UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020

TESIS PARA OBTENER EL GRADO ACADÉMICO DE

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Bohorquez Salcedo, Alberto Ismael (ORCID: 0000-0002-7596-1768)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (ORCID: 0000-0002-0024-668X)

LÍNEA DE INVESTIGACIÓN:

Auditoria de sistemas y seguridad de la información

LIMA — PERÚ

2021

DEDICATORIA

Mi tesis la dedico a mi esposa Luz quien siempre ha está a mi lado para apoyarme, y a mis hijos Loraine y Loen por ser mi motivo de superación personal y profesional. A mis padres y hermanos que me animaron para seguir desarrollándome profesionalmente.

AGRADECIMIENTO

Agradezco primeramente gracias a mi familia por todo su apoyo. También a los distintos docentes de la Universidad Cesar Vallejo por haber contribuido en mi formación profesional.

Índice de contenidos

Índice de tablas

Índice de figuras y gráficos

Resumen

La presente investigación titulada Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020, tuvo como objetivo principal determinar la relación de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

La investigación es de tipo básico, correlacional - no experimental determinándose la relación entre las variables de la investigación. La población de estudio considerada fue de 87 colaboradores de la empresa I & T Electric, se aplicó un tipo de muestreo no probabilístico aleatorio simple, considerando una muestra de 71 colaboradores, la información fue recolectada a través de la técnica de investigación de la encuesta, ejecutándose un cuestionario.

Para la prueba estadística inferencial de los datos se empleó el coeficiente de correlación Rho de Spearman. La investigación concluye evidenciándose una correlación de nivel muy fuerte de 0,832 entre la variable Ciberseguridad y la variable Gestión de tecnología de información.

Palabras clave: Ciberseguridad, Gestión de Tecnologías de información, Seguridad de Sistemas de información

Abstract

The present research entitled "Cybersecurity and its relationship in the management of information technologies in the company I & T Electric, Lima - 2020", had as main objective to determine the relationship of cybersecurity with the management of information technologies in the company I & T Electric, Lima - 2020.

The research is of a basic, correlational - non-experimental type, determining the relationship between the research variables. The study population considered was 87 employees of the company I & T Electric, a type of simple random non-probability sampling was applied, considering a sample of 71 employees, the information was collected through the survey research technique, running a questionnaire.

Spearman's Rho correlation coefficient was used for the inferential statistical test of the data. The research concludes, showing a very strong correlation of 0.832 between the Cybersecurity variable and the Information Technology Management variable.

Keywords: Cybersecurity, Information Technology Management, Information Systems Security

I. INTRODUCCIÓN

Los grandes cambios que se vienen desarrollando en el entorno mundial de las tecnologías de la información hacen que el intercambio de información a través de los medios tecnológicos sea una necesidad cada vez más indispensable, tanto para la industria privada como para el sector público y consecuentemente para la vida cotidiana que conocemos; parte de este desarrollo trae consigo nuevos retos como lo son la protección ante riesgos de ataques informáticos de distintas índoles, ataques que se desarrollan buscando vulnerar la información de las entidades con fines inescrupulosos.

Debido a estas amenazas los países hacen esfuerzos súbitos para no sucumbir ante los ataques de los cibercriminales que evolucionan conjuntamente con las tecnologías, logrando considerarse como los riesgos más latentes en la seguridad de la información; la European Union Agency for Cybersecurity (ENISA, 2020) menciona que en el 2019 se presentó un aumento significativo de casi un 80% respecto a las incidencias de ciberseguridad respecto al año anterior. Sin embargo y a pesar de esas grandes amenazas, un gran porcentaje de las organizaciones no invierten prudentemente en una adecuada gestión de tecnologías de información que pueda afrontar, bloquear o mitigar los riesgos de la ciberseguridad, conllevando en demasiadas ocasiones a la perdida de los activos de información y afectando directamente a la continuidad de las empresas y de las organizaciones.

En el Perú cada vez es más usual escuchar que una entidad ha sufrido un ataque cibercriminal que daño consideradamente los activos de información, el Diario Gestión (2020) menciona que, cuando inicio la cuarentena, los ataques a dispositivos móviles en el Perú se duplicaron, conjuntamente informo, que correos enviados con información engañosa aumentaron un 25% a inicios del 2020, finalmente hacen un énfasis respecto a que los cibercriminales no descansan y por ende, los especialistas ciberseguridad en las organizaciones deben estar alertas constantemente cuando de ciberseguridad se refiere.

Tal es el caso de la Empresa I & T Electric conocido con su marca como Itesa, la cuál será motivo de este estudio de investigación; Desde julio del 2019 hasta agosto del 2020 Itesa ha sufrido ataques a su ciberseguridad, ataques que bien pudieron haberse evitado con una adecuada gestión de las tecnologías de información, la cual le costó a la empresa mucho dinero y tiempo para restablecer los daños causados a sus activos de información, bases de datos y sistemas en general.

Por todo lo anteriormente descrito, a continuación se plantea la siguiente interrogante como problema general ¿Qué relación existe entre la ciberseguridad y la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020? Asimismo se plantean los consecuentes problemas específicos, ¿Cómo se relaciona la gestión de tecnologías de información con la dimensión prevención de la ciberseguridad en la empresa I & T Electric, Lima - 2020? ¿Cómo se relaciona la gestión de tecnologías de información con la dimensión detección de la ciberseguridad en la empresa I & T Electric, Lima - 2020? ¿Cómo se relaciona la gestión de tecnologías de información con la dimensión reacción de la ciberseguridad en la empresa I & T Electric, Lima - 2020?

En la presente investigación se justifica desde cuatro ámbitos: La justificación Epistemológica es fundamental, ya que el investigador expondrá de manera adecuada y detallada los pasos realizados en cada proceso o etapa de la investigación, además se explicará también el uso correcto de los conocimientos científicos empleados, permitiendo así transmitir un nuevo conocimiento claro y conciso respecto al objetivo de la investigación.

Se justifica teóricamente por que se desarrolla un marco teórico y conceptual de las variables de estudio y sus dimensiones respectivas, tomando en cuenta una amplia bibliografía de procedencia académica científica que permite analizar y contrastar la información relevante, para así establecer un enfoque de entendimiento adecuado a la investigación que conlleva a un significativo aporte científico sobre la ciberseguridad y la gestión de tecnologías de información.

Tiene justificación práctica porque se resuelve una interrogante general que permitirá a una organización determinar si debe enfocarse en la ciberseguridad para mejorar una de las principales áreas como lo es tecnologías de información. También se justifica metodológicamente porque las actividades se efectuarán teniendo en cuenta las prácticas recomendadas en una investigación científica con la intención de determinar la relación de las variables de estudio.

El objetivo general del presente trabajo de investigación es determinar la relación de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Subsecuentemente se plantean los siguientes objetivos específicos: Determinar la relación que existe entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Determinar la relación que existe entre la dimensión detección de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Determinar la relación que existe entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020

Luego de establecer los objetivos de estudio, se procede a establecer la hipótesis general, existe relación significativa de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Consecuentemente se plantearon las hipótesis específicas: existe relación significativa entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Existe relación significativa entre la dimensión detección de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Existe relación significativa entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

II. MARCO TEÓRICO.

Para el trabajo de investigación se han considerado como antecedentes, estudios previos nacionales e internacionales con contenidos y objetivos de estudio similares a los del presente. En el ámbito nacional de los antecedentes que se presenta a Huerta (2019) en la investigación denominada sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en una consultora cuyo objetivo principal evaluar la implementación del sistema de gestión de seguridad de la información influye en el proceso de gestión del riesgo en una consultora, llegando a la siguiente conclusión: Se logró constatar que la variable gestión de seguridad incide significativamente y favorablemente en el proceso de la gestión de riesgo en una consultora. Asimismo se tiene a Huayllani (2020) en la investigación denominada Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud cuyo objetivo principal fue medir la influencia de la aplicación de un sistema de gestión de seguridad de la información en la gestión del riesgo, llegando a la siguiente conclusión: El sistema de gestión de seguridad de la información se relaciona con la gestión del riesgo en el Ministerio de Salud para el año 2019, analizado en la unidad de gestión de inversión de reconstrucción con cambios. Por otro lado está Sánchez (2017) en la investigación denominada Adopción de estrategias de ciberseguridad en la protección de la información en la oficina de economía del ejército cuyo objetivo principal fue determinar de qué manera la adopción de estrategias de ciberseguridad incide en la protección de la información en la Oficina de Economía del Ejército, llegando a la siguiente conclusión: Al adoptar estrategias de ciberseguridad se incide significativamente en la protección de la información en la Oficina de Economía del Ejército. Por último está Inoguchi y Macha (2017) en la investigación Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú, cuyo objetivo principal fue determinar la influencia de la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, llegando a la siguiente conclusión: La ciberseguridad que se administra en las empresas para la protección de los activos informáticos debe ser prioridad de la gerencia general, compromiso que también debe ser compartido con todos los

colaboradores sin importar la jerarquía; asimismo se debe elaborar un plan formal con todas las actividades que se ejecutaran.

En relación al ámbito de antecedentes internacionales, se refiere el estudio de Landázuri (2019) en la investigación denominada Diseño de un modelo de gobernabilidad y gestión de tecnologías de Información para el área de desarrollo de proyectos de software de corporación favorita, basado en la metodología Devops, en Ecuador, cuyo objetivo principal fue diseñar un modelo de gobernabilidad y gestión de proyectos de software, basado en las etapas propuestas por la metodología DevOps, que mejore los procesos de desarrollo que se utiliza en el área de desarrollo de proyectos de la corporación Favorita C.A., llegando a la siguiente conclusión: El modelo de gobierno de TI desarrollado comprende el conjunto de cada proceso y el detalle de cada iteración. Por cada proceso se realizó una matriz de caracterización donde se explican los objetivos, actores, entradas, salidas, modo de recolección de la información y forma de medición. De igual manera Garbarino (2014) en la investigación denominada Marco de gobernanza de TI para empresas PyMEs - SMEsITGF, en España, cuyo objetivo principal fue construir un marco que permita a las PyMEs incorporar un marco efectivo para gobernar y gestionar TI adecuadamente, llegando a la siguiente conclusión: Los sistemas informáticos son agentes estratégicos esenciales para el cumplimiento de metas en las organizaciones, más aún cuando los sistemas informáticos están enfocados a los objetivos de la organización. También Arias y Celis (2015) en la investigación denominada Modelo experimental de ciberseguridad y ciberdefensa para Colombia, cuyo objetivo principal fue construir el modelo de referenciación que garantice al estado colombiano parametrizar las condiciones de protección en el ciberespacio como respuesta a los ataques producidos por guerra de la información, llegando a la siguiente conclusión: Se logra evidenciar que el uso de un modelo internacional de ciberseguridad es viable para la protección de la información en las organizaciones. De igual forma Marcos (2018) en la investigación nombrada Ciberseguridad aplicada a la e-democracia: análisis criptográfico y desarrollo de una metodología practica de evaluación para sistemas de voto electrónico remoto y su aplicación a las soluciones más relevantes, en España, cuyo

objetivo principal fue Determinar si existe en la actualidad algún sistema/tecnología de Voto Electrónico Remoto lista para ser implantada en procesos electorales, llegando a la siguiente conclusión: Se logró evidenciar la importancia e influencia de la Ciberseguridad en los votos electrónicos remotos, haciendo hincapié en la importancia de la transparencia que se debe tener en los eventos políticos.

En correspondencia a las conjeturas que avalan la presente investigación se ha considerado la teoría general de sistemas (TGS) donde Ñeco et al. (2018) menciona que al hablar de esta teoría se decreta que un sistema es una red donde sus componentes interaccionan basados en estructura y función. La TGS deslinda distintos niveles de complejidad además emplea términos relativos a procesos de tecnologías que de carácter social, no obstante logran transmitir un enfoque requerido para la constitución de análisis. Desde otra perspectiva Maldonado (2017) señala que la TGS se conforma por metodologías y métodos que mencionados provechosamente facilitan una visión prismática del universo que se ejecuta, produciendo conjuntos de resoluciones para las incógnitas, en tal sentido permite una dinámica donde se circula fácilmente las ideas, permitiendo aportaciones, en tal sentido la sociedad y la ciencia son beneficiados equitativamente. En otro panorama Cathalifaud (1998) indica que la TGS es una concepción de lo real donde se considera la visión sistémica y científica adoptando variados aspectos punitivos. Un factor principal o particular es que se planifica de manera holística e integral, debido a que se consolida la correspondencia entre sus elementos como grupos que se conjugan.

En afinidad a las conjeturas que avalan la presente investigación, se considera la teoría de cibernética en el cual Barberousse (2008) refiere que, se trata de la investigación constante entre los seres vivos, los sistemas de comunicación y las maquinas, en esencia trata sobre el estudio de los aportes que pueden brindar las tecnologías a la vida cotidiana del ser humano. Otra conjetura citada es la teoría de la Información en la cual Borraccimtsac y Tajermtsac (2006) mencionan que se basa o está constituida por datos y que aquellos datos permiten disipar dudas y conocer sobre alguna incógnita respeto a aquello que ignoramos o que queremos conocer.

En el presente proyecto de investigación se ha nombrado como variables de estudio, a la ciberseguridad y a la gestión de tecnologías de información; por ende, se ha recopilado definiciones para cada una de ellas, estás definiciones permitirán un mejor entendimiento del proyecto de investigación, siendo así, en una de las definiciones de la primera variable citadas se contempla a la fundación Telefónica (2016) quienes describen que la ciberseguridad es un proceso que implica prevención, detección y reacción, en el cual se debe considerar aprendizaje objetivo que conlleve a la mejora continua inherente del mencionado proceso. Desde otro plano Becerril (2019) y Solms (2013) coinciden al exponer que la ciberseguridad es una recopilación de instrumentos, normas, definiciones, tips, perspectivas de gestión de riesgos, accionares, enseñanza, mejores hábitos, aval y tecnologías que se emplean o son usadas para la seguridad cibernética y los activos de las organizaciones y de los usuarios. Desde otra concepción Sabillon (2018) resalta que ISACA definió la Ciberseguridad como el salvaguardo de los activos informáticos ya que se da puntualidad a los agentes que amenazan la información tratada, almacenada en las bases de datos y que se comparte usando los sistemas a través de las redes con diferentes fines. En otra perspectiva se tiene a la empresa de antivirus Kaspersky (2020) y la empresa informática CISCO (2019) que coinciden describiendo que la ciberseguridad es en esencia la destreza de mantener a buen resguardo los sistemas, redes, software de seguridad y otras herramientas tecnologías que forman parte de un sistema.

Tomando como referencia el concepto de ciberseguridad brindado por la fundación Telefónica (2016), las dimensiones serían prevención, detección y reacción: Para la primera dimensión de la variable ciberseguridad Mozaffari et al. (2019) menciona que la prevención es aquella fase que tiene como principal fin ofrecer soluciones centradas en el internet de las cosas que optimizan las condiciones físicas, fisiológicas y ambientales para prever eventos de fallas en el servicio, en lo global, la prevención se ofrecen enfocados a los factores de riesgo. En otra perspectiva García y Gonzales (2013) exponen que la prevención está relacionada con la preparación de usuarios humanos y a la par de máquinas que dan soporte para salvaguardarse ante algún tipo de ciberamenaza, de tal manera se promueve una correcta administración de la

seguridad y se evitan tecnologías que podrían ser fáciles de sobrepasar. En otra visión Arend et al. (2020) precisan que la prevención es la toma de acciones anticipadas que podrían poner en riesgo a los usuarios en las empresas, en particular se trata de realizar acciones específicas en medidas de seguridad que puedan disminuir el riesgo de ciberataques. En otro panorama Meyer, Dembinsky y Raviv (2020) exponen que la prevención trata de la anticipación ante las amenazas en los sistemas informáticos e implica el uso de algoritmos que analizan eventos y asignan un valor a cada evento, conforme a este análisis. Los valores resultantes pueden ser usados para brindar a los usuarios datos relevantes informativos mostrándolos como avisos o alertas o no permitiendo el acceso a acciones del perfil del usuario. Desde otra definición Chowdhury, Adam y Teubnerb (2020) precisan que en la prevención se toman las anticipaciones para salvaguardar los activos cibernéticos de posibles amenazas y vulnerabilidades mediante contramedidas que deben estar bien esclarecidas en los objetivos de las políticas de ciberseguridad.

