UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas e Informática

TESIS

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y LOS PROCESOS DE SEGURIDAD INFORMÁTICA EN EL GOBIERNO REGIONAL DE APURIMAC, 2021

Presentada por:

Br. ALEJANDRINA HUAYLLA QUISPE
Br. MARINA VARGAS PANCORBO

Para optar el título profesional de:

INGENIERO DE SISTEMAS E INFORMÁTICA

Abancay- Apurímac - Perú

2022

TESIS

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y LOS PROCESOS DE SEGURIDAD INFORMÁTICA EN EL GOBIERNO REGIONAL DE APURIMAC, 2021

LÍNEA DE INVESTIGACIÓN:

INFORMÁTICA, SOCIEDAD Y GESTIÓN DE CONOCIMIENTO

Asesor:

Mg. EDISON CHICLLA CARRASCO

UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y LOS PROCESOS DE SEGURIDAD INFORMÁTICA EN EL GOBIERNO REGIONAL DE APURIMAC, 2021

Presentado por los bachilleres **ALEJANDRINA HUAYLLA QUISPE - MARINA VARGAS PANCORBO,** para obtener el título profesional de: Ingeniero de Sistemas e informática.

Sustentado y aprobado el 10 de febrero el 2022 ante el jurado:

Presidente : Mg. Soto Palomino Wilfredo

Primer Miembro : Ing. Chávez Vásquez Eduardo

Segundo Miembro : Mg. Maruri Malpartida Nilton

Asesor : Mg. Chiclla Carrasco Edison

DEDICATORIA

Con todo cariño y amor a mi Madre que es mi ángel quien día a día me protege.

De manera especial a mis hijos que durante este tiempo fueron mi fuerza de inspiración para poder superarme, luchar por la vida y darles un futuro mejor, pues sin ellos no hubiera logrado mi desarrollo personal y profesional.

Alejandrina HUAYLLA QUISPE

DEDICATORIA

A Dios por haberme dado la capacidad e inteligencia para desarrollarlo;

A mis padres e hijo por ser mi motivo de superación;

A mis docentes y familiares por su gran apoyo y confianza en mí, que a la vez son mi mayor fortaleza para formarme profesionalmente.

Marina VARGAS PANCORBO

AGRADECIMIENTO

Doy gracias primeramente a Dios,

A mis docentes y asesores de la presente investigación que me enseñaron con gran sabiduría quienes se han esforzado por formarme una buena profesional.

A mis hijos maravillosos e hija por la paciencia que me han tenido durante mis estudios.

Alejandrina HUAYLLA QUISPE

AGRADECIMIENTO

A la Universidad Tecnológica de los Andes porque siguen brindando y apostando por una mejor educación y crear mejores profesionales que contribuyan al desarrollo de nuestro país;

A mis asesores de la investigación y mis docentes por sus conocimientos y hacer posible el logro del presente estudio.

Marina VARGAS PANCORBO

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

GTIC: Gestión de tecnologías de información y comunicación

PSI: Procesos de seguridad informática

UTEA: Universidad Tecnológica de los Andes

GRA: Gobierno regional de Apurímac

DB: Base de datos

TIC: Tecnología de información y comunicación

ERPs: Planificación de recursos empresariales

SGSI: Sistema de gestión de la seguridad de la información

DTIC: Dirección de tecnologías de la información y comunicación

BI: Business intelligence

OTI: Oficina de tecnología de información

CPISI: Escuela profesional de ingeniería de sistemas e informática

CAD: Computer Aided Design

CAM: Computer Aided Manufacturing

RPM: Desarrollo de prototipos y manufactura

SCM: Supply chain management

VPN: Red privada virtual

LAN: Red de área local

SAI: Sistema de alimentación ininterrumpida

RESUMEN

A partir de la realidad problemática de las variables objeto de investigación se esbozó el siguiente objetivo general del estudio, "determinar la relación existente entre la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021.

