectación del 77.8%, esto porque se deben comparar otros componentes creando una cordial predisposición hacia el despliegue del SGSI en la compañía.

Zapata y Merino (2020) en su investigación asumió como intención plantear el establecimiento del programa administrativo de información segura de la provincia de Marcavelica mediante la NTP-ISO/IEC 27001:2014, usando diseños no experimentales y de tipo aplicativa, alineando el mecanismo PDCA a fin de disponer de un planteamiento de programa, teniendo en cuenta las amenazas, vulnerabilidades y consecuencias de peligro de los bienes de información, y por ende plantear y formular políticas y mediciones de control. En plena encuesta, los bienes de información de 113 municipalidades fueron reconocidos y examinados según su clasificación, de los cuales la mayor parte consistía en dispositivos de tratamiento de la data con un estado de peligro altísimo (57,50%), de los cuales la clase de riesgo más ocultos son fallas en los dispositivos, ruptura

de la conexión con relaciones y desgaste de los servicios de soporte. El estado de debilidades se estimó delicado (49%), donde la debilidad más relevante fue el cuidado físico inadecuado y la influencia adversa de los riesgos en 15% y 30% respectivamente. La investigación concluye que las brechas de información segura existentes se pueden establecer sobre el soporte de una investigación de tipo básica a fin de determinar directivas, mediciones de monitoreo orientadas al seguimiento y evaluación de la información segura del municipio.

Rodríguez y Romero (2019) en su investigación asumió como intención establecer el vínculo entre información segura y la administración de peligros en los laboratorios de informática de una Universidad Nacional en el año 2019. El estudio de línea base se hizo con una propuesta no-experimental y una orientación cualitativa correlativa. La muestra se compuso por 13 educandos de los laboratorios de informática de la Universidad. Se usó como mecanismo de extracción de la data: la Encuesta a fin de recolectar data respecto a las variables de investigación y dos cuestionarios (cada uno con 9 preguntas) como herramientas de extracción de la data. Estas dos herramientas se aprobaron por tres revisores especialistas en la temática a fin de asegurar su validez y confiabilidad. La conclusión fue que no existía un vínculo importante entre la información segura y la administración de peligros en los laboratorios de tecnologías de la información de la Universidad. Basado en la correlación de Pearson de 0.055, este logro fue mínimo con valor de significación p=0.859 (p > 0.05). De esta forma, se admite el supuesto negativo y se desecha el supuesto positivo.

Ruíz y Cahuana (2019) en su investigación asumió como intención la sistematización de la información segura según la normativa peruana ISO 27001 orientado a la información segura en una compañía de inversiones. El fin primordial fue verificar la influencia de la sistematización de la información segura propuesta según la normativa técnica nacional ISO 27001 en la compañía en estudio, puesto que, con el uso de esta normativa y sus mecanismos, es viable optimizar puntos débiles. y gestionar correctamente cada peligro informático. El logro obtenido fue que, mediante la sistematización de la data segura sobre la base de la normativa técnica

nacional ISO 27001, en la compañía en mención, se pudo mejorar y sostener la información segura.

Jaén (2019) en su investigación asumió como intención desplegar la normativa técnica nacional ISO/IEC 27001:2014 para promover la información segura en el almacén de datos de la subgestión de la data de RENIEC. Los programas informáticos que soportan las operaciones clave de RENIEC producen altas cantidades de datos que se elevan frecuentemente como resultado de las tareas cotidianas. Anticipar, manejar y tratar los datos crecientes es un alto desafío, en la administración de la data se limita algo más que la propia seguridad, porque se necesita cuidar la ubicación primordial que sostiene la data de más de 38 millones de ciudadanos (adultos y menores), por lo que los controles de acuerdo a la normativa NTP ISO/IEC 27001:2014 aplicado a la subgestión administrativa de la data para administrar la reserva, probidad y disposición mediante la implementación de mejores prácticas basadas en el direccionamiento estratégico de la entidad. Esta investigación tiene una orientación cuantitativa, tipo experimental aplicada, propuesta de pretest y estudio de preprueba y posprueba. Esta investigación busca demostrar cómo el despliegue de la normativa NTP ISO/IEC 27001:2014 contribuyó a la administración de la reserva, probidad y disposición de la data de RENIEC. El trabajo con los jueces especialistas de las unidades orgánicas y la subgerencia de gestión de la base de datos generaron como logro final la creación de legajos regulados con la elección, mediciones y conjeturas de normativas sistemáticas de monitoreo fundamentales para asegurar la información segura del certificado ISO/IEC 27001:2013.

Chinga (2018) en su investigación asumió como intención ofrecer un programa de administración de data segura soportado en lineamientos elegidos sobre la normativa técnica actual de la Secretaría Regional del Trabajo y Promoción del Empleo del Perú. El estudio de los bienes físicos, lógicos e informacionales de la unidad determinó que, mediante cuestionarios y formularios de exploración, existían 30 debilidades y 20 peligros, donde los peligros mencionados fueron examinados utilizando el método de Magerit, dando como resultado un 50% riesgo muy elevado, 40%

elevado, 5% medio y 5% bajo. Adicionalmente, se eligieron 75 mecanismos apropiados para estos peligros con soporte en la Declaración de Idoneidad ISO/IEC 27001:2014 de la NTP. Se recomendaron mecanismos y directivas de seguridad en función de los mecanismos elegidos. Se recomienda que una entidad asegure el uso razonable de sus bienes, estableciendo controles para abordar correctamente los sucesos adversos mediante un programa de gestión de peligros, identificando funciones y líderes a fin de que las violaciones de seguridad puedan abordarse rápidamente y procedimientos y reglas para proteger la seguridad. propiedad no se ha adaptado ningún formato definido para el legajo del SGSI según forma establecida por la ONGEI.

Ventura (2018) en su investigación asumió como intención investigar la influencia de implementar un programa de administración de información segura en línea de acuerdo a la normativa ISO/IEC 27001 en una compañía de mercancías informáticas. La investigación llevada a cabo fue de tipo aplicativa y el programa muestra fue a nivel preprueba. La población consistió en 30 copias de seguridad diarias que contenían datos diarios de las copias de seguridad realizadas en muchos servidores durante el mes. Se empleó la observación como mecanismo de extracción de la data y como apoyo se empleó un formato de registro. Los logros de este estudio corroboran que el despliegue del programa en línea obtuvo un impacto favorable en la administración de la información segura.

Mateo (2018) en su investigación asumió como intención desarrollar una propuesta de seguridad lógica que controla el acceso a Internet y permite la gestión de los roles de acceso de los usuarios finales de SUEZ Group. En otras palabras, es un servidor proxy desarrollado en Linux Centos e implementado en una LAN que administra los derechos de acceso para navegar por Internet, mejorando la efectividad de la cobertura de transmisión de la red mediante un mejor uso del sistema CONCAR (sistema de contabilidad) y STARSOFT. sistema de nómina) aplicaciones internas utilizadas por los socios. El actual modelo de seguridad propuesto en la tesis es utilizado en Pymes y grandes empresas peruanas debido a su mayor uso y bajos costos.

Medrano (2017) en su investigación asumió como intención estudiar cómo el despliegue de un programa administrativo de información segura incide en el procedimiento de administración de peligros de una entidad de salud nacional. El estudio fue de corte aplicativo, el diseño fue preexperimental, debido a que de la población y de la muestra se tomaron los activos de la data crítica vinculados con todo el procedimiento administrativo de riesgos de la institución de salud. La extracción de la data se llevó a cabo a través de una ficha de registro observacional. Respecto al análisis de la data, se utilizó al estadístico Shapiro-Wilk a fin de establecer la data normalizada, el estudio y la separación de los logros en cada una de las etapas anterior y posterior a la prueba realizándose a través de la Estadística. Se usó el ensayo estadístico de Wilcoxon en las mediciones de grado de peligro y cantidad de mecanismos direccionados a confirmar las hipótesis. En definitiva, se afirma que el despliegue de un programa de administración de información segura promovió la administración de peligros en la entidad de salud nacional.

Aliano (2017) en su investigación asumió como intención establecer el efecto del despliegue de la norma de información segura NTP ISO/IEC 27001 en la unidad de montaje y recursos de una sede del Ministerio de Educación. La investigación hecha fue de corte aplicativa y el programa prueba fue de tipo pre. La población lo conformó 4.783 exploraciones de la data de recursos tecnológicos con un tamaño muestral de 136, dicha muestra fue de subtipo probabilística, así como aleatoria sencilla. Se utilizó la observación como método de recolección de la data. El instrumento de recopilación de la data fue aprobado como consecuencia de la examinación de método de arreglo revisado por pares y en cuanto a la confiabilidad se realizó mediante el test de Wilcoxon, cuyos resultados muestran que las muestras Sig. es inferior a 0,05 (valor de significación alfa). Los logros obtenidos en el estudio corroboran que, el despliegue de la normativa técnica ISO/IEC 27001 en el país generó una consecuencia positiva en la información segura. Se registraron 182 casos antes de la cantidad de data reservada publicada, 50 casos luego del despliegue, 322 casos sobre la cantidad o porcentaje de ingreso y/o alteración no autorizada sobre la data

de producción anterior y posterior al despliegue disminuyó a 47 casos, 70,36% de los casos. se registró el porcentaje mediante el cual, el programa estaba habilitado para el operador, luego de la implementación se incrementó a 98.22%.

Castillo (2017) en su investigación asumió como intención realizar un diagnóstico del almacén de datos, temática de investigación debido a que el campo QHSE se encarga de la estandarización e implementación de procedimientos según la norma ISO 9001, la cual produce una gran cantidad de información susceptible de degradación, pérdida, cambio o caída en manos de competidores, porque según la norma ISO 27001, el conocimiento es todo activo fijo de una empresa. Hubo reuniones continuas con los socios de logística, TI y QHSE para ubicar y evaluar los recursos de data de las operaciones implementadas según la normativa ISO 27001, se emplearon cuestionarios y Checklist según la normativa ISO 27001 en cada dimensión. En base a los resultados obtenidos, el 58% de las fugas de documentos especiales son instrucciones, procedimientos, documentos técnicos, menos del 33% de las otras fugas de documentos son causadas por eventos relacionados con datos personales. En definitiva, se puede afirmar que posterior al mencionado informe, se planteó la elaboración de una propuesta técnica que contuviera un control seguro cimentado en la normativa ISO 27001 de acuerdo a los procesos realizados con la norma ISO 9001.

Ramos (2017) en su investigación asumió como intención La implantación de la normativa ISO 27001 en la gerencia de la información segura de una compañía, usando el método del Círculo de Edward Deming o denominado modelo PDCA, el cual es un modo de mejora permanente de la calidad adaptada a la normativa ISO 27001:2014, porque la data es importante como recurso para la continuidad empresarial. en diversas maneras, como software, hardware u otros mecanismos de transferencia en la compañía, toda vez que existían intimidaciones que amenazaban su continuidad; en referencia a la seguridad de la data, se definió como protegerlos de las continuas agresiones que pudiera padecer. La investigación desarrollada tenía como fin fomentar una correcta administración de peligros que permitieran a los programas impedir o

disminuir los errores de la red y las probables agresiones o catástrofes generales. En cuanto a los logros generados, luego del despliegue de la normativa ISO 27001 fueron insuperables en cláusulas de reserva, integridad y usabilidad, puesto que sus mediciones, así como el valor de la data publicada sin consentimiento, incluían data que podía ser divulgada. Las tasas de falsificación y datos frecuentemente inaccesibles se alcanzaron en 90,53%, 95,12% y 80,55% respectivamente, esto muestra un mejor monitoreo y una mejor seguridad. Finalmente, el despliegue de la normativa ISO 27001 minimizó de manera impactante los peligros de la data consiguiendo un valor de libertad y aseguramiento en bienes informáticos.

Estrada (2016) en su investigación asumió como intención detectar la influencia del despliegue de la normativa ISO 27001 en el aseguramiento de los archivos académicos de una entidad educativa. La investigación llevada a cabo fue de tipo aplicativa y el programa prueba fue de tipo pre. El grupo total se conformó por 26 registros de mediciones de peligro y 26 mediciones de cambios permitidos, donde la muestra fue censal. La técnica de recolección de la data usada fue la Observación, empleando como instrumento a la tarjeta de registro. Los logros generados del estudio reafirman que, el despliegue de la normativa ISO 27001 obtuvo un efecto positivo en la contabilidad académica de la entidad educativa según modificaciones permitidas, disminuyó a 80.8% desde la fase de preprueba hasta la fase de posprueba y relacionado a esto los riesgos disminuyeron en un 19%.