Respecto a la segunda dimensión de la variable ciberseguridad se tiene la detección que es definida por Shin y Lowry (2020) expone que en la fase de detección se deben identificar oportunamente las amenazas relevantes, el origen de las mismas y sus detalles en términos de estrategias para poder ejecutar las contramedidas que afrontaran el plan y métodos del atacante. En otra perspectiva AlShboul et al. (2018) mencionan que la detección se enfoca en prácticas para que los usuarios usen, comprendan y administren las herramientas de protección tecnologías logrando así un mayor bloqueo durante posibles ataques en la ciberseguridad. En una última definición de la dimensión detección se tiene a Romero et al. (2018) Quienes exponen que la detección es la fase más compleja y es en la que se debe poseer un adecuado nivel de conocimiento técnico que pueda asegurar una eficiente administración de los elementos y actividades de seguridad de la información. Desde otra óptica, Fuchsberger (2005) refiere que la detección se basa en brindar alertas oportunas sobre ataques en una red, utilizando tecnologías de apoyo como lo pueden ser los sistemas de detección de intrusos.

Para definir la tercera dimensión de la variable Ciberseguridad se cita a Basuchoudhary y Searle (2019) quienes indican que en la reacción es cuando ya se ha detectado una amenaza en los sistemas, entonces se debe proceder con bloquear las acciones del usuario en el cual se detectó la anomalía y proceder con ejecutar los métodos de revisión para evitar la propagación de la amenaza, aquí es vital el conocimiento técnico de los responsables de la Ciberseguridad. En otro sentido Meszaros y Buchalcevova (2017) quienes indican que en la fase de reacción se deciden las opciones adecuadas para el tratamiento del riesgo complementado la acción con: la identificación de tareas adecuadas, la priorización de tareas, la ejecución de tareas, la revisión de los resultados y beneficios de las tareas determinadas. Desde otro panorama. Mansfiel (2017) refiere que la fase de reacción o respuesta es uno de esos puntos que tienen que evolucionar y madurar en las organizaciones a medida que lo hace el negocio, se debe dar importancia a las personas y la tecnología para que a través de esta combinación se asegure una respuesta eficaz antes incidentes de ciberseguridad. Finalmente como última definición de la dimensión reacción nombramos a Romero, et al. (2018) quienes indican que en esta fase los protocolos a seguir son severamente distintos a los de la prevención, ya que llegado a esta fase se tienen que adoptar medidas correctivas que mitiguen, corrijan o bloqueen alguna anomalía que se haya presentado cuando ya se ha dado un hecho, más aún si llega a salirse de control podrían de reflejarse en costos muy elevados para la empresa.

Dentro de las definiciones consideradas para la segunda variable Gestión de tecnologías de información Núñez (2011) describe que la gestión de TI es un proceso gerencial que contempla la planificación, la organización, la dirección y el control de las tecnologías de información en las organizaciones, con la finalidad de conseguir lograr las metas planteadas dentro de las empresas y asimismo conseguir una ventaja competitiva respecto de los competidores en mercado. En otra óptica, Huang et al. (2011) mencionan que la gestión de TI se basa en actividades estandarizadas que se deben ejecutar a diario, como lo es el controlar la eficiencia, derivación de responsabilidades y administración de los diferentes servicios de TI, por ello, está enfocado en brindar eficazmente las actividades y productos que son resultado de una

gestión eficiente en los procesos de dichas tecnologías. Desde otro panorama IBM (2020) expone que la gestión de TI se centra en el monitoreo y administración de los elementos comprometidos con las tecnologías informáticas en una organización; es decir que tengan relación directa con el hardware, el software y las redes; en ese sentido la gestión de TI se resume en cómo hacer que los sistemas de información y todos sus elementos funciones de manera eficiente y sumado a ello ayuden a las personas a realizar mejor sus actividades laborales. También está Ramírez et al. (2019) quien define que la gestión de TI trata de un grupo compuesto de conocimientos y responsabilidades que conllevan a crear valor para la gestión de la organización a través del uso de las tecnologías, logrando también la fabricación y administración fundamental en la realización de las actividades, que desemboca en incrementar el grado de competencia de la organización en el mercado. De similar forma Santana et al. (2019) señala que la gestión de TI realiza un papel de gran importancia en las empresas ya que apoyan optimizando las actividades de las diferentes áreas que las constituyen.

Tomando como referencia el concepto de gestión de tecnologías de información por parte de Núñez (2011), las dimensiones serán planificación, dirección y control**:** Para la primera dimensión de planificación nombramos a Solano et al. (2013) quienes mencionan que esta fase se precisa recopilar sistemáticamente los puntos de vital importancia que permitirán cumplir con las metas en el trayecto, eligiendo acertadas decisiones que posteriormente lograrán cumplir con los objetivos futuros; siendo así, en una correcta fase de planear las tecnologías de información se precisa involucrar una correcta guía en las áreas de la organización que conlleven con una continua mejora para así lograr desarrollar beneficios y oportunidades a la empresa. Otra definición lo proporciona Erosa (2009) quién describe que la planificación se centra en un conjunto de estrategias tecnológicas bien formuladas que se deben acoplar convenientemente con los indicadores de la alta directiva, estas estrategias se convertirán en soluciones de tecnologías de información que permitirán grandes cambios, cuando se tenga la solución debe pasar desde la fase de pruebas heurísticas hasta llegar a producción, una vez allí se tendrá que realizar un análisis del impacto

que logro en los usuarios. En otra perspectiva Aponte (2015) describe que la fase de planear corresponde a procedimientos propios de una estrategia, aquí se elaboran las acciones que serán primordiales para cumplir las metas, estás actividades tendrán que estar orientadas a los propósitos de la empresa y poseerán un nivel descriptivo adecuado para que los empleados asignados puedan entender sin problemas las funciones que realizarán; en resumen aquí se elaboran las tácticas de alcance interno y externo que a futuro servirán como socios estratégicos para los objetivos de la entidad y en el cual ningún empleado debe dejar de participar. Como ultima definición de la dimensión planificación Sareian, Shirazi y Motameni (2019) indica que al realizar una adecuada planificación para operar cooperativamente, en general obliga a los agentes involucrados a contribuir con acciones a la construcción del plan. Desde otro plano Martínez et al. (2010) exponen a la planificación como los procedimientos que pertenecen a toda fase administrativa y que se encarga de proyectar desarrollo a las empresas, parte de esta etapa está directamente relacionada con conservar una correspondencia entre las metas y cada recurso de la entidad, asimismo con las ocasiones de mejora que se puedan presentar para la organización.

Para la segunda dimensión de la variable gestión de tecnologías de información, se tiene a la dirección donde Viloria y Casal (2004) describen que se trata de la etapa parcial en el cual se debe guiar adecuadamente al talento humano para que puedan ejecutar efectivamente las acciones establecidas, está función dependerá directamente del líder que este al mando y del perfil de los integrantes a su cargo, ya que de ello dependerá que se realicen correctamente las acciones planteadas para alcanzar las metas organizacionales. En similar sentido Aguilar et al. (2016) Detallan que la dirección es la etapa con se debe considerar como base primordial las habilidades, conocimientos, preparación y experiencia que tiene el líder, ya que él será el encargado de hacer realidad las ambiciones planteadas por la organización que fueron elaboradas previamente, si el líder esta adecuadamente apto y se relaciona exitosamente con los colaboradores de la organización utilizando sus habilidades de dominio de situaciones y dominio de grupos humanos, promoverá una actitud en la que todos se esforzarán lo mejor posible para el bien de la organización. Por el mismo

contexto Mahdi, Nassar y Almsafir (2018) señalan que la etapa de dirección está totalmente centrado en el cumplimiento de objetivos como mejora de procesos, competitividad y claridad en las organizaciones, esta tarea está totalmente centralizada en la responsabilidad de un individuo al que se le encarga esta misión. Por última Briones et al. (2019) definen la dirección como un componente de la administración en el cual se consiguen hacer realidad las actividades planificadas, estas actividades serán tomadas por las riendas del líder, que a través de la toma correcta de decisiones, asignara o delegara funciones a los colaboradores de la empresa participes a su mando o empleados de apoyo, sumado a ello, se debe realizar también un monitoreo adecuado para constatar que se están ejecutando las ordenes realizadas correctamente.

En tercera instancia se tiene la dimensión de control parte de la variable gestión de tecnologías de información donde Vallejos (2013) menciona que el que el control se ejerce por medio del uso de grupo de mediciones que permitan orientar y evaluar posteriormente el comportamiento de una unidad formativa, tiene que ver con la dirección o dominio de una organización o de un sistema; se considera también como un examen u observaciones cuidadosas que sirve para hacer comprobaciones. Desde otra perspectiva Rubio, Blandon y Serna (2019) definen el control como la fase que se centra principalmente en realizar un cotejo de las actividades que se están realizando o se realizaron correctamente, es aquí donde se examinan que los requisitos planteados al inicio se ejecuten de manera inequívoca. El fin primordial del control trata sobre diagnosticar las fallas, encontrar las acciones que se están realizando diferente de lo planeado, anticiparse a imprevistos y subsanar ejecuciones encontradas que se deslindaron de los objetivos. También se tiene la definición de Servín (2018) quien refiere que, la fase de controlar es más que nada un componente para de la administración donde se deben considerar acciones y revisiones técnicas para contrastar que lo elaborado inicialmente concuerde con los trabajos efectuados. En general, todos los encargados o líderes de una organización deben hacerse cargo de un control con calidad y que garantice desarrollo. Desde otro plano Lamine et al. (2020) precisa que, en la fase de control se realiza un seguimiento, comprobando si se han

tomado decisiones sobre alternativas de tratamiento según instrucciones predefinidas, aquí es donde se proporciona una guía para el refinamiento de los modelos o la transición a la fase de implementación.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

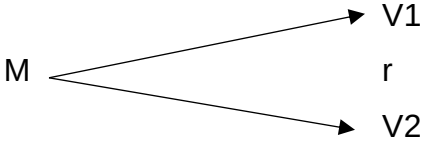
El presente estudio es un tipo de investigación básico, porque se va a agregar o colocar valores a las variables en el cual según Hernández, Fernández y Batista (2014) refieren que en los estudios básicos las variables tienden a relacionarse en torno a una respuesta, así mismo tienen como finalidad describir las cualidades y particularidades de los elementos estudiados a través de un análisis.

Diseño de investigación

El diseño utilizado en el actual estudio investigativo es no experimental, ya que se recolectará información a través de encuestas, con el fin de dar respuesta a una problemática de investigación, además porque existen trabajos de investigación que anteceden al presente. Hernández, Fernández y Batista (2014) describen que el diseño de un estudio alude a la planificación percibida para conseguir la información deseada, además indican que las investigaciones no experimentales son estudios que efectúan sin manipular premeditadamente las variables y se observan analíticamente anormalidades en un ambiente común.

El nivel es correlacional ya que busca establecer la correspondencia respecto a las variables ciberseguridad y gestión de tecnologías de información; Hernández, Fernández y Batista (2014) mencionan las investigaciones correlacionales vinculan las variables a través de patrones previsibles en grupos o poblaciones. También es transversal porque se recolectará información de un lapso de tiempo. Hernández, Fernández y Batista (2014) refieren en cuánto estos modelos de investigación como aquellos que se dan en un instante exacto y exclusivo.

Esquema del diseño de investigación



M: Representa la muestra de la población

V1: Ciberseguridad

V2: Gestión de tecnologías de información

R: Relación entre la variable V1 y V2

3.2. Variables y operacionalización

Variable 1: Ciberseguridad

La variable Ciberseguridad refiera a una variable cualitativa de tipo ordinal.

Definición conceptual de la variable ciberseguridad

Según Fundación Telefónica (2016) la Ciberseguridad es un proceso que implica prevención, detección y reacción, en el cual se debe considerar aprendizaje objetivo que conlleve a la mejora continua inherente del mencionado proceso.

Definición operacional de la variable ciberseguridad

La variable Ciberseguridad se mide a través de las dimensiones: prevención (ítems 1 al 6), detección (ítems 7 al 12) y reacción (ítems 13 al 18); para la escala de medición se emplea la escala de Likert donde: 1 significa Totalmente de acuerdo; 2 es igual a Totalmente en desacuerdo; 3 es igual a Ni de acuerdo ni en desacuerdo; 4 es igual a De acuerdo y 5 es igual a Totalmente de acuerdo.

Tabla 01

Operacionalización de la variable Ciberseguridad.

Dimensiones	Indicadores	Ítems	Escala e índice	Niveles y rango
Prevención	Revisión	1 - 2	Escala de	Alta prevalencia:
	Cambios	3 - 4	Likert	68 - 90
	Mejora	5 - 6	1. Totalmente en	Media
Detección	Revisión	7 - 8	desacuerdo	prevalencia: 43 -
	Cambios	9 - 10	2. En desacuerdo	67
	Mejora	11 - 12	3. Ni de acuerdo ni en	Baja
Reacción	Revisión	13 - 14	desacuerdo	prevalencia: 18 -
	Cambios	15 - 16	4. De acuerdo	42
	Mejora	17 - 18	5. Totalmente de acuerdo	

Fuente: Elaboración propia (2020).

En la tabla 1 se puede contemplar que, los niveles establecidos son: Alta prevalencia en el rango de 68 a 90, Media prevalencia en el rango de 43 a 67 y baja prevalencia en el rango de 18 a 42.

Variable 2: Gestión de tecnologías de información

La variable Gestión de tecnologías de información es una variable cualitativa de tipo ordinal.

Definición conceptual de la variable gestión de tecnologías de información

Según Núñez (2011) refiere que, la gestión de TI es un proceso gerencial que contempla la planificación, la organización, la dirección y el control de las tecnologías de información en las organizaciones, con la finalidad de conseguir lograr las metas planteadas dentro de las empresas y asimismo conseguir una ventaja competitiva respecto de los competidores en mercado

Definición operacional de la variable gestión de tecnologías de información

La variable Gestión de tecnologías de información se mide a través de las dimensiones: planificación (ítems 19 al 24), dirección (ítems 25 al 30) y control (ítems 31 al 36); para la escala de medición se emplea la escala de Likert donde: 1 significa Totalmente de acuerdo; 2 es igual a Totalmente en desacuerdo; 3 es igual a Ni de acuerdo ni en desacuerdo; 4 es igual a De acuerdo y 5 Totalmente de acuerdo.

Tabla 02

Operacionalización de la variable gestión de tecnologías de información.

Dimensiones	Indicadores	Ítems	Escala e índice	Niveles y rango
Planificación	Alcance	19 - 20	Escala de	No optimo: 18 -
	Conocimiento	21 - 22	Likert	42
	Seguridad	23 - 24	1. Totalmente en	Regular: 43 - 67
Dirección	Alcance	25 - 26	desacuerdo	Optimo: 68 - 90
	Conocimiento	27 - 28	2. En desacuerdo	
	Seguridad	29 - 30	3. Ni de acuerdo	
Control	Alcance	31 - 32	ni en desacuerdo	
	Conocimiento	33 - 34	4. De acuerdo	
	Seguridad	35 - 36	5. Totalmente de	
			acuerdo	

Fuente: Elaboración propia (2020).