Es así que la investigación es de enfoque cuantitativo, de tipo básica o fundamental, de nivel o alcance correlacional-descriptivo, de diseño no experimental-transeccional, aplicando el método deductivo y analítico, contando con una población de 82 talentos humanos y el tamaño de la muestra fue de 68 unidades muéstrales determinadas por el método probabilístico y aleatorio simple, considerando como técnica la encuesta e instrumento el cuestionario para la obtención de los datos; de donde por medio la prueba del coeficiente de correlación *r* de Pearson se contrastó la hipótesis de investigación, llegando a concluir que el nivel de relación es significativa, consistente y positiva entre la gestión de las tecnología de información y comunicación, y la seguridad informática en el gobierno regional de Apurímac, 2021, toda vez que el índice *r* de Pearson dio 0.663** y que el *p*-valor logrado de α=0.000 la misma es inferior al nivel de significancia de 1% (p=0.000<0.01), ambiente presentado, latente y frecuente por las inquietudes intrínsecas de los elementos, componentes y factores que sostienen a la gestión de las TIC basadas en la infraestructura, arquitectura, talento humano, conocimientos y las concatenaciones de tecnologías de información y comunicación con el negocio organizacional, las que se encuentran anidadas a las estrategias de afrontamiento operadas para emprender las situaciones, escenarios y contextos de los procesos de confidencialidad, integridad y disponibilidad que exige la seguridad informática para el intercambio, identificación, almacenamiento y envió de información para la toma de decisiones oportunas en cumplimiento a las políticas de seguridad informática y el cambio organizacional regional apurimeña.

Palabras clave: Gestión, tecnologías, información y comunicación, seguridad informática.

ABSTRACT

Based on the problematic reality of the variables under investigation, the following general objective of the study was outlined, "to determine the relationship between the management of information and communication technology and computer security in the regional government of Apurímac, 2021.

Thus, the research is of a quantitative approach, of a basic or fundamental type, of a correlational-descriptive level or scope, of a non-experimental-transectional design, applying the deductive and analytical method, with a population of 82 human talents and the size of The sample consisted of 68 sample units determined by the probabilistic and simple random method, considering the survey as a technique and the questionnaire for obtaining the data; from where, through the Pearson r correlation coefficient test, the research hypothesis was contrasted, concluding that the level of relationship is significant, consistent and positive between the management of information and communication technology, and computer security in the regional government of Apurímac, 2021, since the Pearson r index gave 0.663 ** and that the p-value achieved of $\alpha = 0.000$ is lower than the significance level of 1% ($p = 0.000 < 0.01$), environment presented, latent and frequent by the intrinsic concerns of the elements, components and factors that support the management of ICT based on infrastructure, architecture, human talent, knowledge and the concatenations of information and communication technologies with the organizational business, those that are nested in the coping strategies operated to undertake the situations, scenarios and contexts of the processes of confidentiality, integrity and dis Possibility that computer security requires for the exchange, identification, storage and sending of information for making timely decisions in compliance with information security policies and regional organizational change in Apurimac.

Key words: Management, technologies, information and communication, computer security.

INTRODUCCIÓN

Que hoy día la tecnología de información y comunicación se ha desarrollo de manera que se puede manipular por lo cual las instituciones procesan la información en forma digital a diario, generando costos de producción más bajos y canales novedosos enfocados en los usuarios, con herramientas distintas de internet, vía intranet y entre otros procesos. Donde las TIC se convierten estratégico y su componente significativo para el logro de acciones, sobre todo cambios paradigmáticos que exigen las organizaciones sean competitivas en los diferentes niveles productivos.