También, para un mejor entendimiento de la investigación presente, fue importante examinar un grupo de **bases teóricas** de la siguiente manera:

Seguridad, es un estadio donde los peligros y las circunstancias que causan daño físico, mental o material se manejan para cuidar de la ventura del individuo y también de la comunidad. Representa un origen necesario de la vida del día a día que derive en la persona y en la comunidad a llevar a cabo sus necesidades. Para lograr un grado ideal de seguridad, se necesita que las personas, las comunidades, los regímenes y más actores, independientemente del nivel de vida, creen y sostengan las condiciones citadas: un ambiente de coherencia y armonía mutua e igualdad que cuide

de los derechos y autonomías en el ámbito de la familia, de la localidad, de la nación y fuera de ella; acción preventiva y monitoreo de contusiones y otros perjuicios generados por incidentes; la sumisión a los principios y a la probidad física, material o psíquica de las personas y la existencia de medios efectivos de suspicacia, monitoreo y restitución que aseguren el cumplimiento de las tres primeras condiciones (INSPQ, 2018). De acuerdo con Foucault (2016 pág. 88), la seguridad es una concepción que surgió con la corriente liberal y está referida a una manera de gobierno que tiene como objetivo garantizar que los individuos o la comunidad corran el menor peligro posible, lo que lleva a la salud, delincuencia y comportamiento "antisocial", para combatir y proteger al país de amenazas externas que se identificaron principalmente en las actividades de otros países. Por un lado, estas temáticas, así como los derechos de las personas y el progreso social, tendían a ser prioridades de seguridad; la discusión debió establecer qué componente tiene antelación sobre los otros, en base a su relevancia a al temporal o extenso plazo y los recursos aprovechables del régimen. De ahí sus conceptos actuales: "seguridad" como resultado del empleo de la potencia y la armonía junto con el estado de derecho (Esther, y otros, 2011).

Modelo de defensa, es componente total de los compromisos organizacionales pues demuestra la obligación de la compañía con la ventura de sus colaboradores. Es la orientación que acoge una compañía para desplegar tácticas administrativas de seguridad y varía de acuerdo al sector y la clase de trabajo realizado. La administración de la información segura es un rol que ayuda a la eficiencia empresarial al prevenir peligros e intimidaciones operativas, de procedimiento o circunstanciales incluso antes de su ocurrencia. La administración de la seguridad es un procedimiento táctico que ubica y contempla los problemas de seguridad de los colaboradores. Es fundamental señalar que la gestión de la seguridad no implica únicamente una etapa preventiva, sino incluso la corrección de defectos y faltas de desempeño (Riquelme, 2022). Por otro lado, la gestión de la seguridad es vista como una actividad de poca importancia. Esto se debe a su aparente independencia de los procesos comerciales y de negocio, que crean un valor más tangible. Como resultado, en la práctica, los

departamentos de seguridad a veces se desarrollan como una unidad externa que carece de significado y conexión con otras áreas de la organización. Sin embargo, las empresas más capaces saben que las características de seguridad no son ajenas al negocio principal. Por lo tanto, los departamentos de seguridad necesariamente deben estar organizados con los fines y la cultura de la compañía (INERCO, 2020). Además, gestionar la seguridad de una compañía también representa algo extremadamente complicado, no solamente mirando desde la perspectiva técnica, incluso también desde la perspectiva organizativa; bastaría con imagina que en una gran institución educativa o una compañía con diversos departamentos: si alguien sale de la organización, quitarle el acceso a un determinado sistema no significa problemas técnicos, sino más bien a nivel organizativo. En la perspectiva técnica no hay obstáculo insuperable, pero desde la perspectiva de administración de la seguridad sí lo es (Red IRIS, 2020).

Modelo de defensa informático, representa al grupo de pasos, directivas, lineamientos, funciones y bienes establecidos y administrados por un régimen de cuidado de la data como grupo. Se puede definir a un Modelo de Seguridad Informático o MSI según INACAL (2020) como una orientación sistemática para crear, evaluar, desplegar, sostener, rastrear, promover y examinar la información segura institucional que le permita alcanzar sus objetivos comerciales. MSI se basa en el estudio y examinación de peligros y el hecho de que las entidades aceptan dichos riesgos en un porcentaje que está diseñado para administrarlos de manera efectiva y eficiente. Para implementar con éxito un MSI, es importante analizar los requisitos para una protección adecuada de los datos y, al mismo tiempo, implementar las medidas de control que estén mejor dirigidas a garantizar la protección de los datos relevantes. Las gracias de tener un MSI con la normativa ISO 27001 para Calder (2016) sostiene como trascendentales bases: fomentar el despliegue de su programa de administración, ahorrando turno y capital, brindando a los involucrados evidencias de que los peligros se abordan correctamente, reafirmando de que nada se encuentre al externo del legajo del MSI, optimizando el desempeño de la normativa ISO 27001, que facilita y

simplifica el trabajo de los empleados, reduciendo el margen de falta y desgaste de tiempo al generar sus modelos, evitando posibles cuellos de botella en el diseño, integrando rápidamente el legajo del MSI en sus operaciones comerciales.

Protección de datos, según Cano (2018) son mecanismos de cuidado de la data que conducen a la toma de decisiones en las operaciones organizacionales. Con respecto a estos mecanismos, se tiene tres elementos a considerar: la reserva, la probidad y la disposición, siendo una propuesta de negocio para cualquier compañía que quiera implementarlo. Según Solano (2020), esto es muy trascendental, dado que no debiera existir restricciones a los operadores fuera o dentro de la organización que anhelen emplear la data correctamente, más bien de una empresa previamente acreditada, un ataque cibernético podría afectar los servicios en cuanto a sus operaciones. De acuerdo con el mismo autor, lo más fundamental es que, las compañías acreditadas dispongan de acceso a la data; de esta forma, el incorrecto empleo de la data podría mostrar y generar inconvenientes de tipo legal por empleo no admitido. Es importante que existan formas de garantizar la admisión de operadores aceptados, y finalmente el autor mencionar que, con respecto a la probidad, ésta es la encargada de asegurar que la data no se altere de ninguna forma cuando el operador final está autorizado y, que debe ser auténtico para definir datos protegidos. Todos los estudios presentados incluyen un análisis en profundidad y apuntan a MSI, basados en la prelación de la reserva, disposición y probidad de la data, estas variables son los pilares de la organización de la información segura.

Asimismo, se dispone de un grupo de **enfoques conceptuales** que coadyuva al entendimiento complementario de la investigación como:

Activo informático, representa a los insumos técnicos del contexto computacional y de comunicaciones, siendo componentes de una compañía y que asumen la responsabilidad de la difusión de la data; corresponden a una parte trascendental de las compañías y promueven su permanencia o competencia; donde el cuidado es fundamental para que la data de diversos programas productivos o individuales se mantengan asegurados; protegerse

de probables perjuicios y modificaciones de la data. Una buena gestión de activos de TI permite tomar decisiones basadas en metadatos y registros electrónicos para determinar qué compras se deben realizar y cómo se utilizan los activos para implementar la gestión de activos de TI (ITGROUP, 2020).

Control de seguridad, presenta como objetivo afirmar que los bienes, programas, infraestructura física, data y ficheros vinculados con el empleo de la tecnología informática estén asegurados frente usos no permitidos, posibles perjuicios y usos inapropiados o ilícitos afín de que sean permanentemente asequibles, cuidados y resguardados (AUDIT-IT, 2022).

Dominio de seguridad, contiene los recursos de la data que deben cuidarse y hacer obedecer por completo. Los fines de los dominios según la norma internacional ISO 27002 son: Dominio “Directiva de seguridad”, cuya finalidad es asegurar el soporte y administración de la información segura necesaria para una unidad según con los requisitos por ley; Dominio "Estructuración sobre información segura", cuyo fin es crear una base referencial en el contexto de gestión para el despliegue y el seguimiento de la data segura en la compañía; Dominio "Administración de bienes" cuyo fin es cuidar correctamente los bienes de la compañía; Dominio “Seguridad de los recursos personales”, cuyo fin es implementar los mecanismos necesarios para controlar la información segura desde el enfoque de la gestión del personal de la organización; Dominio “Protección física y ambiental”, tiene por objeto proteger las residencias de las unidades y los datos sensibles procesados por ellas; Dominio "Administración de comunicaciones y operaciones", cuyo fin es definir los pasos y las obligaciones en el contexto operacional a fin de garantizar que el tratamiento de la data se lleven a cabo adecuadamente; Dominio “Monitoreo de acceso”, cuyo fin es cuidad del ingreso de los empleados permitidos a los sistemas automatizados; Dominio “Gestión de compras, despliegue y soporte de sistemas automatizados”, aplicado a compañías que desarrollan software al interno o pueden emplear a un tercero para su proceso; Dominio “Administración de sucesos de información segura” tiene como finalidad desplegar un ciclo de mejoramiento permanente en la administración de

sucesos de información segura; Dominio “Administración de la permanencia del negocio” tiene como finalidad afirmar la permanencia de la compañía utilizando controles que eviten o minimicen las interrupciones efectivas en las actividades de la organización; Dominio “Compliance”, cuyo objeto es afirmar el cumplimiento de los requerimientos normativos de seguridad en la propuesta, operacionalización, empleo y administración de los sistemas de automatizados (ISO-Estándares, 2018).

Se presentó tres (3) **normas de seguridad candidatas** para el despliegue de la solución tecnológica planteada como:

*Norma internacional ISO/IEC 27001, a*ctualmente es el estándar mundial mejor conocido para programas de administración de información segura. Asimismo, permite a las compañías a definir políticas y fines de administración de la información segura y a entender cómo administrar problemas importantes, implementar los mecanismos básicos y determinar fines visibles para fomentar la información segura. Esto hace posible que la compañía gestione su responsabilidad para consumar con los requerimientos normativos correspondientes, como el RGPD (con ISO 27701) y monitorear regularmente su aplicación. También ayuda con el mejoramiento continuo del programa para asegurar el cuidado y corregir las debilidades. Se adopta una orientación holística de la información segura. Los bienes protegidos tanto en formato digital como en físico, así como los bienes físicos (equipos de cómputo y conexiones) incluyendo data de colaboradores a título personal. Las temáticas que se discutirán se originan desde el desarrollo de las experticias del personal hasta el cuidado contra la estafa tecnológica (ISO 27001, 2013).

Norma internacional ISO/IEC 27002, este estándar define pautas y bases fundamentales para empezar, desplegar, sostener y optimizar la administración de la información segura de una compañía. Los fines establecidos en esta norma mundial proveen pautas generales para los fines de administración de información segura plenamente adoptados. Los fines de monitoreo y los mecanismos de esta norma mundial están planteados para obedecer el cumplimiento de los requerimientos reconocidos en el estudio de riesgos. Esta normativa mundial representa una guía práctica

orientado al desarrollo de normativas de seguridad en la compañía y recomendaciones efectivas de administración de data segura, y de este modo fomentar la generación de confianza respecto a las operaciones entre organizaciones (ISO 27002, 2013).

Norma nacional NTP-ISO/IEC 17799, es una normativa técnica peruana que además ayuda en el despliegue de mecanismos de aseguramiento de la data en las organizaciones peruanas, lo cual mejora el desempeño de la organización y aumenta su valor agregado respecto a otras compañías de rubro similar. La norma NTP-ISO/IEC 17799 plantea como finalidad dirigir y sostener la administración de la información segura de acuerdo con los requisitos legales de la compañía, legislación y normativa. La dirección es responsable de establecer claramente los lineamientos de la directiva de seguridad y expresar su respaldo y responsabilidad con la información segura, emitiendo y sosteniendo la directiva de la información segura (ISO 17799, 2005).

Con base a las normas de seguridad postulantes detalladas anteriormente, se inclinó por emplear el método de examinación de jueces especialistas para seleccionar la más adecuada en la propuesta tecnológica planteada siendo elegida *la normativa internacional ISO/IEC 27002:2013* - ver Anexo 3.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

- **Tipo de investigación**

  Aplicada porque se basó en el uso de métodos y técnicas ya comprobadas y aplicadas en la solución de investigaciones similares o afines (Ortega, 2020).

- **Diseño de investigación**

  Preexperimental porque se basó en la observación realizada a un único grupo de personas antes y después de la causa-efecto (Velásquez, 2020).

3.2. Variables y operacionalización

- **Variables**

  - **Variable independiente:** Modelo de defensa informático

    - **Definición Conceptual:**

      "Grupo de pasos, directivas, lineamientos, funciones y bienes establecidos y administrados por un régimen de cuidado de la data como grupo" (INACAL, 2020).