En la tabla 2 se puede contemplar que, los niveles establecidos son: Optimo en el rango de 68 a 90, Regular en el rango de 43 a 67 y No optimo en el rango de 18 a 42.

3.3. Población, muestra y muestreo

Población

En la actual investigación se estableció como población a los trabajadores de la empresa I & T Electric en el año 2020, con un total de 87 trabajadores de todas las áreas de la empresa que usan un dispositivo tecnológico para sus funciones, hombres y mujeres, sin distinción de edad. Hernández Fernández y Bautista (2014) señalan que, la población son todos los fenómenos a estudiar, en el cual cada elemento tiene una cualidad similar a las demás, por ende se analizan y dan inicio al dato de exploración"

Tabla 03

Población identificada por sexo, según el centro de actividad.

Centro de Actividad	Hombres	Mujeres	Total
Almacén	5	2	7
Calidad	4	1	5
Comercial	4	3	7
Compras	2	0	2
Contabilidad	5	3	8
Facturación	0	1	1
Gerencia	2	2	4
Ingeniería	7	4	11
Logística	4	2	6
Mantenimiento	2	2	4
Marketing	1	2	3
Mensajería	1	0	1
Producción	5	2	7
Psicología	1	1	2
RRHH	1	4	5
Secretaria	0	1	1
Seguridad	3	0	3
SST	1	2	3
Tesorería	0	4	4
TI	3	0	3
Total	51	36	87

Fuente: Área administrativa de I & T Electric (2020).

En la tabla 3 se puede contemplar que, los hombres constituyen la mayor cantidad de la población con 51 integrantes mientras que mujer solo tiene 36 individuos.

Muestra

Está comprendida por todos los trabajadores de la empresa I & T Electric, sin distinción de género, tipo de cargo o edad; pero si seleccionando como criterio de inclusión a aquellos que usan algún dispositivo tecnológico otorgado por la empresa para sus funciones. La muestra, según Sánchez et al. (2018) trata de un grupo de elementos que fueron escogidos del universo total.

Tamaño de la Muestra

Para determinar el volumen de la muestra se empleó la herramienta tecnológica de software Decisión Analyst STATS Versión 2.0.0.2.; en el cual se inscribieron los valores solicitados por el programa informático con el fin de calcular la muestra. M = 71

Muestreo

Para el presente estudio se aplicó el muestreo no probabilístico aleatorio simple. Bernal (2010) expone que el muestreo es una de las herramientas de la investigación científica, el cual tiene como función establecer en qué lugar de la población se debe examinar, donde pueden ser probabilístico o no probabilístico. Así mismo Hernández Fernández y Bautista (2014) refieren los muestreos no probabilísticos filtran elementos de acuerdo a uno o muchos fines y no intentan que las casuísticas se reflejen estadísticamente representativa al universo total de estudio.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

La técnica que se empleo fue la encuesta, porque ya que brinda la posibilidad de recopilar precisa para luego ser analizada y procesada. Hernández Fernández y Bautista (2014) indican que la recolección de datos puede involucrar distintos

conjuntos, elementos o indicadores; también distintas congregaciones, condiciones o hitos.

Instrumentos de recolección de datos

En la recolección de información de las variables estudiadas descritas en los acápites anteriores, se optó por un cuestionario. Hernández Fernández y Bautista (2014) describen que los cuestionarios se centran en interrogantes abiertas o cerradas y su entorno de ejecución puede darse a través de una reunión, telefónicamente o vía remoto utilizando una herramienta tecnológica.

Tabla 04

Ficha técnica del instrumento de medición.

Nombre del instrumento	Encuesta de la empresa I & T Electric SAC
Autor	Alberto Ismael Bohorquez Salcedo
Año	2020
Tipo de instrumento	Encuesta
Objetivo	Determinar la relación de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020
Población	Empleados de la empresa I & T Electric que usan un dispositivo tecnológico para sus funciones
Número de ítems	36
Tiempo de aplicación	10 Minutos
Normas de aplicación	El encuestado una opción por cada ítem respecto a la pregunta que se presenta según su criterio.
Escala	Totalmente en desacuerdo En desacuerdo Ni de acuerdo ni en desacuerdo De acuerdo Totalmente de acuerdo
Niveles y rangos de la variable Ciberseguridad	Alta prevalencia (68 - 90) Media prevalencia (43 - 67) Baja prevalencia (18 - 42)
Niveles y rangos de la variable Gestión de tecnologías de información	Optimo (68 - 90) Regular (43 - 67) No optimo (18 - 42)

Fuente: Elaboración propia (2020).

En la tabla 4 se puede contemplar la ficha técnica del instrumento de medición empleado en el presente estudio investigativo.

Validez

Para dar veracidad al instrumento recolector de datos del actual estudio se efectuó el dictamen a través de profesionales calificados, bajo la descripción de validación de expertos. La validación de juicio de expertos es un conjunto de revisiones detalladas que brinda cada experto al instrumento recolector de información aplicado al actual estudio investigativo, obteniendo así en caso de presentarse las observaciones y en caso de no presentarse alguna observación, obteniendo el visto bueno de cada experto que reconoce como aplicable al instrumento, por ende, los mencionados expertos certificaron la precisión, congruencia e importancia de los ítem perteneciente a cada dimensión de las variables estudiadas.

Tabla 05

Validación de expertos.

Nombres y apellidos	Grado	Institución donde labora	Tipo	Calificación
Eduardo Humberto Poletti Gaitan	Magister	Universidad Cesar Vallejo	Temático	Aplicable
Juan Brues Chumpe Agesto	Doctor	Universidad Cesar Vallejo	Temático	Aplicable
Pedro Martin Lezama Gonzales	Doctor	Universidad Cesar Vallejo	Metodólogo	Aplicable

Fuente: Área administrativa de I & T Electric (2020).

En la tabla 5 se puede contemplar que, los especialistas califican el instrumento de recolección de datos aplicable para el presente estudio de investigación.

Confiabilidad

Luego de haber validado la herramienta recolectora de datos mediante la validación de especialistas, se prosiguió con disponer la confiabilidad del mismo, en tal sentido Hernández Fernández y Bautista (2014) determinan que la confiabilidad de una herramienta evaluadora describe el nivel en que la empleabilidad repetida del mismo, obtiene como resultantes valores similares. Para medir la confiabilidad se utilizó el coeficiente de confiabilidad de Alfa de Cronbach, en primera instancia se utilizó una

muestra piloto de 35 individuos y posteriormente se utilizó la muestra del estudio con un total de 71 individuos; Para la estadística se usó el software SPPS v25.

Tabla 06

Confiabilidad del instrumento

Tipo de aplicación	Alfa de cronbach	Número de encuestas	N° de elementos
Piloto	0,901	35	36
General	0,906	71	36

Fuente: Elaboración propia mediante el SPSS v25 (2020).

1 0 a 0.02 => Muy malo

2 0.2 a 0.4 => Malo

3 0.4 a 0.6 => Regular

4 0.6 a 0.8 => Bueno

5 0.8 a 1 => Muy bueno

Como se puede apreciar en la Tabla 6, el valor obtenido de la prueba piloto fue 0,901 y el valor obtenido de la muestra general fue 0,906; con lo cual se puede determinar que la fiabilidad es muy buena, es decir es satisfactoria para el trabajo de investigación.

3.5. Procedimientos

Para poder obtener los resultados estadísticos, se procedió en primera instancia con diseñar la herramienta definida como instrumento recolectora de información, luego se prosiguió con buscar a los expertos relevantes en la temática y metodología para que aprueben como aplicable la mencionada herramienta, ya teniendo la herramienta validada, se procedió con efectuar una toma de datos piloto, realizando la encuesta a un total de 35 individuos, con esas encuestas se prosiguió a un vaciado de datos utilizando el programa Microsoft Excel y se obtuvo la base de datos piloto; luego se realizó el examen de confiabilidad utilizando el estadístico de Alfa de Cronbach. Luego se procedió con al análisis descriptivo, siguiendo la prueba inferencia donde se realizó la constatación de hipótesis.

3.6. Método de análisis de datos

En el análisis de datos se procede con detallar la condición real, para lo cual, se cargaron y tabularon los datos obtenidos a través de las encuestas, posterior se usó el programa informático IBM SPSS Statics v25, consiguiendo como resultado la base de datos del proyecto.

En la realización del análisis descriptivo, se empleó tablas de contingencia para un análisis bidimensional e histogramas con el fin de explicar los valores obtenidos de la muestra.

Al emplear el análisis inferencial se empleó métodos no paramétricos y se aplicó el coeficiente de correlación de Rho Spearman el cual posibilita decretar el nivel de correlación entre las variables, sobre ello Prion y Haerling (2014) refieren que en la "regla empírica" para interpretar Rho de Spearman, se determinan los resultados de la siguiente manera: De 0 a 0,20 es insignificante, de 0,21 a 0.40 es débil, de 0.41 a 0.60 es moderado, de 0.61 a 0,80 es fuerte y de 0,81 a 1,00 se considera muy fuerte.

3.7. Aspectos éticos

En el actual estudio investigativo se expone información de la empresa I & T Electric, que fue brindada con la finalidad de buscar una obtener un análisis informático de la ciberseguridad que les ayude a mejorar la gestión de las tecnologías de información. Por lo cual la empresa brindo los permisos necesarios para la realización del estudio y de haber algún fin no adecuado será censurado por la organización en alusión.

IV. RESULTADOS

Análisis descriptivo

Análisis descriptivo de la variable ciberseguridad y la variable gestión de tecnologías de información

Tabla 07

*Tabla de contingencia ciberseguridad * gestión de tecnologías de información.*

		V2 - Gestión de tecnologías de información			Total
		No optimo	Regular	Optimo	
V1- Ciberseguridad	Baja prevalencia	5 (7,0%)	0 (0,0%)	0 (0,0%)	5 (7,0%)
	Media prevalencia	0 (0,0%)	50 (70,4%)	6 (8,5%)	56 (78,9%)
	Alta prevalencia	0 (0,0%)	0 (0,0%)	10 (14,1%)	10 (14,1%)
	Total	5 (7,0%)	50 (70,4%)	16 (22,5%)	71 (100,0%)

Fuente: Elaboración propia (2020).

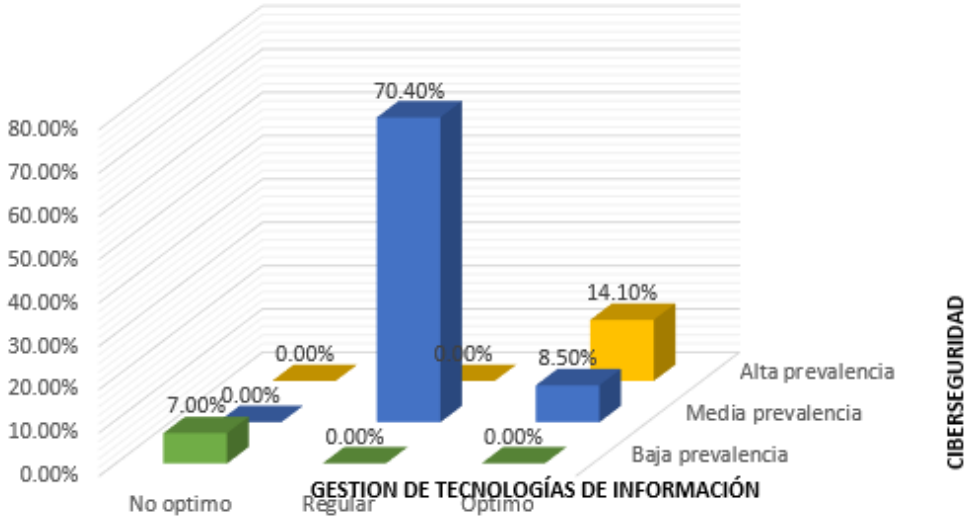


Figura 01: Histograma, *ciberseguridad * gestión de tecnologías de información. Elaboración propia*

Como se logra visualizar en la tabla 7, el índice de más frecuencia de aprobación se presenta en la intersección del nivel media prevalencia de la variable ciberseguridad y el nivel regular de la variable gestión de tecnologías de información, acumulando 50

contestaciones que representan el 70,4% de la totalidad y en el índice de menos frecuencia de aprobación, se muestran en cuatro situaciones, una de ellas en la intersección del nivel alta prevalencia de la variable ciberseguridad y el nivel no óptimo de la variable gestión de tecnologías de información, con 0 contestaciones que representan el 0,0% de la totalidad.

En la Figura 01 se logra visualizar que el nivel regular representa al máximo índice de frecuencia, reuniendo 50 contestaciones (70.4%) para esta inclinación.

Análisis descriptivo de la dimensión prevención de la variable ciberseguridad y la variable gestión de tecnologías de información

Tabla 08

*Tabla de contingencia dimensión prevención de la ciberseguridad * gestión de tecnologías de información.*

		V2 - gestión de tecnologías de información			Total
		No optimo	Regular	Optimo	
D1-Prevención	Baja prevalencia	5 (7,0%)	14 (19,7%)	1 (1,4%)	20 (28,2%)
	Media prevalencia	0 (0,0%)	36 (50,7%)	14 (19,7%)	50 (70,4%)
	Alta prevalencia	0 (0,0%)	0 (0,0%)	1 (1,4%)	1 (1,4%)
	Total	5 (7,0%)	50 (70,4%)	16 (22,5%)	71 (100,0%)

Fuente: Elaboración propia (2020).

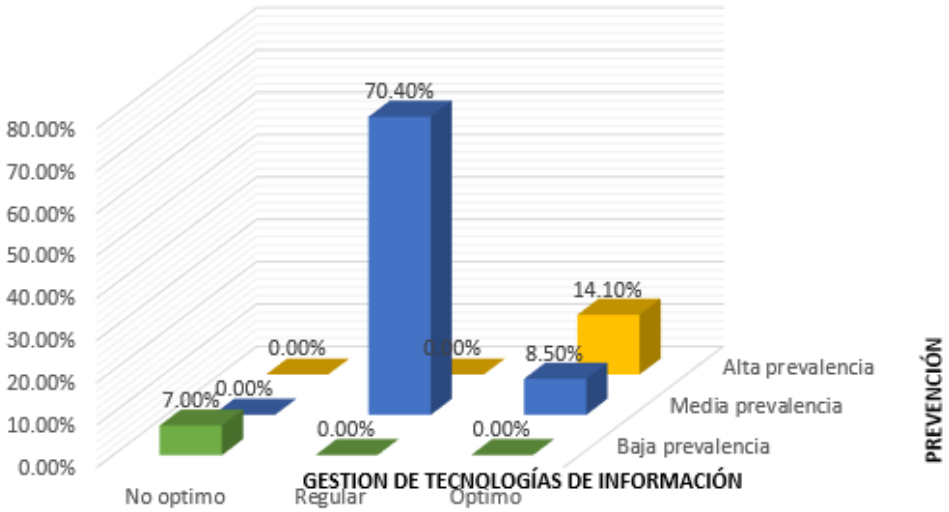


Figura 02: Histograma, dimensión prevención de la variable c*iberseguridad * gestión de tecnologías de información. Elaboración propia.*

Como se logra visualizar en la Tabla 8, el índice de más frecuencia de aprobación se presenta en la intersección del nivel media prevalencia de la dimensión prevención de la variable ciberseguridad y el nivel regular de la variable gestión de tecnologías de información, con 36 contestaciones que representan el 50,7% de la totalidad y en el índice de menos frecuencia de aprobación, se muestran en cuatro situaciones, una de ellas en la intersección del nivel alta prevalencia de la dimensión prevención de la variable ciberseguridad y el nivel no óptimo de la variable gestión de tecnologías de información, con 0 contestaciones que representan el 0,0% de la totalidad.
En la figura 02 se logra visualizar que el nivel media prevalencia representa al máximo índice de frecuencia, reuniendo 50 contestaciones (70.4%) para esta inclinación.