Se ha observado la problemática del gobierno regional que existen muchas dificultades de las TIC y seguridad informática que no le dan el valor, sabiendo que en hoy en día se ha convertido en una herramienta indispensable, las instituciones públicas y privadas se encuentran supeditadas al ataque externo de la ciberdelincuencia producto de las vulneraciones que presentan en cuanto la seguridad informática del Gobierno Regional de Apurímac, al uso inadecuado o robo de su data por parte de su personal, corren el riesgo de vulneraciones en sus redes informáticas. Se llegó a evidenciar que existe una preocupación de la variable 1, el responsable no aplica de manera adecuada las estrategias necesarias para la planificación, organización, dirección y control de TIC, que repercute en la eficiencia de los procesos de la seguridad informáticas.

La presente investigación se realizó en el gobierno regional de Apurímac, donde el objetivo es determinar la relación existente entre la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021, se aplicó la metodología correlacional descriptivo donde se midió el grado de asociación existente de las dos variables , con un diseño no experimental-transeccional, al mismo se aplicó como técnica la encuesta y el cuestionario para la obtención de los datos; llegando a concluir que el nivel de relación es significativa, consistente y positiva entre la “gestión de las tecnología de información y comunicación” y la “seguridad informática”.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Realidad problemática

La aplicación y manejo de las tecnologías información y comunicación en los diferentes procesos productivos de bienes y servicios de las empresas, no es un hecho novedoso en sí mismo, la historia económica de las últimos décadas, se encuentra salpicada por diversas manifestaciones de este tipo, como es el caso del desarrollo de los ordenadores, los celulares, las redes informáticas, los dispositivos de almacenamiento, los medios de comunicación, internet, la seguridad informática, redes sociales y sobre todo el desarrollo de las Tecnologías de información y comunicación (TIC).

Por cuanto la incorporación de la tecnología de la información llevaron hoy en día a las organizaciones a salir de sus procesos densos y rutinarios en transformaciones ligeras, generando costos de producción más bajos y canales novedosos enfocados en los clientes, vía las diferentes herramientas de internet, vía intranet y entre otros procesos operativos tecnológicos de comunicación. Donde las TIC se convierten estratégicamente en un elemento significativo para el logro de las actividades corporativas, sobre todo en tiempos de cambios paradigmáticos que exigen a las organizaciones sean competitivas en los diferentes niveles productivos.

El avance de la tecnología de la información y comunicación ha mejorado y transformado la forma de comunicarse, de transmitir y almacenar la información física y digital, actualmente existen sistemas computarizados con mejores funcionalidades que complementadas con el servicio de internet y sus diferentes aplicaciones como son, los campus virtuales, Apps, ERPs, etc. brindan procesos seguros y robustos para la operatividad de los datos en toda organización. (Sancho, 2006, pp. 17-19)

Las transformaciones de las TIC en las organizaciones se pudieron brindar si estas contaban por otro lado con talentos humanos innovadores, quienes generarán cambios sustanciales en la estructura organizacional que les permitirán a las organizaciones contar con más oportunidades, para innovar los procesos de negocios con menos costos. Por cuanto la tecnología hace que las entidades tiendan a interconectar sus procesos operacionales,

automatizar la información, interconexión con sus proveedores, etc., con la finalidad de disminuir sustancialmente sus costos, perfeccionar el tráfico de los materiales y por ende la productividad. Para lograr los cambios en los procesos estas deben estar anidados integralmente en sus distintos componentes tecnológicos, así como la seguridad de la información, debiendo encargarse por implementar las medidas de seguridad con miras a proteger la información y los datos empresariales, que comprenden tanto los de formato electrónico como los impresos en papel. (Morris, 2009, párr. 1)

Por cuanto, en la actualidad las organizaciones se encuentran supeditadas al ataque externo de la ciberdelincuencia producto de las vulneraciones que estas presentan en cuanto a la seguridad de su información, al uso inadecuado o robo de su data por parte de su talento humano e incluso a que la salud de los procesos operacionales intrínsecos y extrínsecos estén en constante riesgo por la presencia de vulneraciones en sus redes informáticas.