    - **Definición operacional:**

      La medición de esta variable se realizó a través de directivas y pasos de seguridad de la data en la compañía.

  - **Variable dependiente:** Protección de datos

    - **Definición Conceptual:**

      "Mecanismos de cuidado de la data que conducen a la toma de decisiones en las operaciones organizacionales como: la reserva, la probidad y la

disposición, siendo una propuesta de negocio para cualquier compañía a implementarlo" (Cano, 2018).

- **Definición operacional:**

La medición de esta variable se realizó por el nivel de confidencialidad (reserva), el nivel de integridad (probidad) y el nivel de disponibilidad (disposición) de la data en la compañía.

- **Operacionalización**

Con respecto a la operacionalización de las variables de estudio, esto se encuentra detallado en el Anexo 2 del presente documento de investigación.

3.3. Población, muestra y muestreo:

- **Población (N)**

La población en esta investigación estuvo integrada por el total de colaboradores (empleados) de la compañía como sigue:

Tabla 1. *Población*

Cargo / Puesto	Cantidad
Gerente	1
Jefe de área	3
Operario	6
Total	10

$$N = 10\ personas$$

- **Muestra (n)**

Como la Población en la investigación es inferior a 30, se deduce que la muestra resulta ser semejante. Así se tuvo:

$$n = N = 10\ personas$$

- **Muestreo**

  Respecto a la clase de muestreo seleccionada, ésta fue de corte *no probabilístico*, puesto que existió la intervención del investigador en su selección tomando como referencia la población definida anteriormente.

3.4. Técnicas e instrumentos de recolección de datos:

- **Técnicas:**
  - Encuesta.
  - Análisis documental.

- **Instrumentos:**
  - Cuestionario.
  - Ficha de datos.

- **Validez y confiabilidad:**

  En referencia a la Validez, los ítems que conforman los Cuestionarios de la investigación se examinaron y aprobaron gracias a la colaboración de tres jueces especialistas de reconocido prestigio, como se exhibe en el Anexo 5.

  En referencia a la *Confiabilidad*, se usó el coeficiente estadístico “Alfa de Cronbach” cuyo valor fue 0,813; lo cual significó que, la fiabilidad era alta, como se exhibe en el Anexo 6.

3.5. Procedimientos

La investigación en detalle realizó un conjunto de pasos meticulosos a fin de alcanzar el cumplimiento total de cada fin concreto planteado, toda vez que se hizo hincapié al uso de los instrumentos de extracción de la data empleados. Se tuvo:

- *Fin concreto 1: Incrementar la confidencialidad de la data*

  Se optó por extraer la data empresarial a fin de medir el nivel de reserva de la misma usando como instrumento al Cuestionario aplicado a los colaboradores seleccionados según la muestra poblacional seleccionada como se exhibe en el Anexo 4.

- *Fin concreto 2: Incrementar la integridad de la data*

  Se optó por extraer la data empresarial a fin de medir el nivel de probidad de la misma usando como instrumento al Cuestionario aplicado a los colaboradores seleccionados según la muestra poblacional seleccionada como se exhibe en el Anexo 4.

- *Fin concreto 3: Incrementar la disponibilidad de la data*

  Se optó por extraer la data empresarial a fin de medir el nivel de disposición de la misma usando como instrumento al Cuestionario aplicado a los colaboradores seleccionados según la muestra poblacional seleccionada como se exhibe en el Anexo 4.

3.6. Método de análisis de datos

Se optó por recurrir a los mecanismos que hacen referencia al estadístico descriptivo e inferencial a fin de haber logrado el tratamiento y estudio minucioso de la data extraída.

En referencia al uso del estadístico descriptivo, éste tuvo como fin realizar un estudio gráfico y de cálculo de la variable dependiente en los escenarios anterior y posterior a la aplicación de la variable independiente.

En referencia al uso del estadístico inferencial, éste tuvo como fin realizar un estudio de cálculo sobre la normalidad de los indicadores empleados en la medición de la variable dependiente.

Finalmente, se optó por realizar la comprobación de los supuestos planteados en el estudio a fin de exhibir correctamente los logros obtenidos con las distribuciones estadísticas empleadas.

3.7. Aspectos éticos:

En este documento se ha prioriza la ética de la investigación, puesto que se ha dispuesto del uso de documentación formal y oficial que exhibe el Vicerrectorado de Investigación y, pone a disposición “libremente” para el uso de los investigadores, tal es el caso de:

- Declaración de autoría (por los investigadores).
- Declaración de la originalidad del trabajo de investigación (por el asesor).
- Uso de la plataforma Turnitin para conseguir el índice de similitud.

Uso de la norma internacional ISO-690 para la gestión de referencias bibliográficas.

IV. RESULTADOS

Los resultados obtenidos para cada indicador fueron los siguientes:

- **Análisis descriptivo**
  - Indicador “Nivel de confidencialidad de la data”

Se exhibe el estudio descriptivo en la medición del indicador en el escenario preprueba y posprueba respectivamente:

Tabla 2. Análisis descriptivo del primer indicador

	N	Mínimo	Máximo	Media	Desv. Desviación
NCD-PrePrueba	4	1,42	1,87	1,700	,17603
NCD-PosPrueba	4	4,05	4,95	4,7253	,41767
N válido (por lista)	4				

En referencia a lo exhibido en la tabla anterior, se observa que el nivel de reserva de la data extraída precedente de la aplicación de la variable independiente presentaba un promedio de 1.70 puntos y ulterior a la aplicación de la misma presenta un promedio de 4.73 puntos; ello representó un incremento de 3.03 (60.60%). De este modo, se evidencia que ha existido un incremento en el nivel de reserva de la data con la propuesta del modelo de defensa informático, tal como se exhibe en la figura adjunta.

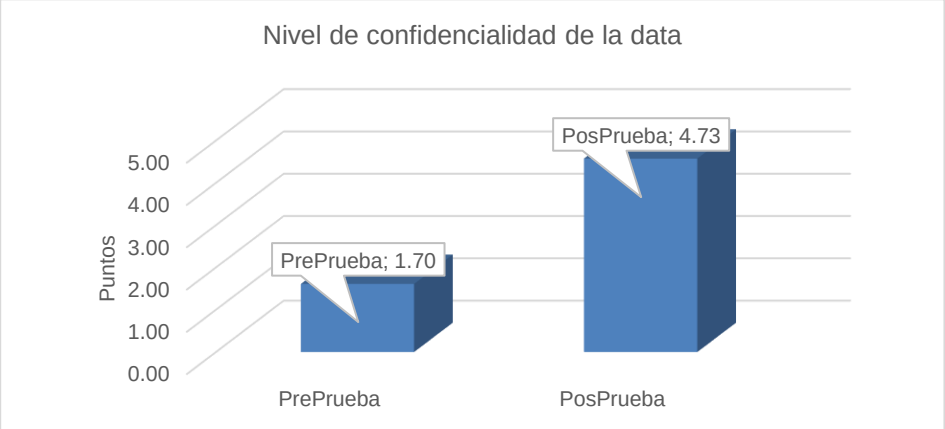

Figura 1. Promedios de pre prueba y pos prueba del primer indicador.

- Indicador “Nivel de integridad de la data”

Se exhibe el estudio descriptivo en la medición del indicador en el escenario preprueba y posprueba respectivamente:

Tabla 3. Análisis descriptivo del segundo indicador

	N	Mínimo	Máximo	Media	Desv. Desviación
NCD-PrePrueba	4	1,43	1,81	1,6487	,17327
NCD-PosPrueba	4	4,15	4,77	4,6234	,42412
N válido (por lista)	4				

En referencia a lo exhibido en la tabla anterior, se observa que el nivel de probidad de la data extraída precedente de la aplicación de la variable independiente presentaba un promedio de 1.81 puntos y ulterior a la aplicación de la misma presenta un promedio de 4.77 puntos; ello representó un incremento de 2.96 (59.20%). De este modo, se evidencia que ha existido un incremento en el nivel de probidad de la data con la propuesta del modelo de defensa informático, tal como se exhibe en la figura adjunta.

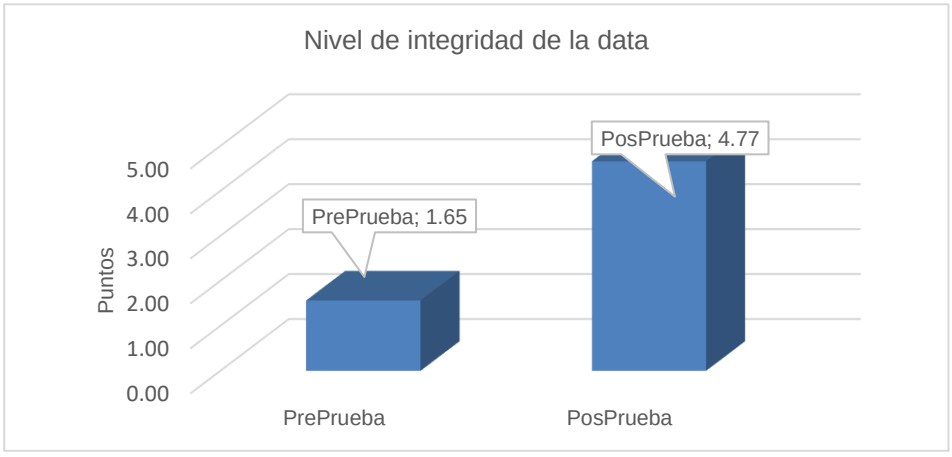

Figura 2. Promedios de pre prueba y pos prueba del segundo indicador.

- Indicador “Nivel de disponibilidad de la data”

Se exhibe el estudio descriptivo en la medición del indicador en el escenario preprueba y posprueba respectivamente:

Tabla 4. Análisis descriptivo del tercer indicador

	N	Mínimo	Máximo	Media	Desv. Desviación
NCD-PrePrueba	4	1,15	1,78	1,6210	,17650
NCD-PosPrueba	4	4,53	5,00	4,8540	,45279
N válido (por lista)	4				

En referencia a lo exhibido en la tabla anterior, se observa que el nivel de disposición de la data extraída precedente de la aplicación de la variable independiente presentaba un promedio de 1.62 puntos y ulterior a la aplicación de la misma presenta un promedio de 4.85 puntos; ello representó un incremento de 3.23 (64.60%). De este modo, se evidencia que ha existido un incremento en el nivel de probidad de la data con la propuesta del modelo de defensa informático, tal como se exhibe en la figura adjunta.

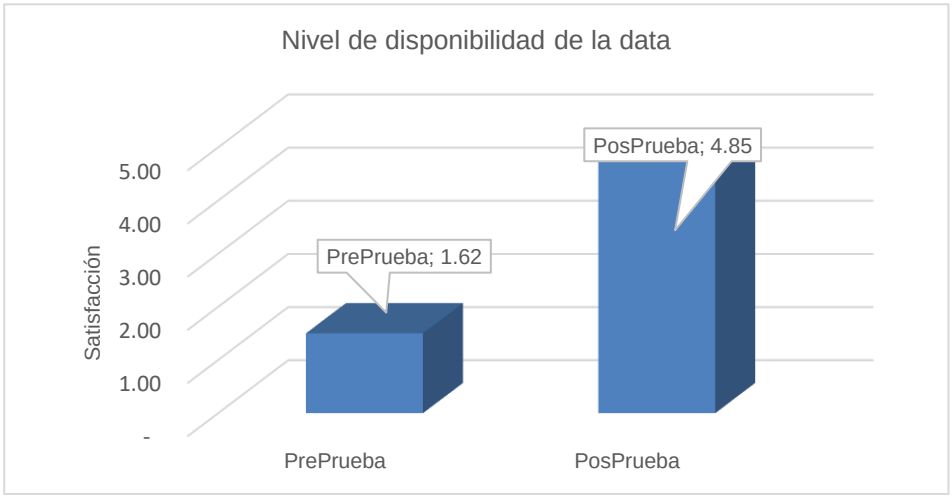

Figura 3. Promedios de pre prueba y pos prueba del tercer indicador.

- **Análisis inferencial**

El fin del análisis inferencial fue llevar a cabo test de normalidad en cada indicador usado, de tal forma que se aplicó para establecer la normalización distribuida muestral. Se tuvo:

- Indicador “Nivel de confidencialidad de la data”

Se examina los resultados conseguidos en el valor de significancia de la preprueba y posprueba de 0.05, formulándose los supuestos respectivos y determinando la normalidad correspondiente.