Análisis descriptivo de la dimensión detección de la variable ciberseguridad y la variable gestión de tecnologías de información

Tabla 09

*Tabla de contingencia dimensión detección de la ciberseguridad * gestión de tecnologías de información.*

		V2 - Gestión de tecnologías de información			Total
		No optimo	Regular	Optimo	
D1-Detección	Baja prevalencia	2 (2,8%)	1 (1,4%)	0 (0,0%)	3 (4,2%)
	Media prevalencia	3 (4,2%)	48 (67,6%)	9 (12,7%)	60 (84,5%)
	Alta prevalencia	0 (0,0%)	1 (1,4%)	7 (9,9%)	8 (11,3%)
	Total	5 (7,0%)	50 (70,4%)	16 (22,5%)	71 (100,0%)

Fuente: Elaboración propia (2020).

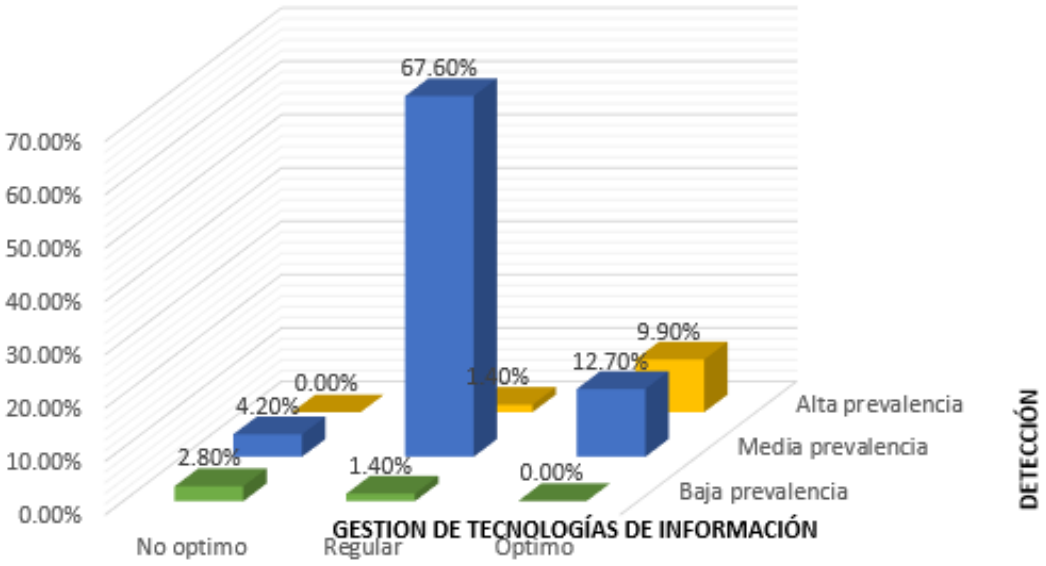


Figura 03: Histograma, dimensión detección de la variable *ciberseguridad* * *gestión de tecnologías de información. Elaboración propia.*

Como se logra visualizar en la Tabla 9, el índice de más frecuencia de aprobación se presenta en la intersección del nivel media prevalencia de la dimensión detección de la variable ciberseguridad y el nivel regular de la variable gestión de tecnologías de información, acumulando 48 contestaciones que representan el 67,6% de la totalidad y en el índice de menos frecuencia de aprobación, se muestran en cuatro situaciones, una de ellas en la intersección del nivel alta prevalencia de la dimensión detección de la variable ciberseguridad y el nivel no óptimo de la variable gestión de tecnologías de información, con 0 contestaciones que representan el 0,0% de la totalidad.

En la figura 03 se logra visualizar que el nivel media prevalencia representa al máximo índice de frecuencia, reuniendo 50 contestaciones (70.4%) para esta inclinación.

Análisis descriptivo de la dimensión reacción de la variable ciberseguridad y la variable gestión de tecnologías de información

Tabla 10

*Tabla de contingencia dimensión reacción de la ciberseguridad * gestión de tecnologías de información.*

		V2 - Gestión de tecnologías de información			Total
		No optimo	Regular	Optimo	
D1-Reacción	Baja prevalencia	4 (5,6%)	1 (1,4%)	0 (0,0%)	5 (7,0%)
	Media prevalencia	1 (1,4%)	49 (69,0%)	9 (12,7%)	59 (83,1%)
	Alta prevalencia	0 (0,0%)	0 (0,0%)	7 (9,9%)	7 (9,9%)
	Total	5 (7,0%)	50 (70,4%)	16 (22,5%)	71 (100,0%)

Fuente: Elaboración propia (2020).

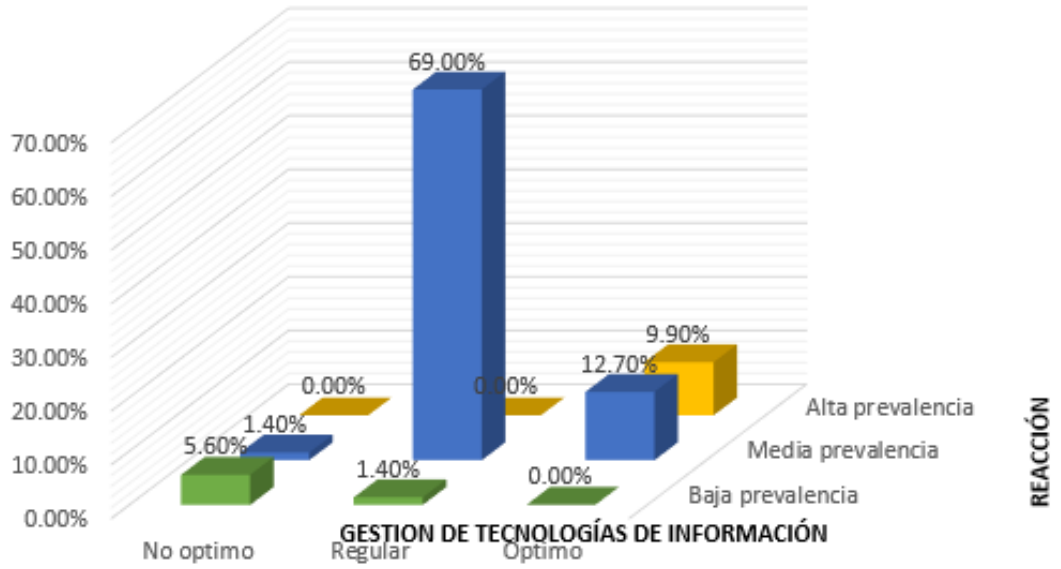


Figura 04: Histograma, dimensión reacción de la variable *ciberseguridad * gestión de tecnologías de información. Elaboración propia.*

Como se logra visualizar en la tabla 10, el índice de más frecuencia de aprobación se presenta en la intersección del nivel media prevalencia de la dimensión reacción de la variable ciberseguridad y el nivel regular de la variable gestión de tecnologías de información, acumulando 49 contestaciones que representan el 69,0% de la totalidad

y en el índice de menos frecuencia de aprobación, se muestran en cuatro situaciones, una de ellas en la intersección del nivel alta prevalencia de la dimensión reacción de la variable ciberseguridad y el nivel no óptimo de la variable gestión de tecnologías de información, con 0 contestaciones que representan el 0,0% de la totalidad. En la figura 02 se logra visualizar que el nivel media prevalencia representa al máximo índice de frecuencia, reuniendo 50 contestaciones (70.4%) para esta inclinación.

Análisis inferencial

Formulación de hipótesis

Hipótesis general

H_1: Existe relación significativa de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

H_0: No existe relación significativa de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Tabla 11

Matriz de correlación de la variable ciberseguridad y la variable gestión de tecnologías de información.

			V1 - Ciberseguridad	V2 - Gestión de TI
Rho de Spearman	V1 - Ciberseguridad	Coeficiente de correlación	1,000	0,832**
		Sig. (bilateral)		0,000
		N	71	71
	V2 - Gestión de TI	Coeficiente de correlación	0,832	1,000
		Sig. (bilateral)	0,000	
		N	71	71

** La correlación es significativa al nivel 0,05 (bilateral)

Fuente: Elaboración propia (2020).

Contrastación de hipótesis estadística:

Se puede contemplar en la tabla 11, que el resultante del coeficiente de correlación Rho de Spearman equivale a 0,832 evidenciándose una correlación muy fuerte; Así mismo debido a que el Sig. es igual a 0,00 y es menor a 0,05 indicando que la relación entre las variables es estadísticamente significativa. Por lo anteriormente expuesto se rechaza la hipótesis nula (Ho) aceptando la hipótesis alterna (H1) con un 95% de confianza, entonces, se determina que existe relación significativa de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Formulación de hipótesis

Hipótesis específica 1

H_1: Existe relación significativa entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

H_0: No existe relación significativa entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Tabla 12

Matriz de correlación de la dimensión prevención de la variable ciberseguridad y la variable gestión de tecnologías de información.

			V1 - Ciberseguridad	V2 - Gestión de TI
Rho de Spearman	D1 - Prevención	Coeficiente de correlación	1,000	0,432**
		Sig. (bilateral)		0,000
		N	71	71
	V2 - Gestión de TI	Coeficiente de correlación	0,432	1,000
		Sig. (bilateral)	0,000	
		N	71	71

** La correlación es significativa al nivel 0,05 (bilateral)

Fuente: Elaboración propia (2020).

Contrastación de hipótesis estadística:

Se puede contemplar en la Tabla 12 que el resultante del coeficiente de correlación Rho de Spearman equivale a 0,432 evidenciándose una correlación moderada; Así mismo debido a que el Sig. es igual a 0,00 y es menor a 0,05 indicando que la relación entre las variables es estadísticamente significativa. Por lo anteriormente expuesto se rechaza la hipótesis nula (Ho) aceptando la hipótesis alterna (H1) con un 95% de confianza, entonces, se determina que existe relación significativa entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Formulación de hipótesis

Hipótesis específica 2

H_1: Existe relación significativa entre la dimensión detección de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

H_0: No existe relación significativa entre la dimensión detección de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Tabla 13

Matriz de correlación de la dimensión detención de la variable ciberseguridad y la variable gestión de tecnologías de información.

			V1 - Ciberseguridad	V2 - Gestión de TI
Rho de Spearman	D1 - Detención	Coeficiente de correlación	1,000	0,575**
		Sig. (bilateral)		0,000
		N	71	71
	V2 - Gestión de TI	Coeficiente de correlación	0,575	1,000
		Sig. (bilateral)	0,000	
		N	71	71

** La correlación es significativa al nivel 0,05 (bilateral)

Fuente: Elaboración propia (2020).

Contrastación de hipótesis estadística:

Se puede contemplar en la Tabla 13 que el resultante del coeficiente de correlación Rho de Spearman equivale a 0,575 evidenciándose una correlación moderada; Así mismo debido a que el Sig. es igual a 0,00 y es menor a 0,05 indicando que la relación entre las variables es estadísticamente significativa. Por lo anteriormente expuesto se rechaza la hipótesis nula (Ho) aceptando la hipótesis alterna (H1) con un 95% de confianza, entonces, se determina que existe relación significativa entre la dimensión detección de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Formulación de hipótesis

Hipótesis específica 3

H_1: Existe relación significativa entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

H_0: No existe relación significativa entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

Tabla 14

Matriz de correlación de la dimensión reacción de la variable ciberseguridad y la variable gestión de tecnologías de información.

			V1 - Ciberseguridad	V2 - Gestión de TI
Rho de Spearman	D1 - Reacción	Coeficiente de correlación	1,000	0,692**
		Sig. (bilateral)		0,000
		N	71	71
	V2 - Gestión de TI	Coeficiente de correlación	0,692	1,000
		Sig. (bilateral)	0,000	
		N	71	71

** La correlación es significativa al nivel 0,05 (bilateral)

Fuente: Elaboración propia (2020).

Contrastación de hipótesis estadística:

Se puede contemplar en la Tabla 14 que el resultante del coeficiente de correlación Rho de Spearman equivale a 0,692 evidenciándose una correlación fuerte; Así mismo debido a que el Sig. es igual a 0,00 y es menor a 0,05 indicando que la relación entre las variables es estadísticamente significativa. Por lo anteriormente expuesto se rechaza la hipótesis nula (Ho) aceptando la hipótesis alterna (H1) con un 95% de confianza, entonces, se determina que existe relación significativa entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

V. DISCUSIÓN

Respecto a la relación de la variable ciberseguridad con la variable gestión de tecnologías de información la evidencia empírica encontrada en el presente estudio de investigación muestra en referencia al análisis descriptivo realizado a los datos que el nivel de media prevalencia de la ciberseguridad está asociado con el nivel regular de la gestión de tecnologías de información, siendo este porcentaje 70,4%; mientras el nivel de alta prevalencia de ciberseguridad se relaciona con el nivel óptimo de la gestión de tecnologías de información con un 14,1%; asimismo el nivel de media prevalencia de la ciberseguridad se logra asociar al nivel óptimo de la gestión de tecnologías de información, siendo este porcentaje 8,5%. Respecto al aspecto inferencial se logró evidenciar una clara correlación existente, en el cual el coeficiente Rho de Spearman resulto equivalente a 0,832 evidenciándose una correlación muy fuerte ya que está dentro del rango de 0,81 a 1,00. Así mismo la significancia es igual a 0,00 y es menor a 0,05 indicando que la relación entre las variables es estadísticamente significativa. Este análisis permite llegar a la determinación de que la ciberseguridad se relaciona significativamente con la gestión de tecnologías de información a un nivel muy fuerte; los resultados encontrados se asemejan en gran similitud a los que logro evidenciar Sánchez (2017), el cual luego de finiquitar su estudio investigativo concluyó que al adoptar estrategias de ciberseguridad incide significativamente en la protección de la información en la oficina de economía del ejército, así mismo concuerda con la investigación de Marcos (2018), quien en su investigación logro evidenciar la importancia de la ciberseguridad en los votos electrónicos remotos, partiendo como base principal la transparencia de estos eventos políticos y de la envergadura del mismo. Respuestas brindadas en margen de la definición de ciberseguridad en el cual Sabillon (2018) definió la ciberseguridad como el salvaguardo de los activos informáticos ya que se da puntualidad a los agentes que amenazan la información tratada, almacenada en las bases de datos y que se comparte usando los sistemas a través de las redes con diferentes fines. De acuerdo a los resultados encontrados en la presente investigación, la aplicación de conocimientos profesionales de ciberseguridad en la empresa I & T Electric requiere que la gerencia brinde la importancia necesaria para que el personal designado y

responsables puedan capacitarse adecuadamente con el fin de lograr afrontar con eficiencia las exigencias de la ciberseguridad que demandan las ciberamenazas a las empresas.