Es así, que el estudio en la sociedad de tecnologías de información y comunicación es sumamente importante, toda vez que se hace preciso y forzoso discurrir sobre la problemática de gestión de las tecnologías de la información y comunicación, y de la seguridad informática en el Gobierno Regional de Apurímac-2021; toda vez que se llegó a evidenciar que existe una preocupación referente al grado de la gestión de las tecnologías de información y comunicación, de donde la unidad responsable de tales fines no aplica de manera adecuada las estrategias necesarias para la planificación, organización, dirección y control de sus tecnologías de información y comunicaciones, y que repercute en la eficiencia de los procesos de la seguridad informática, observación generada de tales deficiencias, principalmente por la falta de interés y preocupación referida a las distintas técnicas, dispositivos y aplicaciones responsables para asegurar la confidencialidad, privacidad, integridad y la disponibilidad de los datos de los sistemas informáticos y por ende de los usuarios internos y externos en la entidad objeto de estudio.

Por cuanto, una vez visto de manera general las diferentes aportaciones teóricas acerca de la correlación que existe entre las tecnologías de información y comunicación con los procesos de seguridad informática, y desde las perspectivas teóricas más recientes, se persiguió enfocar en la determinación de la relación existente entre gestión de la tecnología de información y comunicación, y los procesos de seguridad informática en el gobierno

regional de Apurímac, 2021; analizando y describiendo por separado los diferentes componentes que la integran cada uno de los fenómenos en estudio, situación que permitió exponer alternativas para afrontar los retos de acceso a la información de manera oportuna, veraz, segura, eficaz, precisa y en tiempo real, de cómo se las proporcionan a los usuarios y a toda la organización, de su capacidad de comunicación, así como generar un efecto potenciador en los agentes responsables de la entidad, para que puedan asumir mayor número de tareas y romper esquemas tradicionales, al tener más fuentes de información seguras para resolver contingencias sin tener que acudir a terceros e incluso ser capaces de asumir funciones y toma de decisiones para la marcha de la organización que sin las TIC, quedarían fuera de su alcance y estar interconectados con la finalidad de mejorar y contribuir con los principios, fines, objetivos institucionales el de brindar un servicio ágil, seguro y eficiente para el desarrollo de la sociedad apurimeña.

1.2. Planteamiento del problema

1.2.1. Formulación de problemas

En una sociedad globalizada e intercomunicada, donde la comunidad internacional de manera constante ha manifestado que las organizaciones de hoy consideran que las tecnologías de la información y comunicación son herramientas idóneas que impulsan y generan cambios sustanciales. Toda vez que en los países en vías de desarrollo como es el caso del nuestro país, no es productor de tecnología sino mero importador de las mismas.

La TIC, así como la seguridad informática se convierten en herramientas que coadyuvarán a cumplir las estrategias empresariales, más aún hoy en día en la que se encuentran en tiempos de transformaciones, las que exigen a que las organizaciones no sean pesadas, ser más competitivas y ágiles en los diferentes escenarios corporativos y sociedades a nivel integral.

Por cuanto, las organizaciones peruanas deberán enfocar las tecnologías de información y comunicación sobre estos contextos e integrarla como soporte para la productividad y satisfacción de los usuarios. Toda vez que la entidad será más poderosa en la medida en que tenga buenos procesos de la seguridad informática, de las bases de datos tanto de sus usuarios, productos, clientes, así como de otras organizaciones estatales como privadas, que permitirá facilitar y ejecutar innovadores escenarios de negocios, convertirse en una

entidad competitiva y romper la estructura del administrador sedentario a un gerente activo, que se encuentra interconectado para la toma de decisiones en beneficio de la buena marcha competitiva de la organización.