H_0: “Nivel de confidencialidad de la data (sin la propuesta del modelo de defensa informático) si tiene distribución normalizada.

H_1: “Nivel de confidencialidad de la data” (sin la propuesta del modelo de defensa informático) no tiene distribución normalizada.

H_0: “Nivel de confidencialidad de la data” (con la propuesta del modelo de defensa informático) no tiene distribución normalizada.

H_1: “Nivel de confidencialidad de la data” (con la propuesta del modelo de defensa informático) si tiene distribución normalizada.

Se aproxima el valor de significancia: $\alpha = 0.05$.

Valor de significancia > 0.05, se admite el supuesto negativo (H_0).

Valor de significancia <= 0.05, se admite el supuesto positivo (H_1).

Tabla 5. *Test de normalidad del primer indicador*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NCD-PrePrueba	,736	4	,023
NCD-PosPrueba	,839	4	,067

En referencia a lo exhibido en la tabla anterior, el valor de significancia en el escenario de preprueba fue de 0.023 (≤ 0.05), lo que implica admitir el primer supuesto positivo (indicador no presenta distribución normalizada); mientras que el valor de significancia en el escenario de posprueba fue de 0.067 (> 0.05), lo que implica admitir el segundo supuesto negativo (indicador no presenta distribución normalizada). En base a lo descrito anteriormente, se deduce que el primer indicador no presenta distribución normalizada y será afectado por el test de Wilcoxon.

En seguida, se exhibe los histogramas correspondientes:

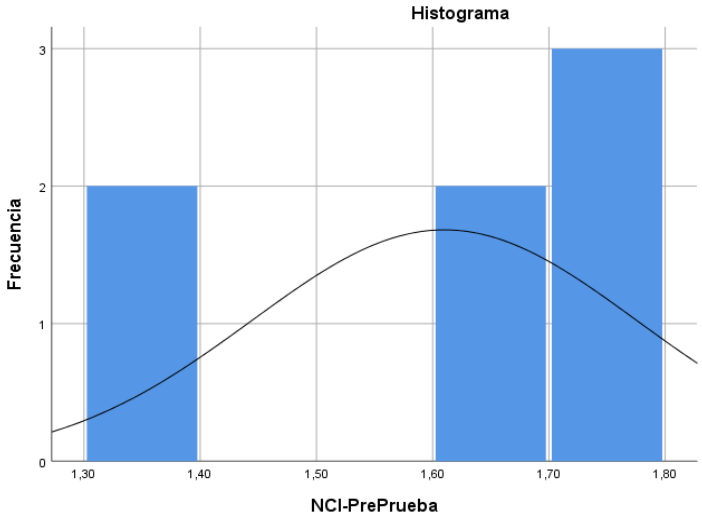

Figura 4. Histograma del primer indicador (PrePrueba)

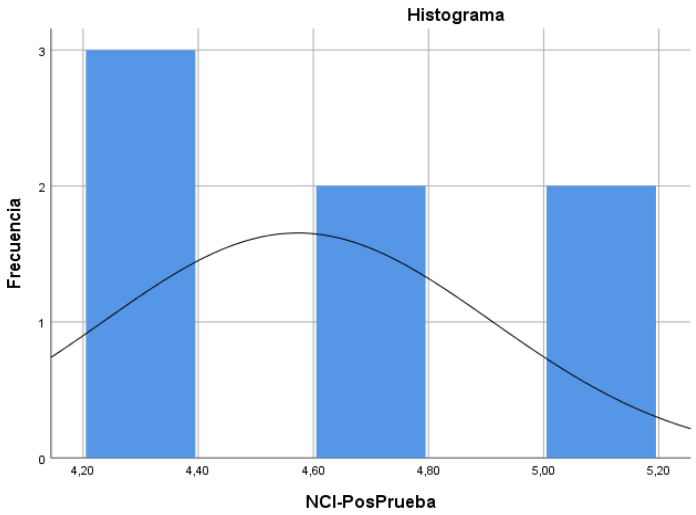

Figura 5. Histograma del segundo indicador (Pos Prueba)

- Indicador “Nivel de integridad de la data”

Se examina los resultados conseguidos en el valor de significancia de la preprueba y posprueba de 0.05, formulándose los supuestos respectivos y determinando la normalidad correspondiente.

H_0: “Nivel de integridad de la data (sin la propuesta del modelo de defensa informático) si tiene distribución normalizada.

H_1: “Nivel de integridad de la data” (sin la propuesta del modelo de defensa informático) no tiene distribución normalizada.

H_0: “Nivel de integridad de la data” (con la propuesta del modelo de defensa informático) no tiene distribución normalizada.

H_1: “Nivel de integridad de la data” (con la propuesta del modelo de defensa informático) si tiene distribución normalizada.

Se aproxima el valor de significancia: α = 0.05.

Valor de significancia > 0.05, se admite el supuesto negativo (H_0).

Valor de significancia <= 0.05, se admite el supuesto positivo (H_1).

Tabla 6. *Test de normalidad del segundo indicador*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NID-PrePrueba	,683	4	,032
NID-PosPrueba	,857	4	,054

En referencia a lo exhibido en la tabla anterior, el valor de significancia en el escenario de preprueba fue de 0.032 (≤ 0.05), lo que implica admitir el primer supuesto positivo (indicador no presenta distribución normalizada); mientras que el valor de significancia en el escenario de posprueba fue de 0.054 (> 0.05), lo que implica admitir el segundo supuesto negativo (indicador no

presenta distribución normalizada). En base a lo descrito anteriormente, se deduce que el segundo indicador no presenta distribución normalizada y será afectado por el test de Wilcoxon.

En seguida, se exhibe los histogramas correspondientes:

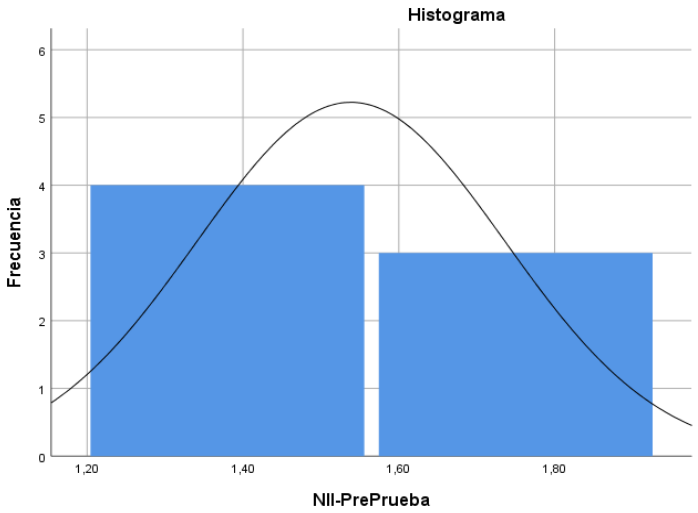

Figura 6. Histograma del nivel de integridad de la data (PrePrueba)

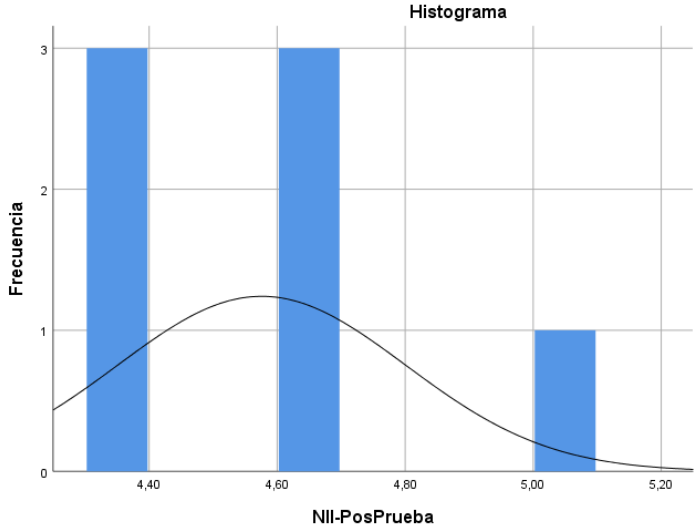

Figura 7. Histograma del nivel de integridad de la data (PosPrueba)

- Indicador “Nivel de disponibilidad de la data”

Se examina los resultados conseguidos en el valor de significancia de la preprueba y posprueba de 0.05, formulándose los supuestos respectivos y determinando la normalidad correspondiente.

H_0: “Nivel de disponibilidad de la data (sin la propuesta del modelo de defensa informático) si tiene distribución normalizada.

H_1: “Nivel de disponibilidad de la data” (sin la propuesta del modelo de defensa informático) no tiene distribución normalizada.

H_0: “Nivel de disponibilidad de la data” (con la propuesta del modelo de defensa informático) no tiene distribución normalizada.

H_1: “Nivel de disponibilidad de la data” (con la propuesta del modelo de defensa informático) si tiene distribución normalizada.

Se aproxima el valor de significancia: $\alpha = 0.05$.

Valor de significancia > 0.05, se admite el supuesto negativo (H_0).

Valor de significancia <= 0.05, se admite el supuesto positivo (H_1).

Tabla 7. *Test de normalidad del tercer indicador*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
NDD-PrePrueba	,876	4	,057
NDD-PosPrueba	,749	4	,072

En referencia a lo exhibido en la tabla anterior, el valor de significancia en el escenario de preprueba fue de 0.057 (> 0.05), lo que implica admitir el primer supuesto negativo (indicador presenta distribución normalizada); mientras que el valor de significancia en el escenario de posprueba fue de 0.072 (> 0.05), lo que implica admitir el segundo supuesto positivo (indicador

presenta distribución normalizada). En base a lo descrito anteriormente, se deduce que el tercer indicador presenta distribución normalizada y será afectado por el test de T-Student.

En seguida, se exhibe los histogramas correspondientes:

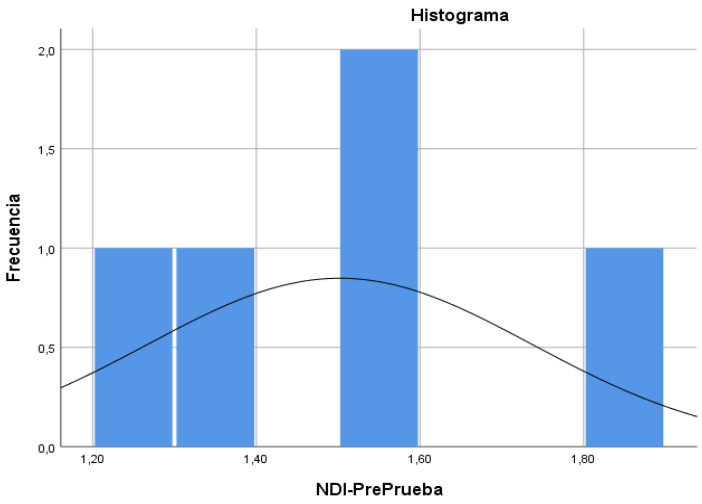

Figura 8. Histograma del tercer indicador (Pre Prueba)

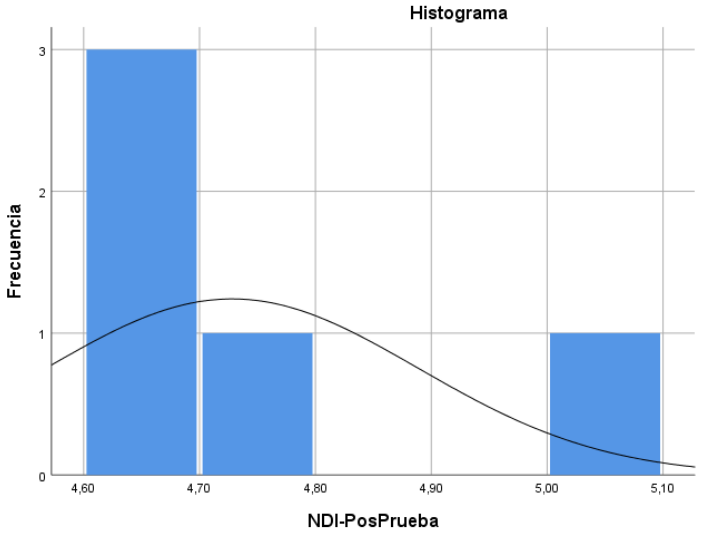

Figura 9. Histograma del tercer indicador (Pos Prueba)

- **Contrastación de hipótesis**

El test de normalización que se empleó en cada uno de los indicadores citados anteriormente determinó la aplicabilidad de las pruebas no paramétricas (Wilcoxon) y paramétricas (T-Student) según correspondía. Se tuvo:

- Supuesto concreto 1: “La propuesta del modelo de defensa informático incrementa el nivel de confidencialidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

En referencia al primer indicador, se eligió emplear la prueba no paramétrica de Wilcoxon debido a los resultados de normalización obtenidos en el paso anterior. De este modo, se establecen los supuestos estadísticos correspondientes (Negativa y Positiva) con un valor de significancia equivalente a 0.05.