Respecto a la relación de la dimensión prevención de la variable ciberseguridad con la variable gestión de tecnologías de información la evidencia empírica encontrada en el presente estudio de investigación muestra en referencia al análisis descriptivo realizado a los datos que el nivel de media prevalencia de la dimensión prevención de la ciberseguridad se logra asociar al nivel regular de la gestión de tecnologías de información, siendo este porcentaje 50,7%; mientras el nivel de media prevalencia de la dimensión prevención de la ciberseguridad se relaciona con el nivel óptimo de la gestión de tecnologías de información con un 19,7%; asimismo el nivel de media prevalencia de la dimensión prevención de la ciberseguridad está asociado con el nivel regular de la gestión de tecnologías de información, siendo este porcentaje 19,7%. Respecto al aspecto inferencial se logró evidenciar una clara correlación existente, en el cual el coeficiente Rho de Spearman resulto equivalente a 0,432 evidenciándose una correlación moderada ya que está dentro del rango de 0,41 a 0,60. Así mismo la significancia es igual a 0,00 y es menor a 0,05 indicando que la relación entre la dimensión prevención de la variable ciberseguridad y la variable gestión de tecnologías de información es estadísticamente significativa. Este análisis permite llegar a la determinación de que la dimensión prevención de la ciberseguridad se relaciona significativamente con la gestión de tecnologías de información a un nivel moderado; los resultados encontrados se asemejan en gran similitud a los que evidenciaron Inoguchi y Macha (2017), quienes en su investigación concluyeron que la ciberseguridad que se administra en las empresas para la protección de los activos informáticos debe ser prioridad de la gerencia general, compromiso que también debe ser compartido con todos los colaboradores sin importar la jerarquía; asimismo se debe elaborar un plan formal con todas las actividades que se ejecutaran, así mismo concuerda con la investigación de Huerta (2019), quien en su investigación logro constatar que este incide significante y favorablemente en el proceso de la gestión de riesgo en una consultora. Respuestas brindadas en margen de la definición de la

dimensión prevención de la ciberseguridad en el cual Meyer, Dembinsky y Raviv (2020), exponen que la prevención trata de la anticipación ante las amenazas en los sistemas informáticos e implica el uso de algoritmos que analizan eventos y asignan un valor a cada evento, conforme a este análisis. Los valores resultantes pueden ser usados para brindar a los usuarios datos relevantes informativos mostrándolos como avisos o alertas o no permitiendo el acceso a acciones del perfil del usuario. De acuerdo a los resultados encontrados en la presente investigación, se debe incrementar el nivel del conocimiento y aplicación de la prevención de amenazas de la ciberseguridad para desarrollar el uso seguro de las tecnologías de información en la empresa I & T.

Respecto a la relación de la dimensión detección de la variable ciberseguridad con la variable gestión de tecnologías de información la evidencia empírica encontrada en el presente estudio de investigación muestra en referencia al análisis descriptivo realizado a los datos que el nivel de media prevalencia de la dimensión detección de la ciberseguridad se logra asociar al nivel regular de la gestión de tecnologías de información, siendo este porcentaje 67,6%; mientras el nivel de media prevalencia de la dimensión detección de la ciberseguridad se relaciona con el nivel óptimo de la gestión de tecnologías de información con un 12,7%; asimismo el nivel de alta prevalencia de la dimensión detección de la ciberseguridad está asociado con el nivel no óptimo de la gestión de tecnologías de información, siendo este porcentaje 9,9%. Respecto al aspecto inferencial se logró evidenciar una clara correlación existente, en el cual el coeficiente Rho de Spearman resulto equivalente a 0.575 evidenciándose una correlación moderada ya que está dentro del rango de 0,41 a 0,60. Así mismo la significancia es igual a 0,00 y es menor a 0,05 indicando que la relación entre la dimensión prevención de la variable ciberseguridad y la variable gestión de tecnologías de información es estadísticamente significativa. Este análisis permite llegar a la determinación de que la dimensión detección de la ciberseguridad se relaciona significativamente con la gestión de tecnologías de información a un nivel moderado; los resultados encontrados se asemejan en gran similitud a los que logro evidenciar Huayllani (2020), el cual luego de finiquitar su estudio investigativo concluyó que el

sistema de gestión de Seguridad de la Información se relaciona con la gestión del Riesgo del Ministerio de Salud para el año 2019, analizado en la unidad de gestión de inversión de reconstrucción con cambios, así mismo concuerda con la investigación de Garbarino (2014), quien en su investigación concluyeron que los sistemas informáticos son agentes estratégicos esenciales para el cumplimiento de metas en las organizaciones, más aún cuando los sistemas informáticos están enfocados a los objetivos de la organización. Respuestas brindadas en margen de la definición de la dimensión detección de la ciberseguridad en el cual Romero et al. (2018) exponen que la detección es la fase más compleja y es en la que se debe poseer un adecuado nivel de conocimiento técnico que pueda asegurar una eficiente administración de los elementos y actividades de seguridad de la información. De acuerdo a los resultados encontrados en la presente investigación, se debe incrementar el nivel del conocimiento y aplicación de la detección de amenazas de la ciberseguridad para desarrollar el uso seguro de las tecnologías de información en la empresa I & T Electric.

Respecto a la relación de la dimensión reacción de la variable ciberseguridad con la variable gestión de tecnologías de información la evidencia empírica encontrada en el presente estudio de investigación muestra en referencia al análisis descriptivo realizado a los datos que el nivel de media prevalencia de la dimensión detección de la ciberseguridad se logra asociar al nivel regular de la gestión de tecnologías de información, siendo este porcentaje 69,0%; mientras el nivel de media prevalencia de la dimensión detección de la ciberseguridad se relaciona con el nivel óptimo de la gestión de tecnologías de información con un 12,7%; asimismo el nivel de alta prevalencia de la dimensión detección de la ciberseguridad se logra asociar al nivel no óptimo de la gestión de tecnologías de información, siendo este porcentaje 9,9%. Respecto al aspecto inferencial se logró evidenciar una clara correlación existente, en el cual el coeficiente Rho de Spearman resulto equivalente a 0.692 evidenciándose una correlación fuerte ya que está dentro del rango de 0,61 a 0,80. Así mismo la significancia es igual a 0,00 y es menor a 0,05 indicando que la relación entre la dimensión reacción de la variable ciberseguridad y la variable

gestión de tecnologías de información es estadísticamente significativa. Este análisis permite llegar a la determinación que la dimensión reacción de la ciberseguridad se relaciona significativamente con la gestión de tecnologías de información a un nivel fuerte; los resultados encontrados se asemejan en gran similitud a los que evidenciaron Arias y Celis (2015), quien al finalizar su investigación concluyó que logra evidenciar que el uso de un modelo internacional de ciberseguridad es viable para la protección de la información en las organizaciones, así mismo concuerda con la investigación de Landázuri (2019), quien en su investigación diseño de un modelo de gobernabilidad y gestión de tecnologías de Información para el área de desarrollo de proyectos de software de corporación favorita, basado en la metodología Devops logro evidenciar que el modelo de gobierno de tecnologías de información desarrollado comprende el conjunto de cada proceso y el detalle de cada iteración. Por cada proceso se realizó una matriz de caracterización donde se explican los objetivos, actores, entradas, salidas, modo de recolección de la información y forma de medición. Respuestas brindadas en margen de la definición de la dimensión reacción de la ciberseguridad en el cual Basuchoudhary y Searle (2019) indican que en la reacción es cuando ya se ha detectado una amenaza en los sistemas, entonces se debe proceder con bloquear las acciones del usuario en el cual se detectó la anomalía y proceder con ejecutar los métodos de revisión para evitar la propagación de la amenaza, aquí es vital el conocimiento técnico de los responsables de la ciberseguridad. De acuerdo a los resultados encontrados en la presente investigación, se debe incrementar el nivel del conocimiento y aplicación de la reacción de amenazas de la ciberseguridad para desarrollar el uso seguro de las tecnologías de información en la empresa I & T Electric.

Respecto a la metodología

La metodología empleada en el presente estudio investigativo ha permitido evidenciar positivamente las bondades de los tipos de estudios básicos en el cual

deja resultados valiosos para futuras investigaciones que pueden tomar como referencia los obtenidos para llegar a plantear investigaciones de envergaduras más trascendentales y ambiciosas. En otro sentido la metodología utilizada en el presente trabajo de investigación permite con respecto a la ejecución del cuestionario, evidenciar una de las debilidades de este tipo de estudios siempre, como lo es el estar expuesto o sujetos al estado de ánimo de los encuestados, pero ello es parte evidente del método científico investigativo.

VI. CONCLUSIONES

Primero La Ciberseguridad se relaciona significativamente con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020, donde el coeficiente Rho de Spearman es igual a 0.832 evidenciándose una correlación de nivel muy fuerte.

Segundo La dimensión prevención de la variable Ciberseguridad se relaciona significativamente con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020, donde el coeficiente Rho de Spearman es igual a 0.432 evidenciándose una correlación de nivel moderada.

Tercero La dimensión detección de la variable Ciberseguridad se relaciona significativamente con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020, donde el coeficiente Rho de Spearman es igual a 0.575 evidenciándose una correlación de nivel moderada.

Cuarto La dimensión reacción de la variable Ciberseguridad se relaciona significativamente con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020, donde el coeficiente Rho de Spearman es igual a 0.692 evidenciándose una correlación de nivel fuerte.

VII. RECOMENDACIONES

Primero Para mantener elevado el nivel fuerte de la relación de la Ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric S.A.C. del distrito de Los Olivos, se recomienda al Gerente General realizar un programa de capacitación anual para brindar a su personal profesional de tecnologías de información y así mismo realizar capacitaciones internas por parte del área de tecnologías de información al personal de todas las áreas; dichas capacitaciones deben ser programadas y brindadas estratégicamente con el fin de mantener y obtener resultados favorables.

Segundo Para elevar el nivel moderado de la relación de la dimensión prevención de la Ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric S.A.C. del distrito de Los Olivos, se recomienda al Gerente Administrativo y al Jefe de tecnologías de información realizar un programa de capacitación anual para brindar al personal de todas las áreas de la empresa involucrados en el flujo del negocio; dichas capacitaciones deben ser programadas y brindadas estratégicamente con el fin de mantener y obtener resultados favorables.

Tercero Para elevar el nivel moderado de la relación de la dimensión reacción de la Ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric S.A.C. del distrito de Los Olivos, se recomienda al Gerente Administrativo y al Jefe de tecnologías de información realizar un programa de capacitación anual para brindar al personal de todas las áreas de la empresa involucrados en el flujo del negocio; dichas capacitaciones deben ser programadas y brindadas estratégicamente con el fin de mantener y obtener resultados favorables.

Cuarto Para elevar el nivel moderado de la relación de la dimensión reacción de la Ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric S.A.C. del distrito de Los Olivos, se recomienda al Gerente Administrativo y al Jefe de tecnologías de información realizar un programa de capacitación anual para brindar al personal de todas las áreas de la empresa involucrados en el flujo del negocio; dichas capacitaciones deben ser programadas y brindadas estratégicamente con el fin de mantener y obtener resultados favorables.

REFERENCIAS

Aguilar, A., Cabral, A., Alvarado, L. y Alvarado, T. (2016). La técnica del proceso administrativo agropecuario estratégico - PAAE versión 2016. *Revista Mexicana de Agronegocios*, *38*, 209-216. https://www.redalyc.org/articulo.oa?id=14146082011

AlShboul, E., Thabtah, F., Abdelhamid, N. y Aldiabat, N.. (2018). A visualization cybersecurity method based on features' dissimilarity. *Computers & Security*, *77*, 289-303. https://doi.org/10.1016/j.cose.2018.04.007

Aponte, G. (2015). El proceso de gestión de innovación tecnológica: sus etapas e indicadores relacionados. *Revista Venezolana de Análisis de Coyuntura*, *XXI*(1), 59-90. https://www.redalyc.org/articulo.oa?id=36442240004

Arend, I., Shabtai, A., Idan, T., Keinan, R. y Bereby, Y. (2020). Passive- and not active-risk tendencies predict cyber security behavior. *Computers & Security*, *96*(101929), 1-7. https://doi.org/10.1016/j.cose.2020.101929

Arias, N. y Celis, J. (2015). *Modelo experimental de ciberseguridad y ciberdefensa para Colombia* [Tesis de grado, Universidad Libre]. https://repository.unilibre.edu.co/handle/10901/10904

Barberousse, P. (2008). Fundamentos teóricos del pensamiento complejo de Edgar Morin. *Revista Electrónica Educare*, XII(2), 95-113. https://www.redalyc.org/articulo.oa?id=194114586009

Basuchoudhary, A. y Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. *Computers & Security*, 87(101591), 1-13. https://doi.org/10.1016/j.cose.2019.101591

Becerril, A. (2019). La ciberseguridad en los Tratados de Libre Comercio. *Revista chilena de derecho y tecnología*, 8(2), 111-137. https://dx.doi.org/10.5354/0719-2584.2019.53447

Bernal, C. (2010). Metodología de la investigación para administración, economía, humanidades y ciencias sociales (3ra. ed.).Colombia: Pearson Educación.

Borraccimtsac, R. y Tajermtsac, C. (2006). Aplicación de la teoría de la información a la investigación clínica. *Revista Argentina de Cardiología*, 74(6), 483-486. https://www.redalyc.org/articulo.oa?id=3053/305326824013

Briones, W., Guanín, E., Morales, F. y Bajaña, F. (2019). Gestión de los procesos administrativos en extractoras de palma africana. *Ciencias Holguín*, 25(2), 1-14. https://www.redalyc.org/articulo.oa?id=181559111001

Cathalifaud, M. y Osorio, F. (1998). Introducción a los Conceptos Básicos de la Teoría General de Sistemas*. Cinta de Moebio*, (3). https://www.redalyc.org/articulo.oa?id=10100306

Chowdhury, N., Adam, M. y Teubnerb, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, 97(101963), 1-13. https://doi.org/10.1016/j.cose.2020.101963

CISCO. (2019). *What is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Diario Gestión. (09 de abril de 2020). *Ciberataques a dispositivos móviles en Perú se duplicaron en marzo*. Gestión Perú. Recuperado el 2 de setiembre de 2020 de https://gestion.pe/peru/ciberataques-a-dispositivos-moviles-en-peru-se-duplicaron-en-marzo-noticia/

Erosa, V. y Almaraz G. (2009). Estrategias para el cambio tecnológico: experiencia en el sector público mexicano. *CienciaUAT*, 4(2), 52-59. https://www.redalyc.org/articulo.oa?id=441942918008

European Union Agency for Cybersecurity. (10 de julio de 2020). *Annual Report on Trust Services Security Incidents in 2019*. https://www.enisa.europa.eu/news/enisa-news/annual-report-on-trust-services-security-incidents-in-2019

Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion Prevention Systems. *Information Security Technical Report,* 10(3), 134-139. https://doi.org/10.1016/j.istr.2005.08.001

Fundación Telefónica (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Ariel.

Garbarino, H. (2014). *Marco de Gobernanza de TI para empresas PyMES - SMEsITGF* [Tesis de doctorado, Universidad Politécnica de Madrid]. http://oa.upm.es/31002/

García, A. y González, F. (2013). *From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation*. Inter-American Development Bank.

Hernández, R., Fernández, C. y Baptista, M. (6ª ed.). (2014). *Metodología de la investigación*. McGRAW-HILL.

Huang, S., Shen, W., Yen, D. y Chou, L. (2011). IT governance: Objectives and assurances in internet banking. *Advances in Accounting*, 27(2), 406-414. https://dx.doi.org/10.1016/j.adiac.2011.08.001

Huayllani, O. (2020). *Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud* [Tesis de Maestría, Universidad Cesar Vallejo]. https://hdl.handle.net/20.500.12692/42775

Huerta, C. (2020). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en una consultora* [Tesis de Maestría, Universidad Cesar Vallejo]. https://hdl.handle.net/20.500.12692/46037

IBM. (2020). *IT Management.* Recuperado el 12 de setiembre de 2020 https://www.ibm.com/topics/it-management

Inoguchi, A. y Macha, E. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las Pymes del Perú* [Tesis de doctorado, Universidad San Ignacio de Loyola]. http://repositorio.usil.edu.pe/handle/USIL/2810

Kaspersky. (2020). *What is Cybersecurity?* Recuperado el 10 de setiembre de 2020. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lamine, E., Thabetf, R., Sienouc, A., Borke, D., Fontanilib, F. y Pingauda, H. (2020). BPRIM: An integrated framework for business process management and risk management. *Computers in Industry, 117*(103199), 1 – 17. https://doi.org/10.1016/j.compind.2020.103199

Landázuri, C. (2019). *Diseño de un modelo de gobernabilidad y gestión de TI para el área de desarrollo de proyectos de software de corporación favorita,*

basado en la metodología Devops [Tesis de Maestría]. Universidad Internacional Sek.