Hoy en día existen diferentes entornos de gestión de tecnologías de información y comunicación en diferentes escenarios empresariales, quienes permitirán reducir la brecha en la necesidad de control, las cuestiones técnicas y riesgos tecnológicos para los procesos de negocio. Además de permitir el desarrollo de políticas de mejora de forma clara y con buenas prácticas de monitoreo de tecnologías de información y comunicación de las instituciones, dichos entornos enfatizara el cumplimiento de las normas que apoyan a la entidad a incrementar el calor de las TIC, sin descuidar de forma reflexiva la seguridad informática, que permitirá establecer de manera oportuna la protección de la información que se llega a generar todos los días para el desarrollo productivo y competitivo empresarial, permitiendo la alineación y simplificación del marco de gestión de dichas tecnologías y analizar la relación con los procesos de la seguridad informática en la entidad objeto de estudio.

1.2.2 Problema General

¿De qué manera la gestión de tecnología de información y comunicación se relacionan con la seguridad informática en el gobierno regional de Apurímac, 2021?

1.2.3 Problema Específicos

1. ¿Cuál es el nivel de relación de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021?
2. ¿Cuál es el grado de asociación de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021?
3. ¿Cuál es el nivel de relación de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021?

4. ¿Cuál es el grado de asociación de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021?

1.3 Justificación

La presente investigación se desarrolló con el propósito de conocer la realidad de la gestión de la tecnología de información y comunicación y de los procesos de seguridad informática que se ejecutan en la entidad objeto de estudio, siendo de mucha significancia para diseñar acciones base para el manejo eficiente de las TIC y de los niveles de seguridad que se debe ejecutar en los procesos informáticos con miras a desarrollar efectivas toma de decisiones en las diferentes unidades organizacionales del gobierno regional de Apurímac.

1.3.1 Justificación social

La investigación se enfocó en la observación de los elementos determinantes del nivel de conocimientos y del empleo de los sistemas y procesos operacionales de las tecnologías de información y comunicación, y la concordancia que existe en los procesos de la seguridad informática que se encuentra implantada en el gobierno regional de Apurímac, 2021; escenario que les concederá a los ejecutivos del gobierno regional y unidades funciones de influencia a establecer un análisis, diseño, desarrollo, implementación e implantación de herramientas necesarias y suficientes para erradicar los cuellos de botella en el tratamiento, almacenamiento y sobre todo en la seguridad informática para el tratamiento de la información de forma oportuna, confiable, verídica, concisa e integral a través de las tecnologías de información y comunicación con las que cuenta la entidad en la búsqueda de sus fines, objetivos y desarrollo de la comunidad apurimeña.

1.3.2 Justificación teórica

Para la ejecución del presente estudio se consideró todos los principios y exigencias teóricas asentadas y enmarcadas a partir de los enfoques pertinentes de los fenómenos en investigación, la que permitió dar a luz y conocer de manera objetiva la situación real, latente del escenario y los procesos operativos de la gestión de tecnología de información y comunicación y de los procesos de seguridad informática en el gobierno regional de

Apurímac, 2021. Escenario que permitió identificar los eventos determinantes en las TIC y del nivel de asociación que puedan tener con cada una de las dimensiones de los procesos de seguridad informática para orientar y diseñar mejoras necesarias y eficientes para un mejor desempeño productivo en el tratamiento de los datos por parte de los actores y unidades operativas en la entidad objeto de estudio.

1.3.3 Justificación metodológica

La conveniencia metodológica del presente estudio permitió brindar información sobre la importancia que tiene en su entorno real la gestión de las tecnologías de información y comunicación, y de los procesos de la seguridad informática que se encuentran implantados y se ejecutan en la entidad objeto de estudio por parte de las unidades responsables y los usuarios internos y externos de la institución. Escenario que permitió constituir un modelo de análisis descriptivo y establecer un procedimiento metodológico de concordancia entre las variables en investigación al establecer el grado de relación entre los fenómenos investigados y brindando un contexto real, preciso y significativo para que los talentos humanos de los diferentes niveles organizacionales puedan mejorar el trabajo productivo, toda vez que la información que generan, manejan, almacenan y distribuyen intrínsecamente y extrínsecamente constantemente se encuentra supeditadas a los ataques de los ciberdelincuentes, quienes continuamente pueden jaquear, vulnerar o haciendo phishig a la Data de las organizaciones. Así mismo llegar a concientizar en temas de políticas de seguridad informática referente a su confidencialidad, integridad, privacidad y disponibilidad para que se llegue a generar estrategias de aseguramiento en la atención eficiente del cliente y usuario de la entidad.