Supuestos estadísticos:

H_0: “La propuesta del modelo de defensa informático no incrementa el nivel de confidencialidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

$$H_0: NCDa >= NCDp$$

En referencia al supuesto anterior, se observa la no existencia de incremento en el indicador.

H_1: “La propuesta del modelo de defensa informático si incrementa el nivel de confidencialidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

$$H_1: NCDa < NCDp$$

En referencia al supuesto anterior, se observa la no existencia de incremento en el indicador.

Valor de significancia: $\alpha = 0.05$.

Valor de significancia > 0.05, se admite el supuesto negativo (H_0).

Valor de significancia <= 0.05, se admite el supuesto positivo (H_1).

Tabla 8. *Prueba Wilcoxon para el primer indicador*

Estadísticos de prueba[a]

	NCD-PosPrueba - NCD-PrePrueba
Z	-2,379[b]
Sig. asintótica(bilateral)	,023

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En referencia a la tabla anterior, el valor de significancia conseguido fue 0.023 (< 0.05); en tal sentido, se desestimó el supuesto estadístico negativo admitiéndose el supuesto estadístico positivo. Se infiere que: “Hay bastante certeza estadística que la propuesta del modelo de defensa informático si incrementa de forma tarscedental el nivel de confidencialidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

- Supuesto concreto 2: “La propuesta del modelo de defensa informático incrementa el nivel de integridad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

En referencia al segundo indicador, se eligió emplear la prueba no paramétrica de Wilcoxon debido a los resultados de normalización obtenidos en el paso anterior. De este modo, se establecen los supuestos estadísticos correspondientes (Negativa y Positiva) con un valor de significancia equivalente a 0.05.

Supuestos estadísticos:

H_0: “La propuesta del modelo de defensa informático no incrementa el nivel de integridad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

H_0: NIDa >= NIDp

En referencia al supuesto anterior, se observa la no existencia de incremento en el indicador.

H_1: “La propuesta del modelo de defensa informático si incrementa el nivel de integridad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

H_1: NIDa < NIDp

En referencia al supuesto anterior, se observa la no existencia de incremento en el indicador.

Valor de significancia: α = 0.05.

Valor de significancia > 0.05, se admite el supuesto negativo (H_0).

Valor de significancia <= 0.05, se admite el supuesto positivo (H_1).

Tabla 9. *Prueba Wilcoxon para el segundo indicador*

Estadísticos de prueba[a]

	NCD-PosPrueba - NCD-PrePrueba
Z	-2,414[b]
Sig. asintótica(bilateral)	,032

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En referencia a la tabla anterior, el valor de significancia conseguido fue 0.032 (< 0.05); en tal sentido, se desestimó el supuesto estadístico negativo admitiéndose el supuesto estadístico positivo. Se infiere que: “Hay bastante certeza estadística que la propuesta del modelo de defensa informático si incrementa de forma trascendental el nivel de integridad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

- Supuesto concreto 3: “La propuesta del modelo de defensa informático incrementa el nivel de disponibilidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

En referencia al tercer indicador, se eligió emplear la prueba paramétrica de T-Student debido a los resultados de normalización obtenidos en el paso anterior. De este modo, se establecen los supuestos estadísticos correspondientes (Negativa y Positiva) con un valor de significancia equivalente a 0.05.

Supuestos estadísticos:

H_0: “La propuesta del modelo de defensa informático no incrementa el nivel de disponibilidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

H_0: NIDa >= NIDp

En referencia al supuesto anterior, se observa la no existencia de incremento en el indicador.

H_1: “La propuesta del modelo de defensa informático si incrementa el nivel de disponibilidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

H_1: NIDa < NIDp

En referencia al supuesto anterior, se observa la no existencia de incremento en el indicador.

Valor de significancia: $\alpha = 0.05$.

Valor de significancia > 0.05, se admite el supuesto negativo (H_0).

Valor de significancia <= 0.05, se admite el supuesto positivo (H_1).

Tabla 10. *Prueba t-student para el tercer indicador*

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
NDD_PrePrueba NDD_PosPrueba	-3,22600	,28466	,12730	-3,57945	-2,87255	-23,579	4	,000

El valor de T obtenido es -23.579 y es superior a -1.8415; de este modo, se desestimó el supuesto negativo admitiéndose el supuesto positivo. El T calculado, se encuentra localizado en la zona de desestimación, por lo cual, se infiere que: “Hay bastante certeza estadística que la propuesta de un modelo de defensa informático si incrementa de forma trascendental el nivel de disponibilidad de la data de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022”.

V. DISCUSIÓN

En referencia al primer indicador “Nivel de confidencialidad de la data”, se consiguió anterior y posterior a la propuesta del modelo de defensa informático valores de 1.70 y 4.73 puntos, representando un incremento de 3.03 (60.60%). Estos logros son semejantes a los conseguidos por (Quispe, 2021) quien logró una puntuación favorable de confidencialidad de datos de 75,52% a 87,36%, rendimiento de integridad de datos de 50,83% a 76,32% y un aumento significativo en la disponibilidad de datos de 96,81% a 99,93%. Asimismo, son semejantes a (Villarreal, 2021) cuyo logro fue positivo en las dimensiones de información segura, el 68.85% de vulnerabilidad de la confidencialidad de la data disminuyó a 15.40%, de integridad de la data disminuyó en vulnerabilidad de 52.60% a 11.40% y, finalmente en disposición de la data se consiguió reducir la debilidad en las tres dimensiones de 47.15% a 11.95%. Lo sucedido, se soporta en la base teórica del modelo de defensa informático como una orientación sistemática para crear, evaluar, desplegar, sostener, rastrear, promover y examinar la información segura institucional que le permita alcanzar sus objetivos comerciales (INACAL, 2020).

En referencia al segundo indicador “Nivel de integridad de la data”, se consiguió anterior y posterior a la propuesta del modelo de defensa informático valores de 1.81 y 4.77 puntos, representando un incremento de 2.96 (59.20%). Estos logros son semejantes a los conseguidos por (Aliano, 2017), quien obtuvo una consecuencia positiva en la información segura. Se registraron 182 casos antes de la cantidad de data reservada publicada, 50 casos luego del despliegue, 322 casos sobre la cantidad o porcentaje de ingreso y/o alteración no autorizada sobre la data de producción anterior y posterior al despliegue disminuyó a 47 casos, 70,36% de los casos se registró el porcentaje mediante el cual, el programa estaba habilitado para el operador, luego de la implementación se incrementó a 98.22%. Asimismo, son semejantes con los resultados de (Ramos, 2017), fueron insuperables en cláusulas de reserva, integridad y usabilidad, puesto que sus mediciones, así como el valor de la data publicada sin consentimiento, incluían data que podía ser divulgada. Las tasas de falsificación y datos frecuentemente

inaccesibles se alcanzaron en 90,53%, 95,12% y 80,55% respectivamente, esto muestra un mejor monitoreo y una mejor seguridad. Lo sucedido, se soporta en la base teórica del modelo de defensa informático, el cual sostiene como trascendentales bases: fomentar el despliegue de su programa de administración, ahorrando turno y capital, brindando a los involucrados evidencias de que los peligros se abordan correctamente, reafirmando de que nada se encuentre al externo del legajo del MSI, optimizando el desempeño de la normativa ISO 27001, que facilita y simplifica el trabajo de los empleados (Calder, 2016).

En referencia al tercer indicador “Nivel de disponibilidad de la data”, se consiguió anterior y posterior a la propuesta del modelo de defensa informático valores de 1.62 y 4.85 puntos, representando un incremento de 3.23 puntos (64.60%). Estos logros son semejantes a los conseguidos por (Jaén, 2019), quien registró el despliegue de la normativa NTP ISO/IEC 27001:2014 contribuyó a la administración de la reserva, probidad y disposición de la data de RENIEC. Asimismo, son semejantes por (Quispe, 2021) quien logró una puntuación favorable de confidencialidad de datos de 75,52% a 87,36%, rendimiento de integridad de datos de 50,83% a 76,32% y un aumento significativo en la disponibilidad de datos de 96,81% a 99,93%. Lo sucedido, se soporta en la base teórica del modelo de defensa informático se basa en el estudio y examinación de peligros y el hecho de que las entidades aceptan dichos riesgos en un porcentaje que está diseñado para administrarlos de manera efectiva y eficiente. Para implementar con éxito un MSI, es importante analizar los requisitos para una protección adecuada de los datos y, al mismo tiempo, implementar las medidas de control que estén mejor dirigidas a garantizar la protección de los datos relevantes (INACAL, 2020).

VI. CONCLUSIONES

1. Se consiguió comprobar la influencia del modelo de defensa informático con respecto al nivel de confidencialidad de la data de la empresa, generándose un incremento del primer indicador con valores de 1.70 y 4.73 puntos, representando un incremento de 3.03 puntos (60.60%) posterior a la solución tecnológica propuesta para la compañía.
2. Se consiguió comprobar la influencia del modelo de defensa informático con respecto al nivel de integridad de la data de la empresa, generándose un incremento del segundo indicador con valores de 1.81 y 4.77 puntos, representando un incremento de 2.96 puntos (59.20%) posterior a la solución tecnológica propuesta para la compañía.
3. Se consiguió comprobar la influencia del modelo de defensa informático con respecto al nivel de disponibilidad de la data de la empresa, generándose un incremento del tercer indicador con valores de 1.62 y 4.85 puntos, representando un incremento de 3.23 puntos (64.60%) posterior a la solución tecnológica propuesta para la compañía.
4. En referencia al incremento de valores de los tres (3) indicadores se infiere que, el modelo de defensa informático influyó de forma trascendental en la protección de datos de la empresa CGS MAXIMA S.A.C. de la ciudad de Lima en el año 2022.

VII. RECOMENDACIONES

Al Gerente general:

Se sugiere el despliegue de la propuesta tecnológica descrita en esta investigación (modelo de defensa informático) implementando los requisitos de hardware, software y de red indicados en el anexo correspondiente.

Al Jefe de informática:

Se sugiere complementar la propuesta tecnológica descrita generando proyectos de ciberseguridad que apunten a una protección de datos en la nube para la empresa.

Al Jefe de recursos humanos:

Se sugiere diseñar mecanismos de sensibilización en el manejo seguro de la data empresarial, toda vez que éstos sean publicados en la Intranet institucional.

A los trabajadores:

Se sugiere poner en marcha la educación informática recibida sobre el uso de adecuadas prácticas de protección de los datos que establece la normativa mundial ISO/IEC 27002:2013.

REFERENCIAS

Aliano, Hugo. 2017. *"Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin".* Lima : UCV, 2017.

AUDIT-IT. 2022. [En línea] 10 de Febrero de 2022. [Citado el: 16 de Mayo de 2022.] https://www.auditool.org/blog/auditoria-de-ti/8317-que-son-los-controles-de-seguridad-de-ti.

Bonilla, Sleem. 2021. *"Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en Secretaría Ejecutiva de Policía Nacional del Perú".* Lima : UCV, 2021.

Bustinza, Raúl. 2022. *"Modelo de seguridad de la información basado en la normativa ISO/IEC 27001:2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021".* Arequipa : UCV, 2022.

Cáceres, Alejandro. 2017. *"Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño".* Santiago de Chile : UCH, 2017.

Calder, Alan. 2016. *"Nine Steps to Success - An ISO 27001 Implementation Overview".* s.l. : ISGP, 2016. B01F5MCPP0.

Cano, Yolanda. 2018. Política de Privacidad y Protección de Datos. [En línea] 5 de Diciembre de 2018. [Citado el: 22 de Mayo de 2022.] https://yolandamunozcano.com/politica-privacidad-proteccion-datos.

Castillo, Manuel. 2017. *"Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001".* Piura : UCV, 2017.

CGS MAXIMA. 2018. Sitio web de CGS MAXIMA. [En línea] 1 de Enero de 2018. [Citado el: 22 de Mayo de 2022.] https://compuempresa.com/info/cgs-maxima-del-peru-sac-20492168743.

Chinga, Gerson. 2018. *"Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - Piura".* Piura : UCV, 2018.

Esther, Barbé y Orienta, Perni. 2011. *"Mas allá de la seguridad nacional".* Granada : Comares, 2011.