Maldonado, C. (2017). Ciencia hecha realidad. Reseña de C. A. Ossa, Teoría general de sistemas. Conceptos y aplicaciones. *INNOVAR. Revista de Ciencias Administrativas y Sociales*, 27(64), 157-159 https://www.redalyc.org/articulo.oa?id=81850404014

Mansfiel, S. (2017). The right response: how organisations should react to security incidents. *Network Security, 2017*(12), 16 – 19. https://doi.org/10.1016/S1353-4858(17)30124-1

Marcos, D. (2018). *Ciberseguridad aplicada a la e-democracia: análisis criptográfico y desarrollo de una metodología practica de evaluación para sistemas de voto electrónico remoto y su aplicación a las soluciones más relevantes* [Tesis de doctorado, Universidad de León]. http://hdl.handle.net/10612/7959

Mahdi, O., Nassar, I., y Almsafir, M. (2018). Knowledge management processes and sustainable competitive advantage: An empirical examination in private universities. *Journal of Business Research*, 94(1), 320-334. https://doi.org/10.1016/j.jbusres.2018.02.013

Martínez, R., Dueñas, R., Miyahira, J. y Dulanto, L. (2010). El Cuadro de Mando Integral en la ejecución del Plan Estratégico de un hospital general. *Revista Médica Herediana*, 21(3), 153-159 https://www.redalyc.org/articulo.oa?id=3380/338038899007

Meszaros, J. y Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security, 65*(101944), 300 – 313. https://doi.org/10.1016/j.cose.2016.12.008

Meyer, J., Dembinsky, O. y Raviv, T. (2020). Alerting about possible risks vs blocking risky choices: A quantitative model and its empirical evaluation. *Computers & Security, 97*(101944), 1 – 37. https://doi.org/10.1016/j.cose.2020.101944

Mozaffari, N., Rezazadeh, J., Farahbakhsh, R., Yazdani, S. y Sandrasegaran, K. (2019). Practical fall detection based on IoT technologies: *A survey. Internet of Things, 8*(100124), 1 – 41. https://doi.org/10.1016/j.iot.2019.100124

Núñez, E. (2011). Gestión tecnológica en la empresa: definición de sus objetivos fundamentales. *Revista de Ciencias Sociales* (Ve), XVII(1), 156-1665-9518. https://www.redalyc.org/articulo.oa?id=28022755013

Ñeco, L., Baños, M., Bernal, I., Gonda, C., Guilló A., Amatriain, M., Leal, A., & Martínez, L., Merafina, M., Pina, R., Valenciano, G. y Santamaría, S. (2018). Teorías sistémicas y paradigma de investigación performativa en los estudios superiores de danza. *El Artista*, (15). https://www.redalyc.org/articulo.oa?id=87457958009

Prion, S. y Haerling, K. (2014). Making Sense of Methods and Measurement: Spearman-Rho Ranked-Order Correlation Coefficient. *Clinical Simulation in Nursing*, 10(10), 535-536 https://doi.org/10.1016/j.ecns.2014.07.005

Ramírez, R., Royero, G. y El Kadi, O. (2019). Gestión tecnológica como factor clave de éxito en universidades privadas. *Telos*, 21(1), 10-32 https://www.redalyc.org/articulo.oa?id=99357718023

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Alava, C., Murillo, Á. y Castillo, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Área de Innovación y Desarrollo. http://dx.doi.org/10.17993/IngyTec.2018.46

Rubio, G., Blandón, A. y Serna, H. (2019). Análisis de los factores que componen un sistema de gestión empresarial. Estudio de caso. *Revista Científica Hermes*, 25, 408-430 https://www.redalyc.org/articulo.oa?id=477662439011

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, 9(1), 127-137 https://www.redalyc.org/articulo.oa?id=5722/572261854012

Sánchez, J. (2017). *Adopción de estrategias de ciberseguridad en la protección de la información en la oficina de economía del ejército* [Tesis de Maestría, Instituto científico tecnológico del ejército]. http://repositorio.icte.ejercito.mil.pe/handle/ICTE/26

Sánchez, H., Reyes, C., y Mejía, K. (2018). Manual de términos en investigación científica, tecnológica y humanística. Lima: Bussiness Support Aneth S.R.L.

Santana, L., Pérez, P. y Abreu, R. (2019). La gestión de Tecnologías de la Información: análisis factorial confirmatorio. *Ingeniería Industrial.* XL(3), 272-284. https://www.redalyc.org/articulo.oa?id=360461152006

Sareian, Shirazi y Motameni (2019). Optimal autonomous architecture for uncertain processes Management. *Information Sciences*, 501(1), 84-99. https://doi.org/10.1016/j.ins.2019.05.095

Servín, R., Cruz, C., Hidalgo, J., Ramírez, G. y Ramos, A. (2018). Factores criticos en la administración de trapiches de la región de huatusco, veracruz. *Revista Mexicana de Agronegocios.* 42( ), 919-928. https://www.redalyc.org/articulo.oa?id=14156175011

Shin, B. y Lowry, P. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, 92(101761), 1-16 https://doi.org/10.1016/j.cose.2020.101761

Solano, O., Riascos, S., y Aguilera, A. (2013). Determinantes de los planes estratégicos de los sistemas de información en las pymes colombianas: caso Santiago de Cali - Colombia. *Entramado*, 9(1), 26-36 https://www.redalyc.org/articulo.oa?id=265428385003

Solms R. (2013). From information security to cyber security. *Computers & Security*, 38(2), 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Vallejos, M. (2013). Modelo de gestión universitaria y unidades académicas de calidad. UCV-HACER. *Revista de Investigación y Cultura*, 2(1), 141-144. https://www.redalyc.org/articulo.oa?id=521752180017

Viloria, N. y C, R. (2004). Las Ciencias de la Educación a través del Proceso Administrativo. *Actualidad Contable Faces,* 7(8), 96-107. https://www.redalyc.org/articulo.oa?id=25700809

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
Problema principal: ¿Qué relación existe entre la ciberseguridad y la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020? **Problemas específicos:** PE1: ¿Cómo se relaciona la gestión de tecnologías de información con la dimensión prevención de la ciberseguridad en la empresa I & T Electric, Lima - 2020? PE2: ¿Cómo se relaciona la gestión de tecnologías de información con la dimensión detección de la	**Objetivo principal:** Determinar la relación de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. **Objetivos específicos:** OE1: Determinar la relación que existe entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. OE2: Determinar la relación que existe entre la dimensión detección de la ciberseguridad con la	**Hipótesis principal:** Existe relación significativa de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020. **Hipótesis específicos:** HE1: Existe relación significativa entre la dimensión prevención de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. HE2: Existe relación significativa entre la dimensión detección de la ciberseguridad con la	**Variable - 1: Ciberseguridad**

Dimensiones	Indicadores	Ítems	Niveles
Prevención	Anticipación	1-2	Alta prevalencia
	Confiabilidad	3-4	
	Integridad	5-6	
Detección	Anticipación	7-8	Media prevalencia
	Confiabilidad	9-10	
	Mejora	11-12	Baja prevalencia
Reacción	Revisión	13-14	
	Disponibilidad	15-16	
	Mejora	17-18	

Variable - 2: Gestión de tecnologías de información

Dimensiones	Indicadores	Ítems	Niveles
Planificación	Revisión	19-20	Optimo
	Disponibilidad	21-22	
	Mejora	23-24	Medio

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
ciberseguridad en la empresa I & T Electric, Lima - 2020? PE3: ¿Cómo se relaciona la gestión de tecnologías de información con la dimensión reacción de la ciberseguridad en la empresa I & T Electric, Lima - 2020?	gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. OE3: Determinar la relación que existe entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020.	gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. HE3: Existe relación significativa entre la dimensión reacción de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020.	Dirección	Revisión	25-26	No Optimo
				Confiabilidad	27-28	
				Verificación	29-30	
			Control	Revisión	31-32	
				Verificación	33-34	
				Mejora	35-36	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Básica **Diseño:** No experimental.	**Población:** 87 empleados **Tamaño de muestra:** 71 empleados. **Muestreo:** Probabilístico aleatorio simple	**Técnicas:** Entrevista. **Instrumentos:** Encuesta.	**Descriptiva:** Para realizar el análisis descriptivo, se emplea tablas de contingencia para un análisis bidimensional e histogramas que permitan describir la información respectiva a la muestra. **Inferencial:** Para realizar el análisis inferencial se empleó métodos no paramétricos y se aplicó el coeficiente de correlación de Rho Spearman que permitió determinar el grado de correlación entre las variables.

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable – 1: Ciberseguridad La Fundación Telefónica (2016) describen que la ciberseguridad es un proceso que implica prevención, detección y reacción, en el cual se debe considerar aprendizaje objetivo que conlleve a la mejora continua inherente del mencionado proceso	**Prevención** Mozaffari et al. (2019) menciona que la prevención es aquella fase que tiene como principal fin ofrecer soluciones centradas en el internet de las cosas que optimizan las condiciones físicas, fisiológicas y ambientales para prever eventos de fallas en el servicio, en lo global, la prevención se ofrecen enfocados a los factores de riesgo.	Anticipación	1	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	Totalmente en desacuerdo En desacuerdo Ni de acuerdo ni en desacuerdo De acuerdo Totalmente de acuerdo
			2	¿La oficina de tecnología de información lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	
		Confiabilidad	3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	
			4	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	
		Integridad	5	¿Cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?	
			6	¿Cree usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?	

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Detección Romero et al. (2018) quienes exponen que la detección trata sobre las fases de detección son más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso	Anticipación	7	¿Cree usted que la oficina de tecnología de información tiene incorporado planes de protección de detección contra los cibercriminales?	
			8	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	
		Confiabilidad	9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la empresa para evitar acciones desleales que conlleven a pérdida o robo de información?	
			10	¿La oficina de tecnología de información implementa cámaras de seguridad para detectar evitar accionares de personas no autorizadas con la información?	
		Mejora	11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	
			12	¿La empresa cuenta con algún medio de seguridad tecnológico para que los empleados se identifiquen al ingresar?	

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Reacción Romero, et al. (2018) quienes indican que en esta fase se tiene una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo.	Revisión	13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	
			14	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ciberataque?	
		Disponibilidad	15	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?	
			16	¿Considera usted que en el último año se ha perdido información importante por acusa de algún virus informático?	
		Mejora	17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	
			18	¿Cree usted que el área de TI busca mejoras para la ciberseguridad?	

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Variable – 2: Gestión de tecnologías de información Núñez (2011) describe que La gestión de TI es un proceso gerencial que contempla la planificación, la organización, la dirección y el control de las tecnologías de información en las organizaciones, con el propósito de conseguir alcanzar los objetivos planteados dentro de la organización y lograr ventajas competitivas en el mercado a través de una mejora continua	**Planificación** Erosa (2009) quién describe que la planificación es una especificación del modelo estratégico al que se alineó la estructura de la solución tecnológica, prueba de la solución en desarrollo y posteriormente su implantación en productivo, diseño del esquema de formación de competencias de los usuarios en las variantes estratégica y operativa.	Revisión	19	¿Considera usted que la oficina de tecnología de información cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?	Totalmente en desacuerdo En desacuerdo Ni de acuerdo ni en desacuerdo De acuerdo Totalmente de acuerdo
			20	¿Considera usted que la oficina de tecnología de información prevé adecuadamente la atención de incidencias de TI?	
		Disponibilidad	21	¿Cree usted que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	
			22	¿Qué tan conforme está usted con la disponibilidad del internet dentro de la empresa?	
		Mejora	23	¿Cree usted que la oficina de tecnología de información realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?	
			24	¿Cree usted que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la empresa?	
	Dirección	Revisión	25	¿Considera usted que la oficina de tecnología de información realiza mantenimientos oportunos a	

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	Briones et al. (2019) definen la dirección como aquel elemento en el que se logra la realización efectiva de todo lo planeado, por medio de la autoridad del líder, ejercida a base de decisiones, ya sea tomadas directamente, ya, con más frecuencia, se delega dicha autoridad, y se vigila simultáneamente que se cumplan en la forma adecuada todas las órdenes emitidas.			los dispositivos de la organización (computadoras, celulares, tablets, impresoras, etc.?	
			26	¿Ha recibido capacitación de parte de la oficina de tecnología de información respecto al uso adecuado de las tecnologías de la empresa?	
		Confiabilidad	27	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna?	
			28	¿Tiene usted conocimiento de cómo actuar ante una incidencia con los servicios de TI?	
		Verificación	29	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, le informan oportunamente sobre el estado del mismo?	
			30	¿Considera usted que la dirección de la oficina de tecnología de información es adecuada?	
	Control Rubio, Blandon y Serna (2019) definen el control como una función,	Revisión	31	¿Considera usted que los sistemas de información de la empresa son vitales en el accionar de su función y centro de actividad?	

TÍTULO: Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020.

AUTOR: ALBERTO ISMAEL BOHORQUEZ SALCEDO

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	que esencialmente cumple un rol de regulación, verificando que los criterios seleccionados inicialmente se lleven a la práctica. La principal finalidad del control es el diagnóstico de errores, la identificación de variaciones y la prevención y corrección de las desviaciones identificadas. Por ende, el control debe estar relacionado con los planes inicialmente definidos, debe permitir la medición y cuantificación de los resultados, la detección de desviaciones y el establecimiento de medidas correctivas y preventivas.		32	¿Cree que usted que la oficina de tecnología de información ayuda a los objetivos de su centro de actividad?	
		Verificación	33	¿Cree usted que ha obtenido resultados óptimos de la oficina de tecnología de información?	
			34	¿Cree usted que la oficina de tecnología de información responde adecuadamente a las necesidades tecnológicas de su área?	
		Mejora	35	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	
			36	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto al hardware, software y redes?	

Anexo 3: Instrumento de Recolección de Datos
Cuestionario para empleador de I & t Electric

Fecha: [/ /] **Edad:** [ ]
Sexo: Femenino[ ] Masculino[ ]
Tipo de cargo: Practicante[ ] Asistente[ ] Encargado[ ]
Grado de estudio: Primaria [ ] Secundaria [ ] Superior Técnica[ ] Superior Universitaria[ ]

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente **ejemplo**: Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5).

No	Pregunta	Valoración				
		1	2	3	4	5
	Sobre la ciberseguridad					
1	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	Totalmente en desacuerdo				
2	¿La oficina de tecnología de información lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?					
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?					
4	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?					
5	¿Cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?					
6	¿Cree usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?					
7	¿Cree usted que la oficina de tecnología de información tiene incorporado planes de protección de detección contra los cibercriminales?					
8	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?					
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la empresa para evitar acciones desleales que conlleven a pérdida o robo de información?					
10	¿La oficina de tecnología de información implementa cámaras de seguridad para detectar evitar accionares de personas no autorizadas con la información?					
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?					
12	¿La empresa cuenta con algún medio de seguridad tecnológico para que los empleados se identifiquen al ingresar?					
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?					
14	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ciberataque?					
15	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?					
16	¿Considera usted que en el último año se ha perdido información importante por acusa de algún virus informático?					
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?					
18	¿Cree usted que el área de TI busca mejoras para la ciberseguridad?					

¡Gracias por su tiempo!