1.3.4 Justificación práctica

El presente estudio se ejecutó porque existió la necesidad de llegar a determinar la realidad actual de la gestión de las TIC y su nivel de asociación con los procesos de seguridad informática en el gobierno regional de Apurímac, 2021, la misma que generó la examinación y descripción de manera práctica los factores responsables en la generación de los cuellos de botella existentes para una efectiva gestión de los fenómenos en estudio, de donde se diseñó estrategias y modelos en mérito a la realidad en que la información se llega a incrementar exponencialmente en la entidad en estudio, resaltando

el comportamiento y las buenas prácticas del talento humano quienes cumplen el desarrollo de sus funciones encargadas sobre la operatividad de las TIC y los procesos de seguridad informática en cumplimiento de los fines y objetivos de la organización.

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

Determinar la relación existente entre la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021.

1.4.2 Objetivos Específicos

1. Determinar el nivel de relación de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021.
2. Determinar el grado de asociación de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021.
3. Determinar el nivel de relación de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021.
4. Determinar el grado de asociación de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.

1.5. Delimitación de la investigación

1.5.1 Espacial

La investigación se llegó a desarrollar en las dependencias del gobierno regional de Apurímac, ubicada en el Jirón Puno N° 107, de la ciudad de Abancay, Provincia de Abancay.

1.5.2 Temporal

El ciclo de ejecución de la investigación fue desde mayo hasta noviembre de 2021.

1.5.3 Social

En el estudio participaron como unidades muéstrales los talentos humanos pertenecientes a las diferentes unidades directorales ejecutivas, la subgerencia de desarrollo institucional, estadística e informática y la unidad de tecnologías de información del gobierno regional de Apurímac.

1.5.4 Conceptual

La misma que estuvo basada en las bases teóricas y conceptuales de los fenómenos estudiados, que permitieron analizar y describir oportunamente la realidad latente y en su ambiente único de la gestión de las TIC y la seguridad informática que se establecieron en la entidad objeto de estudio. Por cuanto fue importante analizar las TIC que permiten desarrollar los procesos operacionales de manejo de la información veraz, precisa y en tiempo real, del cómo se estaban proporcionando las mismas a los usuarios de la institución y a toda la organización para poder determinar el nivel de asociación que pueda existir con la seguridad informática, la misma estuvo direccionada a observar la correcta seguridad en la entidad, bajo el personal experto en tecnologías informáticas capaces para predecir las amenazas y los riesgos a los sistemas de información internos de la entidad regional de Apurímac.

1.6. Viabilidad de la investigación

La investigación de acuerdo a la significancia para el desarrollo productivo eficiente y eficaz de la entidad objeto de investigación estuvo enmarcado en su viabilidad, toda vez que contó con los recursos tangibles e intangibles suficientes desde la fase inicial hasta la culminación de la misma.

De donde, la viabilidad económica partió de la recopilación de elementos cuantitativos, que permitió determinar los aspectos monetarios suficientes para favorecer la inversión para la concreción de los materiales y la tecnología necesarios que se adapten a las exigencias de la investigación.

Además, la viabilidad social estuvo ceñida a la aplicación de un cuestionario a los talentos humanos de las unidades del gobierno regional de Apurímac, para capturar datos de manera oportuna de los fenómenos objeto de estudio y llegar a determinar la existencia de una correlación entre estas.

De otra parte, la viabilidad técnica fue basada en la optimización de los recursos y el equipo participante para la realización de la investigación a partir de la captura de datos de la entidad en estudio y efectuar un análisis robusto sobre el nivel de asociación que existe entre la gestión de tecnologías de información y comunicación, y los procesos de seguridad informática la seguridad, escenario fundamental para la iniciación del presente estudio.