Estrada, Enrique. 2016. *"Norma ISO 27001 para la seguridad de información del área de Registros Académicos del colegio Nuestra Señora del Carmen".* Lima : UCV, 2016.

Foucault, Michael. 2016. *"El nacimiento de la Biopolítica".* Buenos Aires : FCE, 2016.

González, Andrea. 2015. *"Diseño de un modelo de los controles necesarios asociados a la gestión de activos, bajo el cumplimiento de la norma ISO/IEC 27002 anexo A, en una entidad bancaria".* Bogotá : UCC, 2015.

Hernández, Gerardo. 2015. *"Desarrollo de un programa de auditoría para la evaluación del sistema para la gestión de la seguridad de la información del Banco Popular, de conformidad con los marcos de referencia: ISO/IEC 27001 Y COBIT".* Costa Rica : UCR, 2015.

INACAL. 2020. Normas Técnicas Peruanas sobre seguridad de la información. [En línea] 30 de Noviembre de 2020. [Citado el: 22 de Mayo de 2022.] https://www.gob.pe/institucion/inacal/campa%C3%B1as/6610-normas-tecnicas-peruanas-sobre-seguridad-de-la-informacion.

INERCO. 2020. [En línea] 11 de Diciembre de 2020. [Citado el: 10 de Junio de 2022.] https://www.inerco.com/blog/gestion-de-seguridad/.

INSPQ. 2018. Concepto de Seguridad. [En línea] 17 de Agosto de 2018. [Citado el: 4 de Junio de 2022.] https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad.

ISO 27001. 2013. ISO 27001 - Sistema de Gestión de Seguridad de la Información. [En línea] 1 de Enero de 2013. [Citado el: 22 de Junio de 2022.] https://www.dnv.com/ar/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-

3327#:~:text=La%20norma%20ISO%2FIEC%2027001%20le%20ayudar%C3%A1%20a%20proteger%20su,y%20los%20m%C3%A9todos%20de%20tratamiento..

ISO 27002. 2013. ISO/IEC 27002:2013. *Information technology - Security techniques - Code of practice for information security controls.* [En línea] 1 de Octubre de 2013. [Citado el: 28 de Mayo de 2022.] https://www.iso.org/standard/54533.html.

ISO. 2005. ISO/IEC 17799:2005. *Information technology — Security techniques — Code of practice for information security management.* [En línea] 1 de Junio de 2005. [Citado el: 28 de Mayo de 2022.] https://www.iso.org/standard/39612.html.

ISO-Estándares. 2018. NTP ISO 27002: Los Dominios de la Seguridad de la Información. [En línea] 1 de Enero de 2018. [Citado el: 16 de Mayo de 2022.] https://www.isotools.pe/ntp-iso-27001-dominios/.

ISO-TI. 2021. ¿Qué es la seguridad de la información y cuantos tipos hay? [En línea] 11 de Marzo de 2021. [Citado el: 23 de Mayo de 2022.] https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/.

ITGROUP. 2020. [En línea] 1 de Enero de 2020. [Citado el: 16 de Mayo de 2022.] https://peritojudicial.com/activos-informaticos/#:~:text=1.-,Qu%C3%A9%20son%20los%20activos%20inform%C3%A1ticos,ejemplo%20de%20hardware%20y%20software..

Jaén, Moises. 2019. *"Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC".* Lima : UCV, 2019.

Larco, Vinicio. 2017. *"Diseño de modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura" – planta central Quito".* Quito : EPG-UQ, 2017.

LeyProteccionDatos. 2019. Seguridad de la información: Aspectos a tener en cuenta. [En línea] 1 de Enero de 2019. [Citado el: 25 de Mayo de Marzo.] https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/.

LOGITEK. 2019. Estrategia de Defensa en profundidad en ciberseguridad industrial. [En línea] 8 de Noviembre de 2019. [Citado el: 22 de Junio de 2022.]

https://www.ciberseguridadlogitek.com/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/.

Mateo, Edison. 2018. *"Modelo de Seguridad para el Control del Tráfico de la Red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ".* Lima : UCV, 2018.

Medrano, Miguel. 2017. *"Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017".* Lima : UCV, 2017.

Moran, Diana. 2021. *"Análisis de factores críticos de éxito para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa Inversiones Prisco S.A.C – Sechura".* Piura : UCV, 2021.

Ortega, Cristina. 2020. Investigación aplicada: Definición, tipos y ejemplos. [En línea] 1 de Enero de 2020. [Citado el: 22 de Mayo de 2022.] https://www.questionpro.com/blog/es/investigacion-aplicada/.

Prado, Ángel y Roman, Alexander. 2021. *"Sistema web basado en la ISO/IEC 27001 para la gestión de la información en la Empresa P.A Perú S.A.C.".* Lima : UCV, 2021.

Quispe, William. 2021. *"Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021".* Lima : UCV, 2021.

Ramos, Juan. 2017. *"Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017".* Lima : UCV, 2017.

Red IRIS. 2020. Gestión de la seguridad. [En línea] 1 de Enero de 2020. [Citado el: 10 de Junio de 2022.] https://www.rediris.es/cert/doc/unixsec/node31.html.

Riquelme, Matías. 2022. Gestión de la seguridad de la empresa. [En línea] 6 de Enero de 2022. [Citado el: 10 de Junio de 2022.] https://www.webyempresas.com/la-gestion-de-la-seguridad-en-la-empresa/.

Rodríguez, Jorge y Romero, Alejandro. 2019. *"Seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019".* Callao : UCV, 2019.

Ruíz, Alexander y Cahuana, Luis. 2019. *"Automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN INVERSIONES GENERALES S.R.L".* Lima : UCV, 2019.

Solano, Carla. 2020. Mesa redonda sobre Seguridad y Protección de datos. [En línea] 7 de Octubre de 2020. [Citado el: 22 de Mayo de 2022.] https://haycanal.com/noticias/16824/mesa-redonda-sobre-seguridad-y-proteccion-de-datos.

Triguero, David. 2015. *"Protocolos de criptografía para la privacidad y seguridad de información almacenada en aplicaciones libres de la computación en la nube".* La Paz : UMSA, 2015.

Velásquez, Aldrín. 2020. Investigación experimental: Qué es, tipos y cómo realizarla. [En línea] 1 de Enero de 2020. [Citado el: 22 de Mayo de 2022.] https:// www.questionpro.com/blog/es/investigacion-experimental/.

Ventura, José. 2018. *"Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina".* Lima : UCV, 2018.

Villarreal, Eduardo. 2021. *"Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021".* Lima : UCV, 2021.

Zapata, Junior y Merino, Oscar. 2020. *"Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014".* Piura : UCV, 2020.

ANEXOS

Anexo 1 - Matriz de consistencia de la investigación

Título: Modelo de defensa informático para la Protección de datos en la empresa CGS MAXIMA S.A.C., Lima 2022

Autores: Vergaray Pintado Willy Frank / Manihuari Arimuya Luis Carlos

Problema	Objetivo	Hipótesis	Variable	Dimensión	Indicador	Instrumento
General: ¿En qué condición un modelo de defensa informático impacta en la protección de los datos en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022?	General: Incrementar la protección de datos de la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022 mediante la propuesta de un modelo de defensa informático.	General: "El modelo de defensa informático incrementa de manera significativa la protección de datos en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022".	Independiente: Modelo de defensa informático			
Específicos: 1. ¿En qué condición un modelo de defensa informático impacta en la confidencialidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022? 2. ¿En qué condición un modelo de defensa informático impacta en la integridad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022? 3. ¿En qué condición un modelo de defensa informático impacta en la disponibilidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022?	Específicos: 1. Incrementar la confidencialidad de la data en la empresa. 2. Incrementar la integridad de la data en la empresa. 3. Incrementar la disponibilidad de la data en la empresa.	Específicas: 1. "El modelo de defensa informático incrementa la confidencialidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022". 2. "El modelo de defensa informático incrementa la integridad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022". 3. "El modelo de defensa informático incrementa la disponibilidad de la data en la empresa CGS MAXIMA S.A.C de la ciudad de Lima en el año 2022"	Dependiente: Protección de datos	Confidencialidad	Nivel de confidencialidad de la data	Cuestionario
				Integridad	Nivel de integridad de la data	Cuestionario
				Disponibilidad	Nivel de disponibilidad de la data	Cuestionario

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Modelo de defensa informático	“Grupo de pasos, directivas, lineamientos, funciones y bienes establecidos y administrados por un régimen de cuidado de la data como grupo” (INACAL, 2020).	La medición de esta variable se realizó a través de directivas y pasos de seguridad de los datos en la compañía.			
Dependiente: Protección de datos	“Mecanismos de cuidado de la data que conducen a la toma de decisiones en las operaciones organizacionales como: la reserva, la probidad y la disposición, siendo una propuesta de negocio para cualquier compañía a implementarlo” (Cano, 2018).	La medición de esta variable se realizó por el nivel de confidencialidad (reserva), el nivel de integridad (probidad) y el nivel de disponibilidad (disposición) de la data en la compañía.	Confidencialidad	Nivel de confidencialidad de la data	Ordinal
			Integridad	Nivel de integridad de la data	Ordinal
			Disponibilidad	Nivel de disponibilidad de la data	Ordinal

Anexo 3 - Método de juicio experto

Apellidos y nombres del experto: Agreda Gamboa, Everson David

Título profesional y/o Grado académico: Ingeniero de Sistemas / Doctor

Fecha: 06/05/2022

Título del proyecto de investigación: "Modelo de defensa informático para la Protección de datos en la empresa CGS MAXIMA S.A.C., Lima 2022".

Autores: Vergaray Pintado Willy Frank / Manihuari Arimuya Luis Carlos

Evaluación de las normas internacionales para la propuesta de un modelo de defensa informático

Mediante el método de juicio experto, Usted tiene la facultad de calificar las normas internacionales involucradas, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Asimismo, le exhortamos en la correcta determinación de la norma internacional para implementar la solución propuesta en la presente investigación y, también si hubiese algunas sugerencias al respecto:

Ítem	Criterios	Normas internacionales		
		ISO/IEC 27001	ISO/IEC 27002	NTP 17799
1	Tiempo de implementación	3	3	2
2	Información	2	3	2
3	Requerimientos	3	3	2
4	Complejidad	3	3	2
5	Conocimiento	2	3	2
Total		13	**15**	10

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las normas internacionales propuestas

Ítem	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Apellidos y nombres del experto: Mendoza Rivera, Ricardo Darío

Título profesional y/o Grado académico: Ingeniero Industrial / Doctor

Fecha: 06/05/2022

Título del proyecto de investigación: "Modelo de defensa informático para la Protección de datos en la empresa CGS MAXIMA S.A.C., Lima 2022".

Autores: Vergaray Pintado Willy Frank / Manihuari Arimuya Luis Carlos

Evaluación de las normas internacionales para la propuesta de un modelo de defensa informático

Mediante el método de juicio experto, Usted tiene la facultad de calificar las normas internacionales involucradas, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Asimismo, le exhortamos en la correcta determinación de la norma internacional para implementar la solución propuesta en la presente investigación y, también si hubiese algunas sugerencias al respecto:

Ítem	Criterios	Normas internacionales		
		ISO/IEC 27001	ISO/IEC 27002	NTP 17799
1	Tiempo de implementación	2	2	2
2	Información	2	3	2
3	Requerimientos	3	3	2
4	Complejidad	2	2	1
5	Conocimiento	2	3	2
Total		11	**13**	9

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las normas internacionales propuestas

Ítem	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Apellidos y nombres del experto: Córdova Otero, Juan Luis

Título profesional y/o Grado académico: Ingeniero de Computación y Sistemas / Maestro

Fecha: 06/05/2022

Título del proyecto de investigación: "Modelo de defensa informático para la Protección de datos en la empresa CGS MAXIMA S.A.C., Lima 2022".

Autores: Vergaray Pintado Willy Frank / Manihuari Arimuya Luis Carlos

Evaluación de las normas internacionales para la propuesta de un modelo de defensa informático

Mediante el método de juicio experto, Usted tiene la facultad de calificar las normas internacionales involucradas, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Asimismo, le exhortamos en la correcta determinación de la norma internacional para implementar la solución propuesta en la presente investigación y, también si hubiese algunas sugerencias al respecto:

Ítem	Criterios	Normas internacionales		
		ISO/IEC 27001	ISO/IEC 27002	NTP 17799
1	Tiempo de implementación	3	3	2
2	Información	2	3	2
3	Requerimientos	3	3	2
4	Complejidad	2	3	2
5	Conocimiento	3	3	2
Total		13	**15**	10

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las normas internacionales propuestas

Ítem	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Anexo 4 - Instrumentos de recolección de datos

Cuestionario aplicado a los empleados de la empresa CGS MAXIMA S.A.C.