No	Pregunta	Valoración				
		1	2	3	4	5
	Sobre la Gestión de Tecnologías de información					
19	¿Considera usted que la oficina de tecnología de información cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?					
20	¿Considera usted que la oficina de tecnología de información prevé adecuadamente la atención de incidencias de TI?					
21	¿Cree usted que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?					
22	¿Qué tan conforme está usted con la disponibilidad del internet dentro de la empresa?					
23	¿Cree usted que la oficina de tecnología de información realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?					
24	¿Cree usted que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la empresa?					
25	¿Considera usted que la oficina de tecnología de información realiza mantenimientos oportunos a los dispositivos de la organización (computadoras, celulares, tablets, impresoras, etc.?					
26	¿Ha recibido capacitación de parte de la oficina de tecnología de información respecto al uso adecuado de las tecnologías de la empresa?					
27	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna?					
28	¿Tiene usted conocimiento de cómo actuar ante una incidencia con los servicios de TI?					
29	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, le informan oportunamente sobre el estado del mismo?					
30	¿Considera usted que la dirección de la oficina de tecnología de información es adecuada?					
31	¿Considera usted que los sistemas de información de la empresa son vitales en el accionar de su función y centro de actividad?					
32	¿Cree que usted que la oficina de tecnología de información ayuda a los objetivos de su centro de actividad?					
33	¿Cree usted que ha obtenido resultados óptimos de la oficina de tecnología de información?					
34	¿Cree usted que la oficina de tecnología de información responde adecuadamente a las necesidades tecnológicas de su área?					
35	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?					
36	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto al hardware, software y redes?					

¡Gracias por su tiempo!

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos
Validación de experto N° 1

VARIABLE: Ciberseguridad

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PREVENCIÓN	Si	No	Si	No	Si	No	
1	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	X		X		X		
2	¿La oficina de tecnología de información lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	X		X		X		
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	X		X		X		
4	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	X		X		X		
5	¿Cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?	X		X		X		
6	¿Cree usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?	X		X		X		
	DETECCIÓN	Si	No	Si	No	Si	No	
7	¿Cree usted que la oficina de tecnología de información tiene incorporado planes de protección de detección contra los cibercriminales?	X		X		X		
8	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	X		X		X		
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la empresa para evitar acciones desleales que conlleven a pérdida o robo de información?	X		X		X		
10	¿La oficina de tecnología de información implementa cámaras de seguridad para detectar evitar accionares de personas no autorizadas con la información?	X		X		X		
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	X		X		X		
12	¿La empresa cuenta con algún medio de seguridad para que los empleados se identifiquen al ingresar?	X		X		X		
	REACCIÓN	Si	No	Si	No	Si	No	
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	X		X		X		
14	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ciberataque?	X		X		X		
15	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?	X		X		X		
16	¿Considera usted que en el último año se ha perdido información importante por acusa de algún virus informático?	X		X		X		
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	X		X		X		
18	¿Cree usted que el área de TI busca mejoras para la ciberseguridad?	X		X		X		

VARIABLE: Gestión de tecnología de información

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PLANIFICACIÓN	Si	No	Si	No	Si	No	
19	¿Considera usted que la oficina de tecnología de información cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?	X		X		X		
20	¿Considera usted que la oficina de tecnología de información prevé adecuadamente la atención de incidencias de TI?	X		X		X		
21	¿Cree usted que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	X		X		X		
22	¿Qué tan conforme está usted con la disponibilidad del internet dentro de la empresa?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
23	¿Cree usted que la oficina de tecnología de información realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?	X		X		X		
24	¿Cree usted que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la empresa?	X		X		X		
	DIRECCIÓN	Si	No	Si	No	Si	No	
25	¿Considera usted que la oficina de tecnología de información realiza mantenimientos oportunos a los dispositivos de la organización (computadoras, celulares, tablets, impresoras, etc.?	X		X		X		
26	¿Ha recibido capacitación de parte de la oficina de tecnología de información respecto al uso adecuado de las tecnologías de la empresa?	X		X		X		
27	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna?	X		X		X		
28	¿Tiene usted conocimiento de cómo actuar ante una incidencia con los servicios de TI?	X		X		X		
29	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, le informan oportunamente sobre el estado del mismo?	X		X		X		
30	¿Considera usted que la dirección de la oficina de tecnología de información es adecuada?	X		X		X		
	CONTROL	Si	No	Si	No	Si	No	
31	¿Considera usted que los sistemas de información de la empresa son vitales en el accionar de su función y centro de actividad?	X		X		X		
32	¿Cree que usted que la oficina de tecnología de información ayuda a los objetivos de su centro de actividad?	X		X		X		
33	¿Cree usted que ha obtenido resultados óptimos de la oficina de tecnología de información?	X		X		X		
34	¿Cree usted que la oficina de tecnología de información responde adecuadamente a las necesidades tecnológicas de su área?	X		X		X		
35	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	X		X		X		
36	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto al hardware, software y redes?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

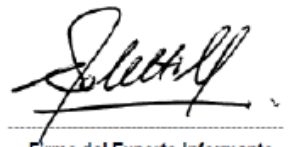
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

13 de octubre del 2020

Apellidos y nombre s del juez evaluador: POLETTI GAITAN, EDUARDO HUMBERTO DNI: 18073124

Especialista: Metodólogo [ ] Temático [X]

Grado: Maestro [X] Doctor [ ]



Firma del Experto Informante

[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 al componente o dimensión específica del constructo

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

Validación de experto N° 2

VARIABLE: Ciberseguridad

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PREVENCIÓN	Sí	No	Sí	No	Sí	No	
1	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	X		X		X		
2	¿La oficina de tecnología de información lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	X		X		X		
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	X		X		X		
4	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	X		X		X		
5	¿Cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?	X		X		X		
6	¿Cree usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?	X		X		X		
	DETECCIÓN	Sí	No	Sí	No	Sí	No	
7	¿Cree usted que la oficina de tecnología de información tiene incorporado planes de protección de detección contra los cibercriminales?	X		X		X		
8	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	X		X		X		
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la empresa para evitar acciones desleales que conlleven a pérdida o robo de información?	X		X		X		
10	¿La oficina de tecnología de información implementa cámaras de seguridad para detectar evitar accionares de personas no autorizadas con la información?	X		X		X		
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	X		X		X		
12	¿La empresa cuenta con algún medio de seguridad para que los empleados se identifiquen al ingresar?	X		X		X		
	REACCIÓN	Sí	No	Sí	No	Sí	No	
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	X		X		X		
14	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ciberataque?	X		X		X		
15	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?	X		X		X		
16	¿Considera usted que en el último año se ha perdido información importante por acusa de algún virus informático?	X		X		X		
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	X		X		X		
18	¿Cree usted que el área de TI busca mejoras para la ciberseguridad?	X		X		X		

VARIABLE: Gestión de tecnología de información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PLANIFICACIÓN	Sí	No	Sí	No	Sí	No	
19	¿Considera usted que la oficina de tecnología de información cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?	X		X		X		
20	¿Considera usted que la oficina de tecnología de información prevé adecuadamente la atención de incidencias de TI?	X		X		X		
21	¿Cree usted que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	X		X		X		
22	¿Qué tan conforme está usted con la disponibilidad del internet dentro de la empresa?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
23	¿Cree usted que la oficina de tecnología de información realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?	X		X		X		
24	¿Cree usted que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la empresa?	X		X		X		
	DIRECCIÓN	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Considera usted que la oficina de tecnología de información realiza mantenimientos oportunos a los dispositivos de la organización (computadoras, celulares, tablets, impresoras, etc.?	X		X		X		
26	¿Ha recibido capacitación de parte de la oficina de tecnología de información respecto al uso adecuado de las tecnologías de la empresa?	X		X		X		
27	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna?	X		X		X		
28	¿Tiene usted conocimiento de cómo actuar ante una incidencia con los servicios de TI?	X		X		X		
29	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, le informan oportunamente sobre el estado del mismo?	X		X		X		
30	¿Considera usted que la dirección de la oficina de tecnología de información es adecuada?	X		X		X		
	CONTROL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
31	¿Considera usted que los sistemas de información de la empresa son vitales en el accionar de su función y centro de actividad?	X		X		X		
32	¿Cree que usted que la oficina de tecnología de información ayuda a los objetivos de su centro de actividad?	X		X		X		
33	¿Cree usted que ha obtenido resultados óptimos de la oficina de tecnología de información?	X		X		X		
34	¿Cree usted que la oficina de tecnología de información responde adecuadamente a las necesidades tecnológicas de su área?	X		X		X		
35	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	X		X		X		
36	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto al hardware, software y redes?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Lima, 14 de octubre del 2020

Apellidos y nombre s del juez evaluador: Chumpe Agesto, Juan Brues **DNI: 44824114**

Especialista: Metodólogo [ ] Temático [X]

Grado: Maestro [ ] Doctor [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 al componente o dimensión específica del constructo

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

Firma del Experto Informante

Validación de experto N° 3

VARIABLE: Ciberseguridad

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PREVENCIÓN	Si	No	Si	No	Si	No	
1	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	X		X		X		
2	¿La oficina de tecnología de información lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	X		X		X		
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	X		X		X		
4	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	X		X		X		
5	¿Cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?	X		X		X		
6	¿Cree usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?	X		X		X		
	DETECCION	Si	No	Si	No	Si	No	
7	¿Cree usted que la oficina de tecnología de información tiene incorporado planes de protección de detección contra los cibercriminales?	X		X		X		
8	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	X		X		X		
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la empresa para evitar acciones desleales que conlleven a pérdida o robo de información?	X		X		X		
10	¿La oficina de tecnología de información implementa cámaras de seguridad para detectar evitar accionares de personas no autorizadas con la información?	X		X		X		
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	X		X		X		
12	¿La empresa cuenta con algún medio de seguridad para que los empleados se identifiquen al ingresar?	X		X		X		
	REACCIÓN	Si	No	Si	No	Si	No	
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	X		X		X		
14	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ciberataque?	X		X		X		
15	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?	X		X		X		
16	¿Considera usted que en el último año se ha perdido información importante por acusa de algún virus informático?	X		X		X		
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	X		X		X		
18	¿Cree usted que el área de TI busca mejoras para la ciberseguridad?	X		X		X		

VARIABLE: Gestión de tecnología de información

N°	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	PLANIFICACION	Si	No	Si	No	Si	No	
19	¿Considera usted que la oficina de tecnología de información cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?	X		X		X		
20	¿Considera usted que la oficina de tecnología de información prevé adecuadamente la atención de incidencias de TI?	X		X		X		
21	¿Cree usted que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	X		X		X		
22	¿Qué tan conforme está usted con la disponibilidad del internet dentro de la empresa?	X		X		X		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
23	¿Cree usted que la oficina de tecnología de información realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?	X		X		X		
24	¿Cree usted que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la empresa?	X		X		X		
	DIRECCIÓN	Si	No	Si	No	Si	No	
25	¿Considera usted que la oficina de tecnología de información realiza mantenimientos oportunos a los dispositivos de la organización (computadoras, celulares, tablets, impresoras, etc.?	X		X		X		
26	¿Ha recibido capacitación de parte de la oficina de tecnología de información respecto al uso adecuado de las tecnologías de la empresa?	X		X		X		
27	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna?	X		X		X		
28	¿Tiene usted conocimiento de cómo actuar ante una incidencia con los servicios de TI?	X		X		X		
29	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, le informan oportunamente sobre el estado del mismo?	X		X		X		
30	¿Considera usted que la dirección de la oficina de tecnología de información es adecuada?	X		X		X		
	CONTROL	Si	No	Si	No	Si	No	
31	¿Considera usted que los sistemas de información de la empresa son vitales en el accionar de su función y centro de actividad?	X		X		X		
32	¿Cree que usted que la oficina de tecnología de información ayuda a los objetivos de su centro de actividad?	X		X		X		
33	¿Cree usted que ha obtenido resultados óptimos de la oficina de tecnología de información?	X		X		X		
34	¿Cree usted que la oficina de tecnología de información responde adecuadamente a las necesidades tecnológicas de su área?	X		X		X		
35	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	X		X		X		
36	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto al hardware, software y redes?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

13 de octubre del 2020

Apellidos y nombre s del juez evaluador: LEZAMA GONZALES PEDRO MARTÍN **DNI: 09656793**

Especialista: Metodólogo [X] Temático [ ]

Grado: Maestro [ ] Doctor [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 al componente o dimensión específica del constructo