1.7 Limitaciones

Se consideraron todas las contingencias que se presentaron durante todo el proceso de ejecución de la investigación, las mismas que generaron ciertos retrasos antes y durante el desarrollo de la misma, de las cuales se puede citar:

- Restricciones de acceso a las instalaciones de la organización objeto de estudio, por el estado de emergencia sanitaria y el aislamiento social que el país se encuentra viviendo por efecto del COVID-19.
- Demora en la atención y aprobación del documento para la ejecución y aplicación de los instrumentos por parte de la autoridad competente del gobierno regional de Apurímac.
- Existencia escasa de revistas, artículos científicos y materiales bibliográficos relacionados a las variables en nuestra localidad.
- Retardada participación del talento humano de las unidades consideradas de la entidad de influencia, para el empleo de los cuestionarios.
- Poca predisposición y disponibilidad de tiempo de los directivos y responsable de administrar las tecnologías de información y comunicación y de la seguridad informática del gobierno regional de Apurímac.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de investigación

2.1.1 A nivel internacional

Considerando la investigación de Lino, Quimi y Loraine (2019), *"Las tecnologías de información y comunicación (tic) y su influencia en la administración de las pequeñas empresas del ecuador 2017-2018"*. Tesis de pregrado. Universidad de Guayaquil, Guayaquil-Ecuador. Cuyo objetivo: analizar la magnitud de la influencia de la falta de aplicación de las TIC en la administración de las pequeñas empresas en la parroquia Tarqui de la ciudad de Guayaquil-Ecuador. La metodología: investigación con diseño experimental, descriptivo y explicativo. Cuyos resultados fueron; que el uso de las TIC ayudará a las empresas a obtener mejor gestión administrativa en el negocio con la finalidad de tomar decisiones eficientes para la maximización del recurso en las pequeñas empresas. Llegando a concluir, que las pequeñas empresas necesitan incorporar como estrategia para expansión de su negocio las tecnologías, siendo la única manera para mantenerse en el mercado competitivo. Además los gerentes de las pequeñas empresas se ven interesados en el cambio y la aplicación de nuevas estrategias para el negocio, en el cual aceptan que la implementación de un sistema CRM permitirá realizar un seguimiento de todas las actividades (p. 50).

A partir de Guevara (2017), en su investigación de grado titulado *"Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnologías de la información y comunicación del distrito 18D01 de educación"*. Universidad Técnica de Ambato, Ambato-Ecuador. Estableciendo el objetivo: Implementar un Sistema de Gestión de Seguridad de la Información bajo parámetros de las normas ISO/IEC 27001. Cuya metodología: modalidad de campo y documental – bibliográfica. De donde los resultados fueron: que la entidad estudiada no cuenta con la documentación específica de las políticas de seguridad, aplicando, únicamente se aplican ciertas normativas para gestionar la información las cuales no son suficientes para garantizar que la información esté asegurada. Al final llega a la conclusión: que la entidad estudiada no cuenta con procesos orientados a salvaguardar la información, donde las

actividades que llegan a emprender sobre la seguridad de los datos son tan sólo correctivos generándose un desperdicio de recursos para entidad educativa (p. 86).

Así mismo Camargo (2017), en la investigación titulada *"Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil - CNSC basado en la norma ISO27000 e ISO27001"*. Universidad Nacional Abierta y a Distancia, Bogota D.C.-Colombia. Donde el objetivo fue: Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27000 e 27001 para mejorar la seguridad de las tecnologías de información y las comunicaciones (TI's) en la Comisión Nacional del Servicio Civil (CNSC). Aplicando la metodología: de investigación de campo y línea enfocada a la gestión de la seguridad y la seguridad de la información. Llegando a los resultados: que el área de informática se encuentra implementando procesos para mejorar el nivel de seguridad de la información, se determinó que no existe documentación referente a estos procesos, además el estado actual de la seguridad de la información, se encuentra en estado medio, ya que el personal lleva a cabo el trabajo, acatando buenas practicas, pero no existen procesos claros que permitan establecer roles y responsabilidades en los empleados de la entidad. Al final concluye: que el área informática tiene procesos establecidos, políticas implementadas, activos de información, pero no cuentan con la respectiva documentación y directriz para la ejecución de estas, así mismo sostiene que el recurso humano de la entidad, es uno de los riesgos más altos para la seguridad de la información, ya que si no se tienen buenas prácticas y una divulgación acertada sobre la seguridad informática, la entidad puede tener un nivel alto de vulnerabilidad (p. 102).