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a la percepción de la protección de datos por parte de los empleados de la empresa.

Se requiere saber su opinión por cada uno de los ítems presentados. Por favor, indique su apreciación objetiva marcando con una “X” sobre cualquier de los números 1, 2, 3, 4 ó 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Protección de datos	Confidencialidad	1. ¿Se cumple con los requerimientos de negocio para el monitoreo de accesos?					
		2. ¿Se cumple con la administración adecuada de ingreso de los usuarios?					
		3. ¿Existe un uso responsable de la data de los usuarios?					
		4. ¿Existe un monitoreo de acceso adecuado a los sistemas y aplicaciones de la empresa?					
	Integridad	5. ¿Se cuenta con obligaciones y procedimientos de operacionalización?					
		6. ¿Se cuenta con el cuidado adecuado frente a código ladino?					
		7. ¿Se cuenta con el uso de copias de seguridad apropiadas?					
		8. ¿Existe un registro conveniente de tarea y monitoreo de los eventos?					
	Disponibilidad	9. ¿Se cumple con una administración adecuada de la seguridad en la red informática?					
		10. ¿Se cuenta con una interconexión segura de la data con terceros?					
		11. ¿Se gestiona un monitoreo de implementación de software en redes tecnológicas?					
		12. ¿Se cuenta de métodos de seguridad vinculados a una infraestructura de servicios de red?					

Anexo 5 - Validación de los instrumentos de recolección de datos

Hoja de validación del instrumento

I. Datos generales:

Cuestionario

II. II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia.*

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Se cumple con los requerimientos de negocio para el monitoreo de accesos?	x		x		x		
2. ¿Se cumple con la administración adecuada de ingreso de los usuarios?	x		x		x		
3. ¿Existe un uso responsable de la data de los usuarios?	x		x		x		
4. ¿Existe un monitoreo de acceso adecuado a los sistemas y aplicaciones de la empresa?	x		x		x		
Dimensión 2: Integridad							
5. ¿Se cuenta con obligaciones y procedimientos de operacionalización?	x		x		x		
6. ¿Se cuenta con el cuidado adecuado frente a código ladino?	x		x		x		
7. ¿Se cuenta con el uso de copias de seguridad apropiadas?							
8. ¿Existe un registro conveniente de tarea y monitoreo de los eventos?	x		x		x		
Dimensión 3: Disponibilidad							
9. ¿Se cumple con una administración adecuada de la seguridad en la red informática?	x		x		x		
10. ¿Se cuenta con una interconexión segura de la data con terceros?	x		x			x	
11. ¿Se gestiona un monitoreo de implementación de software en redes tecnológicas?	x		x			x	
12. ¿Se cuenta de métodos de seguridad vinculados a una infraestructura de servicios de red?	x		x		x		

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Especialidad del evaluador	Redes y Comunicaciones
 **DNI:** 18161457	Trujillo, 27 de mayo del 2022

Hoja de validación del instrumento

I. Datos generales:

Cuestionario

II. II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia*.

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Se cumple con los requerimientos de negocio para el monitoreo de accesos?	x		x		x		
2. ¿Se cumple con la administración adecuada de ingreso de los usuarios?	x		x		x		
3. ¿Existe un uso responsable de la data de los usuarios?	x		x		x		
4. ¿Existe un monitoreo de acceso adecuado a los sistemas y aplicaciones de la empresa?	x		x		x		
Dimensión 2: Integridad							
5. ¿Se cuenta con obligaciones y procedimientos de operacionalización?	x		x		x		
6. ¿Se cuenta con el cuidado adecuado frente a código ladino?	x		x		x		
7. ¿Se cuenta con el uso de copias de seguridad apropiadas?							
8. ¿Existe un registro conveniente de tarea y monitoreo de los eventos?	x		x		x		
Dimensión 3: Disponibilidad							
9. ¿Se cumple con una administración adecuada de la seguridad en la red informática?	x		x			x	
10. ¿Se cuenta con una interconexión segura de la data con terceros?	x		x			x	
11. ¿Se gestiona un monitoreo de implementación de software en redes tecnológicas?	x		x			x	
12. ¿Se cuenta de métodos de seguridad vinculados a una infraestructura de servicios de red?	x		x		x		

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Mendoza Rivera, Ricardo Darío
Especialidad del evaluador	Gestión de Proyectos de TIC
 **DNI:** 18070765	Trujillo, 27 de mayo del 2022

Hoja de validación del instrumento

I. Datos generales:

Cuestionario

II. II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (√) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia.*

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Se cumple con los requerimientos de negocio para el monitoreo de accesos?	x		x		x		
2. ¿Se cumple con la administración adecuada de ingreso de los usuarios?	x		x		x		
3. ¿Existe un uso responsable de la data de los usuarios?	x		x		x		
4. ¿Existe un monitoreo de acceso adecuado a los sistemas y aplicaciones de la empresa?	x		x		x		
Dimensión 2: Integridad							
5. ¿Se cuenta con obligaciones y procedimientos de operacionalización?	x		x		x		
6. ¿Se cuenta con el cuidado adecuado frente a código ladino?	x		x		x		
7. ¿Se cuenta con el uso de copias de seguridad apropiadas?							
8. ¿Existe un registro conveniente de tarea y monitoreo de los eventos?	x		x		x		
Dimensión 3: Disponibilidad							
9. ¿Se cumple con una administración adecuada de la seguridad en la red informática?	x		x		x		
10. ¿Se cuenta con una interconexión segura de la data con terceros?	x		x			x	
11. ¿Se gestiona un monitoreo de implementación de software en redes tecnológicas?	x		x		x		
12. ¿Se cuenta de métodos de seguridad vinculados a una infraestructura de servicios de	x		x		x		

[1]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

[2]**Pertinencia:** Si el ítem pertenece a la dimensión.

[3] **Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Ms. Córdova Otero, Juan Luis
Especialidad del evaluador	Sistemas de información y comunicación
 **DNI:** 18122765	Trujillo, 27 de mayo del 2022

Anexo 6 - Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,813	12

Anexo 7 - Solución propuesta

Modelo de defensa informático para la empresa CGS MAXIMA S.A.C.

Según LOGITEK (2019), el modelo Confidencialidad - Integridad - Disponibilidad o llamado también “CIA” no es adecuado para una comprensión completa de los requisitos de seguridad de una infraestructura crítica. Para ello, hace falta considerar otros requisitos fundamentales como:

- Control de acceso: proteger los activos de accesos e información de accesos no autorizados.
- Control de uso: proteger a los activos de operaciones no autorizadas.
- Integridad de la información: proteger los canales de comunicación contra de cambios no autorizados de la información que transportan.
- Confidencialidad de la información: asegurar que la información del espionaje.
- Restringir los flujos de datos: proteger los canales de comunicación para evitar que la información llegue a destinos no autorizados.
- Respuesta a incidentes: asegurar que se responde a incidentes de ciberseguridad de forma correcta. Implica: monitorización, reporte de alertas y la ejecución de acciones correctoras.
- Disponibilidad de recursos: asegurar que todos los recursos del sistema están disponibles y protegerlos de denegaciones de servicio.

Por tanto, es necesario implementar nuevos controles de seguridad que los proteja, asegure su disponibilidad y su correcto funcionamiento, tanto de las operaciones como de los equipos de la organización.

En las contramedidas típicas a utilizar para minimizar amenazas externas son:

- ✓ Autenticación de usuarios y equipos.
- ✓ Controles de acceso.
- ✓ IDS
- ✓ Uso de cifrado.
- ✓ Uso de firmas digitales
- ✓ Aislamiento y/o segregación de redes/dispositivos.
- ✓ Escáneres de vulnerabilidades.
- ✓ Monitorización de la actividad de los equipos y de la red.
- ✓ Seguridad física.

Para la mitigación de amenazas internas hace falta una aproximación diferente, dado que un posible atacante tendría la posibilidad de saltarse las contramedidas normales. En este caso, se requiere poner más énfasis en contramedidas como las políticas y procedimientos, separación de roles, monitorización de las actividades, cifrado y auditoría de sistemas.

Por tanto, una tecnología, producto o solución única no es suficiente para proteger adecuadamente los sistemas de control. Se requiere emplear una estrategia multicapa que incluya dos o más mecanismos de seguridad que se superpongan, es decir, emplear estrategias de defensa informática.

Una estrategia de defensa informática incluye el uso de cortafuegos, creación de DMZ, el uso de soluciones para la detección de intrusiones, políticas de seguridad efectivas, programas de formación, respuesta ante incidentes, mecanismos para garantizar la seguridad física y mecanismos para la monitorización y alerta de incidentes. De esta manera, si una salvaguarda en particular falla, existirán otras en las capas inferiores que mantendrán el riesgo en niveles aceptables.

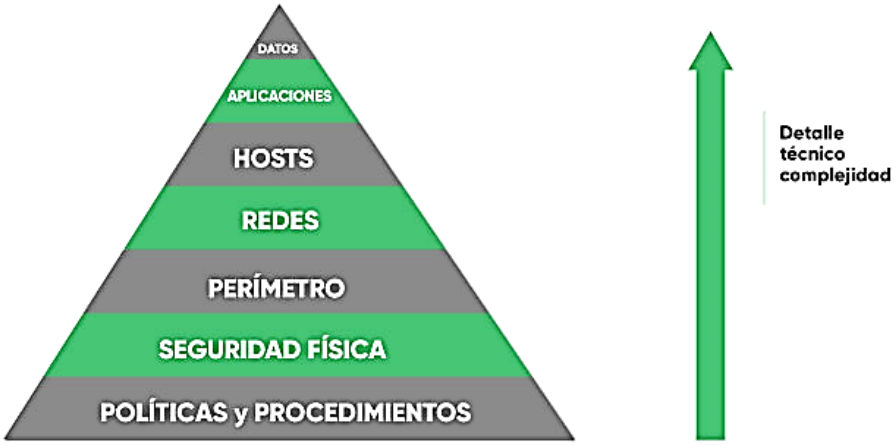

Figura. Modelo de defensa informático propuesto

El modelo de defensa informático presentará los siguientes niveles o capas de protección:

- Nivel 1: Políticas y procedimientos de seguridad.
- Nivel 2: Seguridad física y del entorno.
- Nivel 3: Defensa perimetral.
- Nivel 4: Defensa de red.
- Nivel 5: Defensa de equipos.
- Nivel 6: Defensa de aplicaciones.
- Nivel 7: Defensa de datos.

- *Nivel 1: Políticas y procedimientos de seguridad*

Este nivel se encuentra conformado por un conjunto de reglas, obligaciones y procedimientos que definan el enfoque de la organización para la protección y seguridad de la información. Las políticas deben comunicarse a toda la organización en una forma apropiada, entendible y accesible.

Se diagnosticó lo siguiente:

- ✓ Existen políticas de seguridad de la información definido y aprobado por la alta dirección, socializado al interno de la empresa.
- ✓ Existe un área de control interno encargado de mantener actualizadas las políticas de seguridad de información.
- ✓ El personal del área de Informática vela por la seguridad de la información interna de la empresa, establece una estructura organizacional aprobada por la alta gerencia, para la designación de deberes.
- ✓ La jefatura del área de Informática planifica las reuniones con la alta dirección con actas de reunión.
- ✓ Se establece una política sobre el control de actividades de los usuarios de los dispositivos móviles.
- ✓ Se utiliza VPN y aplicaciones de control remoto de los ordenadores al personal de todo nivel jerárquico de la empresa.
- ✓ Se solicita la presentación de antecedentes penales y judiciales, a personal postulante a un puesto de trabajo en la empresa.
- ✓ Se detallan las funciones de cada trabajador en el documento contractual.
- ✓ Se entrega a todo personal al ingreso su reglamento interno de trabajo.
- ✓ El área de recursos humanos y la jefatura del área establecen las condiciones de salida del colaborador.

Se planteó lo siguiente:

- ✓ Contactar con grupos especializados en seguridad de la información para que se brinde capacitaciones a la organización y así estar actualizados sobre los últimos avances sobre el tema.
- ✓ Tener una política de seguridad de la información en la planificación de los proyectos y designar responsables que velen por el cumplimiento de las misma durante la ejecución de los proyectos.
- ✓ Se plantea realizar talleres de capacitación al personal de la empresa sobre seguridad de la información.