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

Firma de Experto Informante

Anexo 5: Base de datos de la aplicación

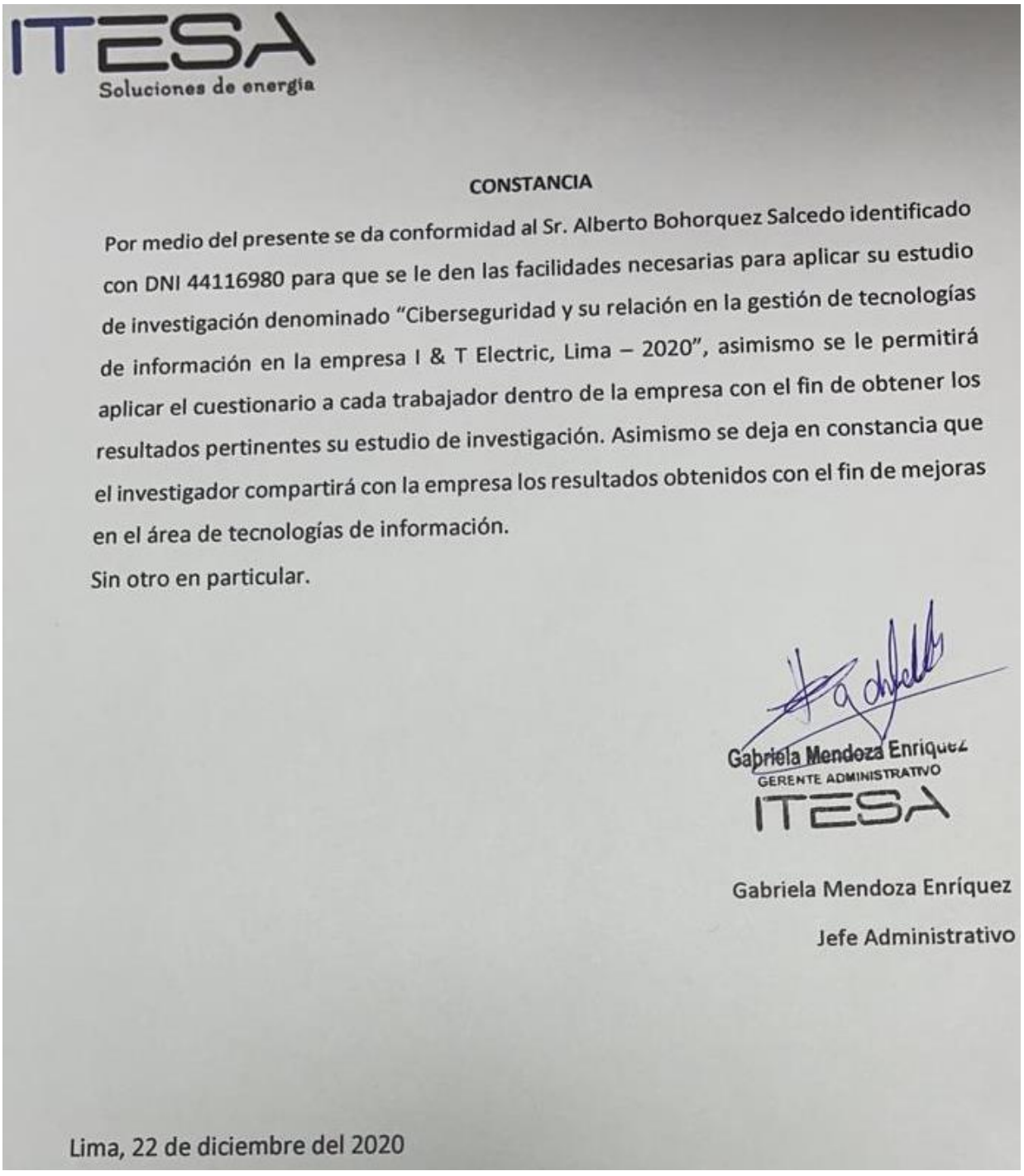
				Variable 1																		Variable 1																	
				D1						D2						D3						D4						D5						D6					
				I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N°	Edad	Sexo	T. Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
1	34	2	1	3	4	5	1	2	1	4	1	4	3	2	4	2	1	3	4	5	4	3	2	1	5	5	3	4	3	5	1	5	1	2	3	4	3	4	4
2	19	1	3	3	4	3	2	3	3	4	1	3	3	3	5	3	2	5	5	3	3	2	4	2	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3
3	22	2	3	4	4	4	4	3	2	4	3	5	4	4	5	3	5	4	4	4	5	3	4	2	4	4	4	4	5	4	5	5	4	4	4	4	4	4	4
4	26	2	1	4	5	5	3	2	4	4	1	5	5	5	4	3	2	4	4	4	5	4	4	1	5	5	4	4	4	3	5	5	4	4	4	5	5	5	4
5	21	1	2	3	4	3	4	2	2	3	3	4	5	4	5	1	1	5	3	3	4	3	3	3	3	3	4	4	4	3	4	4	4	3	3	4	3	3	4
6	29	2	1	3	3	1	2	2	2	1	1	3	2	3	4	3	1	3	1	3	3	3	4	2	2	4	1	3	2	4	1	2	1	1	3	1	3	2	3
7	31	1	1	3	3	4	2	4	3	4	1	5	5	5	3	5	3	5	5	4	4	3	4	2	5	4	4	4	4	4	2	5	4	4	4	4	5	3	3
8	34	2	2	4	4	5	3	1	2	4	1	5	4	3	3	2	1	4	3	3	4	3	4	1	4	2	3	3	4	4	2	5	2	4	4	4	4	4	3
9	33	2	1	4	5	2	1	1	1	4	2	4	3	4	3	3	1	5	5	3	4	5	4	3	4	3	4	3	4	3	4	4	3	4	4	5	5	5	5
10	32	2	1	2	2	1	1	1	3	4	2	4	3	3	4	1	3	3	3	3	3	2	2	2	4	4	3	3	2	4	2	4	2	4	2	2	2	2	2
11	29	1	2	4	4	4	1	2	1	4	2	3	5	3	4	2	1	5	5	5	4	4	3	3	3	4	4	5	4	4	5	5	4	4	4	4	4	4	5
12	30	1	3	5	4	4	2	1	3	3	3	3	3	3	4	3	2	4	4	3	4	3	5	1	4	4	4	3	4	4	4	4	5	5	5	4	4	4	3
13	34	1	2	4	4	3	1	2	1	4	1	4	4	4	5	3	2	3	5	3	2	4	4	2	4	3	4	3	1	3	3	4	3	1	4	4	4	1	3
14	24	1	3	4	4	1	1	2	1	3	1	3	3	3	2	1	1	3	3	3	2	3	3	1	3	1	1	3	2	3	1	3	1	2	3	2	3	2	3
15	30	2	2	5	5	3	2	4	3	5	3	4	5	4	4	4	2	5	4	3	5	3	5	3	5	4	4	3	4	4	5	5	5	5	5	5	4	4	4
16	20	1	1	4	4	4	1	1	3	3	1	3	5	3	3	2	1	3	5	4	3	4	4	2	5	4	4	3	4	4	1	5	1	2	4	4	4	4	2
17	22	1	2	4	4	4	2	2	1	4	2	4	3	3	5	3	2	3	4	4	3	4	4	3	4	4	4	4	4	4	4	5	5	4	5	5	4	4	4
18	29	2	3	4	4	3	1	1	3	3	3	4	5	4	3	2	3	4	4	3	4	2	3	3	3	4	4	4	4	4	3	4	2	3	3	4	3	3	2
19	27	2	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3	3	3	3	3	4	3	4

				Variable 1																		Variable 1																	
				D1						D2						D3						D4						D5						D6					
				I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N°	Edad	Sexo	T. Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
20	27	2	3	4	4	3	1	3	3	3	1	3	3	2	5	2	2	4	5	4	3	4	4	1	4	4	4	4	3	3	1	4	1	2	4	4	4	4	2
21	33	2	2	5	4	3	3	3	2	3	1	4	4	4	3	1	3	3	5	4	3	4	4	2	4	4	4	5	4	4	3	5	5	4	5	4	4	4	4
22	30	1	1	3	3	2	2	2	3	2	1	2	3	3	3	2	3	4	3	3	3	3	3	1	3	2	2	2	3	3	3	3	3	2	3	3	3	3	3
23	48	2	1	4	4	4	2	2	1	4	3	4	3	4	3	3	1	5	3	3	3	4	4	2	4	3	4	4	4	4	4	5	4	4	4	4	4	4	2
24	40	1	2	4	4	3	2	3	2	4	1	4	3	4	5	2	2	3	3	3	3	3	3	3	3	3	4	3	4	4	3	3	3	3	4	4	3	3	3
25	31	2	2	3	4	4	1	1	3	4	1	4	3	3	3	1	3	3	4	4	4	3	3	3	4	2	4	4	4	2	3	3	2	3	3	4	4	4	3
26	44	1	3	4	4	3	3	3	1	3	1	3	5	3	3	1	1	3	3	4	4	3	3	1	4	3	4	3	4	4	4	3	3	3	4	3	3	3	4
27	39	2	2	3	4	3	1	2	2	4	1	4	4	4	5	2	2	3	3	4	3	3	4	1	4	4	4	4	4	4	2	3	2	2	4	4	3	3	2
28	31	1	3	3	4	2	2	1	1	4	3	4	3	3	3	2	1	5	4	4	4	4	4	2	4	4	4	4	4	4	2	4	2	4	4	4	4	4	4
29	47	2	1	3	4	3	1	4	3	4	4	5	4	4	5	3	5	5	5	3	4	4	4	1	5	3	5	4	4	4	4	5	5	5	3	4	3	4	4
30	25	2	3	3	4	3	1	2	1	4	1	4	4	4	5	3	3	3	4	4	4	3	4	1	4	3	4	4	3	4	3	4	4	3	4	4	4	4	4
31	23	2	1	4	4	3	1	3	2	3	3	3	5	3	5	2	1	5	5	4	4	4	4	2	4	4	4	4	4	4	3	3	3	3	4	4	4	3	4
32	39	1	3	4	4	4	3	4	4	5	2	4	5	4	5	4	3	4	5	4	4	3	4	3	3	4	5	5	4	4	2	4	4	5	4	4	4	3	4
33	47	2	3	1	2	3	1	2	1	2	2	2	4	4	5	2	3	5	3	4	1	3	2	3	4	3	3	3	4	3	4	5	1	1	1	2	2	1	1
34	25	1	1	4	4	3	3	2	3	4	2	4	3	4	4	3	3	3	4	3	2	3	3	3	4	4	4	4	3	3	2	4	2	3	4	4	4	3	3
35	46	1	1	4	5	5	4	5	5	5	3	2	5	4	3	5	5	5	5	4	5	2	3	3	3	3	3	4	3	3	5	5	5	5	4	5	5	4	4
36	21	1	1	2	3	4	3	3	3	2	2	4	3	3	3	3	3	3	5	2	3	4	2	3	3	4	4	2	3	3	2	3	4	3	4	4	2	3	2
37	26	2	2	3	4	2	2	2	1	4	2	4	5	3	4	1	1	4	5	2	2	3	3	2	4	3	4	4	3	3	2	3	2	2	3	4	2	3	4
38	27	2	3	4	4	4	2	1	1	2	3	4	3	2	4	2	3	5	3	2	2	3	3	3	3	4	3	3	3	3	3	3	2	3	3	4	4	4	4
39	35	1	1	4	2	4	3	1	1	3	1	4	5	3	3	1	3	3	4	4	3	3	4	3	4	2	2	4	2	2	4	4	4	2	4	2	2	2	3

				Variable 1																		Variable 1																	
				D1						D2						D3						D4						D5						D6					
				I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N°	Edad	Sexo	T. Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
40	33	1	2	2	2	4	2	3	1	3	2	3	3	2	3	2	2	5	3	3	2	3	4	1	3	2	3	3	2	2	2	3	4	3	4	4	3	2	3
41	31	2	1	2	2	2	3	1	1	3	1	2	5	3	3	3	2	5	5	4	4	4	3	2	4	4	4	3	4	5	3	2	4	2	3	3	4	2	4
42	20	2	1	2	3	3	3	1	2	2	2	4	4	3	3	1	1	3	5	2	4	4	4	2	4	3	3	2	3	4	3	2	3	2	4	4	4	4	2
43	23	2	2	2	2	2	1	2	3	3	1	2	5	2	4	1	3	4	5	3	4	4	4	2	4	3	2	2	3	2	3	4	3	3	3	2	4	4	3
44	18	1	1	4	3	2	3	3	2	2	1	4	3	2	5	3	3	3	5	3	3	2	4	3	4	3	4	3	2	4	3	3	3	2	4	3	2	2	3
45	25	1	3	3	3	2	3	1	2	2	1	3	4	3	5	1	2	3	3	2	3	2	4	3	2	2	3	4	3	3	2	4	2	3	3	2	4	3	2
46	28	1	3	3	2	2	3	1	1	2	1	2	5	4	4	1	3	3	3	4	4	3	4	1	3	4	4	2	2	4	4	3	2	3	4	4	5	4	3
47	29	2	1	4	3	5	2	3	3	4	3	4	5	4	5	3	5	5	5	4	3	4	4	4	3	4	4	4	3	3	4	4	4	3	5	5	4	4	4
48	24	2	1	4	2	2	5	1	3	3	2	3	5	3	3	1	1	4	5	4	4	3	4	2	4	4	2	2	4	2	2	2	4	2	4	2	3	4	4
49	33	1	2	3	2	4	2	3	2	3	2	2	4	3	4	1	1	3	5	2	3	2	3	1	2	4	2	3	4	2	4	2	2	4	4	2	2	2	4
50	31	1	1	2	2	2	3	2	1	3	1	4	4	4	4	1	3	4	4	2	2	2	5	2	2	4	3	2	3	3	3	2	2	3	3	4	2	2	2
51	30	1	1	3	3	3	4	2	1	2	1	3	5	2	3	3	1	4	4	3	3	3	2	1	2	4	2	4	3	4	3	3	3	3	3	3	4	3	4
52	41	2	3	4	3	4	4	2	3	3	1	4	3	4	4	2	2	4	4	2	2	4	3	1	2	4	2	4	4	3	4	4	2	3	2	2	4	2	2
53	37	1	2	3	2	4	4	3	1	3	2	4	5	2	4	2	1	5	4	2	4	4	2	1	4	2	4	3	4	4	2	2	2	2	4	2	4	2	2
54	20	2	3	2	3	4	3	1	3	3	1	3	5	3	4	1	3	4	3	4	4	3	2	2	2	3	3	4	4	4	3	4	2	3	3	2	2	2	2
55	49	1	1	4	3	2	3	3	2	3	1	4	4	2	5	3	2	3	4	2	2	2	4	2	3	4	2	3	3	2	3	1	2	4	4	3	4	4	2
56	50	2	1	2	2	2	2	1	1	2	1	2	4	2	3	1	1	5	5	2	4	2	2	1	2	2	4	4	2	2	3	1	2	1	3	3	3	3	2
57	33	1	2	3	4	2	2	1	3	2	1	2	4	3	3	3	2	5	5	2	4	3	2	1	4	4	2	2	4	2	4	2	3	2	3	4	3	3	4
58	44	2	3	4	3	2	2	2	2	2	3	4	3	4	3	3	3	4	3	3	4	2	4	1	3	3	4	2	4	2	2	3	3	4	3	4	3	2	4
59	28	1	3	4	2	4	4	3	2	4	3	2	5	4	4	1	3	5	3	3	2	3	3	3	3	2	2	3	3	4	3	4	2	2	2	4	2	3	4

				Variable 1																		Variable 1																	
				D1						D2						D3						D4						D5						D6					
				I1		I2		I3		I4		I5		I6		I7		I8		I9		I10		I11		I12		I13		I14		I15		I16		I17		I18	
N°	Edad	Sexo	T. Cargo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
60	38	1	2	3	2	4	4	3	2	4	2	1	3	4	5	1	2	3	3	2	3	4	3	3	3	2	4	3	4	3	4	4	3	3	2	4	2	3	4
61	33	1	2	3	2	2	4	1	2	2	3	2	3	3	3	2	1	5	4	2	4	4	2	3	2	3	4	3	2	4	3	4	4	2	2	3	3	3	3
62	27	2	2	3	4	3	2	1	2	3	1	2	5	3	3	2	2	5	5	2	2	4	3	3	3	3	4	2	2	4	4	3	3	2	4	3	3	3	4
63	27	2	3	3	4	4	4	5	3	3	1	2	5	5	4	5	4	5	5	2	4	4	3	1	5	4	5	4	4	4	2	5	4	3	4	4	5	4	4
64	33	2	2	3	2	4	3	3	2	3	1	2	5	4	3	3	1	5	3	3	3	4	3	2	3	3	3	4	4	4	4	4	2	4	4	4	4	2	2
65	30	1	1	2	4	4	4	5	2	3	4	4	5	4	5	4	3	5	4	4	3	4	4	5	3	4	4	2	4	4	5	4	4	2	4	5	4	4	3
66	48	2	1	2	2	2	4	1	2	4	1	2	3	2	3	1	1	3	3	2	1	2	4	1	2	2	3	1	3	4	3	1	2	1	4	2	2	2	2
67	40	1	2	3	2	2	2	1	2	3	1	2	4	2	4	1	1	2	3	2	1	3	3	1	4	3	2	1	4	2	3	1	2	1	3	2	2	1	2
68	31	2	2	3	1	2	2	3	1	4	3	3	4	4	4	3	2	3	5	4	3	2	2	3	2	3	2	4	2	2	2	4	2	3	4	4	2	4	4
69	44	1	3	2	4	3	3	2	3	4	1	4	5	2	5	2	1	3	3	3	2	4	4	3	3	2	2	2	2	4	2	3	3	2	2	2	3	4	3
70	39	2	2	3	3	2	2	3	2	4	1	3	4	4	4	3	2	3	3	4	3	3	3	2	4	4	3	4	4	3	2	5	2	2	2	4	2	4	3
71	31	1	3	2	3	4	2	1	3	4	1	4	5	3	4	1	1	5	3	2	4	4	2	1	4	4	3	2	2	4	3	2	4	3	3	3	2	2	3

Anexo 6: Documento de autorización de la empresa



ITESA
Soluciones de energía

CONSTANCIA

Por medio del presente se da conformidad al Sr. Alberto Bohorquez Salcedo identificado con DNI 44116980 para que se le den las facilidades necesarias para aplicar su estudio de investigación denominado "Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020", asimismo se le permitirá aplicar el cuestionario a cada trabajador dentro de la empresa con el fin de obtener los resultados pertinentes su estudio de investigación. Asimismo se deja en constancia que el investigador compartirá con la empresa los resultados obtenidos con el fin de mejoras en el área de tecnologías de información.

Sin otro en particular.

Gabriela Mendoza Enríquez
GERENTE ADMINISTRATIVO
ITESA

Gabriela Mendoza Enríquez

Jefe Administrativo

Lima, 22 de diciembre del 2020