- *Nivel 2: Seguridad física y del entorno*

Este nivel tiene como objetivo evitar que un posible atacante disponga de acceso físico a los equipos e infraestructuras de red industrial (al hardware). Las barreras, mecanismos de control de acceso físico y de vigilancia son los pilares para incrementar la seguridad de esta dimensión.

Se diagnosticó lo siguiente:

- ✓ Se tiene una distribución adecuada para los lugares de trabajo.
- ✓ Se tiene una vigilancia permanente para el acceso a las zonas de trabajo.
- ✓ Se tiene un personal que encarga que las oficinas estén debidamente cerradas al momento de culminar la hora de trabajo, se tiene cámaras de seguridad.
- ✓ Se tiene una infraestructura basada en el reglamento nacional de edificaciones.
- ✓ Se tiene áreas señalizadas y distribuidas adecuadamente.
- ✓ Se tiene un ambiente de almacén para la entrega y carga de equipos.
- ✓ Anualmente se hace auditoria de tecnologías de la información y si dejará observaciones para ser subsanadas en el siguiente periodo.

Se planteó lo siguiente:

- ✓ Contactar con grupos especializados en seguridad de la información para que se brinde capacitaciones a la organización y, así estar actualizados sobre los últimos avances sobre el tema.
- ✓ Separar los ambientes para el trabajo específico en la empresa.
- ✓ Se debería tener una gestión adecuada para cualquier cambio en las instalaciones.
- ✓ Se debe tener una documentación adecuada sobre las vulnerabilidades de las instalaciones y ambientes de trabajo, así como las medidas que se deberían tomar.
- ✓ Las áreas restringidas a personal autorizado deberían contar con un área de recepción atendida o medios de control adecuados para limitar el acceso físico.
- ✓ Si es aplicable deberían considerarse barreras físicas que impidan el acceso no autorizado y protejan el área de agentes ambientales adversos.
- ✓ Contar con sistemas de protección contra el fuego cumpliendo con la legislación vigente.
- ✓ Se deben considerar sistemas de detección de intrusos (por ejemplo: alarmas).
- ✓ Deberían separarse físicamente las áreas de proceso de información que van a ser gestionadas por personal externo de las propias de la organización.

- *Nivel 3: Defensa perimetral*

En este nivel, el perímetro es el punto o conjunto de puntos de la red interna de confianza, gestionada por la propia organización, entra en contacto con otras redes externas o no fiables, cómo puede ser Internet o redes gestionadas por terceros. El atacante puede tener acceso a los servicios ofrecidos o accesibles desde el exterior y aprovecharse de ellos para realizar una actividad maliciosa. Las medidas en esta capa se centran en el aseguramiento de los accesos remotos a la red.

Se diagnosticó lo siguiente:

- ✓ El área de Informática cuenta con una política de restricción a los privilegios de acceso a los usuarios remotos.
- ✓ Se tiene documentación especificando responsabilidades de terceros generado por el área de Informática.
- ✓ Se reportan todos los eventos de seguridad de información externos vía correo electrónico o anexo telefónico.
- ✓ Se tiene una respuesta rápida antes los incidentes externos de seguridad la información.
- ✓ Anualmente la empresa tiene auditorías externas sobre la seguridad de la información validando el cumplimiento de las políticas y estándares de seguridad.
- ✓ Se cuenta con un plan de trabajo para la verificación del cumplimiento técnico a través de auditorías externas.
- ✓ Se tiene un plan de trabajo para asegurar la continuidad de la seguridad de la información a través de backups, dispositivos virtuales, etc.
- ✓ Se realizan los backups de dispositivos, servidores virtuales y base de datos con la especificación técnica correspondiente.
- ✓ Se tiene una política de revisión de backups realizados aplicando auditoría interna.

Se planteó lo siguiente:

- ✓ Contar con procedimientos de inicio de sesión seguro para evitar el ingreso de personas no autorizadas y puedan manipular información sensible.
- ✓ Contar con un sistema de reportes donde se reporten las vulnerabilidades externas en el tema de seguridad de información
- ✓ Realizar una valoración a los eventos de seguridad de la información externas y, por lo tanto, tomar decisiones efectivas.
- ✓ Contar con una bitácora de colección de evidencias de los incidentes.

- *Nivel 4: Defensa de red*

En este nivel, si el atacante tiene acceso a la red, puede monitorizar el tráfico que circula por ésta, de forma pasiva (solo lectura) o activa (modificación posible). Para proteger la red de estas amenazas suelen utilizarse sistemas de detección de intrusiones y sistemas de prevención de intrusiones.

Se diagnosticó lo siguiente:

- ✓ En cuanto a los controles de red, seguridad en los servicios en red y la segregación en redes, todos estos servicios son brindados por una empresa tercerizadora.
- ✓ Se tiene protocolos para la transferencia de información.
- ✓ Dentro del acuerdo para la transferencia de información, hay cláusulas de confidencialidad y por lo tanto penalidades.
- ✓ Los colaboradores de la empresa tienen conocimiento de las políticas de control de acceso a la red.
- ✓ Cada área cuenta con una infraestructura de red apropiada para sus requerimientos.
- ✓ Se cuenta con una política de registro y baja registro de usuario de red efectiva, administrada por las jefaturas de las áreas responsables.
- ✓ Se establecen permisos y privilegios por grupos de usuario de red en cada área.
- ✓ Se cuenta con una política de autenticación secreta de usuarios de la red.
- ✓ Existe una política para seleccionar a los proveedores que cumplan los requerimientos de acceso a Internet.
- ✓ Se tiene políticas de auditorías con los proveedores de Internet que brindan servicios de comunicación para que, en caso de incumplir la forma de servicio se impondría penalidades al proveedor.
- ✓ Para todo software a nivel de red que se tiene en la empresa, se cuenta con la licencia respectiva, sino se usaría software libre.

Se planteó lo siguiente:

- ✓ Utilizar un protocolo para el envío de información por mensajería electrónica.
- ✓ Se debería tener un flujo de trabajo sobre todos los cambios que en los servicios de Internet que realiza el proveedor.
- ✓ Se plantea la mejora en el proceso de generación de logs para el administrador de red, dado que actualmente se cuenta con un log de operador.
- ✓ Generar una base de conocimiento para almacenar todos los incidentes de seguridad de la información en el ámbito de las redes.

- *Nivel 5: Defensa de equipos*

En este nivel, la seguridad de equipos, tanto servidores como clientes, se basa en la implementación de medidas de protección de estos equipos que permiten a los usuarios finales realizar sus operaciones de negocio cotidianas.

Se diagnosticó lo siguiente:

- ✓ Se cuenta con un servicio tercerizado que se encarga de la instalación y el constante mantenimiento del equipo para su correcto funcionamiento.
- ✓ Se cuenta con un servicio brindando por un tercero, pero se está en constante evaluación.
- ✓ Se tiene un protocolo de firma de constancia tanto de salida como de entrada de los activos a las diferentes sedes.
- ✓ El servicio externo una vez el equipo se encuentra inoperativo se encarga de extraerlo de la empresa.
- ✓ Servicio in-house brindando por un tercero.
- ✓ Servicio brindado por un tercero que se encarga de la limpieza diaria de las oficinas y el pulido de pisos cada tres meses.
- ✓ Se realiza una medición y seguimiento del uso de recursos de hardware presentes en los equipos informáticos.

Se planteó lo siguiente:

- ✓ Instalar parches de seguridad para eliminar vulnerabilidades conocidas.
- ✓ Desactivar todos los servicios innecesarios para minimizar el factor de exposición del equipo.
- ✓ Disponer de un antimalware activo en todos los equipos informáticos.
- ✓ Controlar las comunicaciones entrantes mediante un cortafuegos.
- ✓ Restringir la ejecución de aplicaciones en equipos dedicados como los servidores.
- ✓ Utilizar protocolos de salida y llega de los equipos informáticos al momento de ser movilizados de un lugar a otro.
- ✓ Los equipos deberían escanearse periódicamente especialmente cuando se va a instalar un nuevo software.
- ✓ Planificar las ampliaciones de capacidad de los recursos de hardware de los equipos cuando sea necesario.
- ✓ El proceso de sincronización de relojes en los servidores debe estar documentado con los requisitos necesarios para que esto se cumpla.

- *Nivel 6: Defensa de aplicaciones*

  En este nivel, las aplicaciones se protegen realizando un control de acceso mediante la sólida implantación de mecanismos de autenticación y autorización.

  Se diagnosticó lo siguiente:

  ✓ Aparte de los requerimientos funcionales, el área de Informática se encarga de asesorar sobre la seguridad de los sistemas de información.

  ✓ Se tiene una monitorización sobre el adecuado funcionamiento de los sistemas que tienen contacto directo con el cliente.

  ✓ Se tiene protocolos para la confirmación de los pagos y el ingreso de datos del área operacional.

  ✓ Una vez puesto en producción los sistemas de información, se guardan copias de seguridad debidamente documentado.

  ✓ Una vez puesto en producción el sistema se tiene un protocolo de monitoreo por dos semanas.

  ✓ Se realizan cambios en los módulos del sistema, previamente testeados y monitoreados.

  ✓ Se tiene implementado un servidor de versiones el cual controlamos los cambios por fechas de los desarrollos.

  ✓ Solamente el área de Informática tiene los privilegios de acceso al código fuente de los programas.

  ✓ Se le presenta una versión demo al área que hace el requerimiento para que haga todas las pruebas necesarias para dar la conformidad del requerimiento.

  Se planteó lo siguiente:

  ✓ Se debe tener un software controlador de versiones para todos los cambios que se realicen en los sistemas de información.

  ✓ Se debe de implementar todos los principios de seguridad que normal la Ingeniería de Sistemas.

  ✓ En la actualidad, sólo se tiene un software (Spring) con soporte tercerizado, pero el resto de sistema brinda soporte informático.

  ✓ Se implantará un software controlador de versiones para todos los cambios que se realicen en los sistemas.

  Plantear políticas de desarrollo y modificaciones de los sistemas informáticos de la empresa por parte de empresas proveedoras del servicio de desarrollo de software.

- *Nivel 7: Defensa de datos*

En este nivel, si un atacante ha conseguido traspasar todas las protecciones anteriores y tiene acceso a la aplicación, la autenticación y autorización, así como el cifrado, constituyen las tecnologías más empleadas para proteger los datos.

Se diagnosticó lo siguiente:

- ✓ Anualmente la empresa realiza un inventariado total, a través de un tercero, de los activos de información que posee dentro de sus instalaciones.
- ✓ Se categoriza la propiedad de los activos de información con que cuenta la empresa.
- ✓ Se comunica a los usuarios sobre el correcto uso y cuidado de los activos de información.
- ✓ Se comunica al propietario del activo de información sobre las penalidades por incumplimiento o daño sobre el mismo.
- ✓ Existe una administración de la información dentro de la misma empresa y, se estable un buen manejo según su clasificación.
- ✓ Existe un etiquetado de la información para su codificación y facilitar su búsqueda.
- ✓ Se cuenta con una política para el manejo de activos, inventariado y análisis de estado.
- ✓ La jefatura de cada área se encarga de la gestión de medios removibles a su cargo.
- ✓ La jefatura de cada área se encarga de la eliminación de medios.
- ✓ Se establece por ley, el uso confidencial de los datos de la empresa.
- ✓ Se cuenta con las restricciones a los usuarios no autorizado.
- ✓ Se cuenta con una política de gestión de contraseñas para acceso a la información.
- ✓ Existe la generación de llaves tanto públicas como privadas.
- ✓ Los datos de prueba se encuentran administrados por el encargado de la base de datos de manera que es el único que brinda permisos a las tablas y las operaciones que se pueden hacer sobre las mismas.

Se planteó lo siguiente:

- ✓ Usar de mecanismos automatizados para realizar copias de seguridad de los sistemas de control que permita disponer de un control de versiones.
- ✓ Redundar el almacenamiento de las copias de seguridad.
- ✓ Para el adecuado control y respaldo de la información que se transporta.
- ✓ Disponer de una política en el uso de controles cifrados para que en caso de que la información caiga en manos no autorizadas, esta no sea legible ni pueda descifrarse.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, AGREDA GAMBOA EVERSON DAVID, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Modelo de defensa informático para la Protección de los datos en la empresa CGS MAXIMA S.A.C., Lima 2022", cuyos autores son MANIHUARI ARIMUYA LUIS CARLOS, VERGARAY PINTADO WILLY FRANK, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 01 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
AGREDA GAMBOA EVERSON DAVID **DNI:** 18161457 **ORCID:** 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 01-12-2022 06:34:59

Código documento Trilce: TRI - 0465003

INVESTIGA UCV