De otra parte Muñoz (2016), en su trabajo de investigación *"Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la Universidad de Cuenca",* Ecuador. Cuyo objetivo fue: Analizar las políticas de seguridad Informática para la DTIC, en base a la Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27002:2009. Además la metodología utilizada: basada en el método de análisis de las normas y de las políticas de seguridad informática internacional ISO 27002. Obteniendo los resultados: los dominios de mayor resultados son los relacionados con "7. Gestión de Activos", "10. Gestión de comunicaciones y Operaciones", "11. Controles de Acceso", "14. Gestión de la

continuidad del Negocio", gracias a los procesos considerados en la DTIC. Así mismo los dominios con bajo cumplimiento son los asociados a: "5. Políticas se Seguridad", "15. Cumplimiento", por la falta de políticas de seguridad y del seguimiento adecuado hasta llegara a su cumplimiento. Sosteniendo las conclusiones siguientes: que la seguridad informática se encuentra en un 52 % de acuerdo según los 11 dominios de seguridad de la norma ISO 27002, además existen controles con 0% por la naturaleza de la entidad educativa. Señalando además que la falta de políticas de seguridad informática, lo que conlleva a una falta de revisión y verificación del cumplimiento, adicionalmente existe algunos inconvenientes con la seguridad física y del entorno, la falta de seguridades en las puertas de acceso en las oficinas de la DTIC en el horario de trabajo (pp. 63-65).

De otra parte Ochoa (2015), en su estudio *"Implementación de las tecnologías de la información y la comunicación TIC para la mejora de la gestión contable y financiera en la empresa Fundimetales"*. Universidad Pedagógica y Tecnológica de Colombia, Tunja Boyacá-Colombia. En donde se tuvo como objetivo: Diseñar un análisis de costos que soporte la implementación de las Tecnologías de la Información y la Comunicación, facilitando información relevante para la toma de decisiones y como base en el manejo de la información contable y financiera y en la mejora de los procesos operativos. Cuya metodología fue: estudio exploratorio y descriptivo. De donde los resultados: existe ausencia de estructuración y sistematización de los procesos; se hace necesario para la organización de cada proceso, la puesta en marcha de las TIC. Arribando a la conclusión: que la empresa Fundimetales no cuenta con un sistema contable, peor aún de costos, lo que no permite obtener resultados claros, precisos y la fijación del precio de venta en el producto final, pero con la implementación del sistema de costos por órdenes de producción se espera poder solucionar todos estos fallos en la empresa, además el departamento de contabilidad es deficiente por cuanto el personal no recibe los datos de los distintos departamentos en forma oportuna, no existiendo funciones definidas de trabajo en ningún departamento, lo que causa mala organización y no hay responsabilidad del personal, al final señala que la falta de un sistema contable computarizado adecuado, no permite obtener información precisa e inmediata, lo que

dificulta la toma de decisiones oportunas que beneficien al desarrollo sostenido de la empresa (p. 89)

2.1.2 A nivel nacional

Considerando la investigación de Machicao (2019). *"Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) –UNA Puno 2018"*. Universidad Nacional del Altiplano, Puno-Perú. Bajo el objetivo: Analizar los riesgos para proponer políticas de seguridad de la información para la oficina de tecnologías de información (OTI) UNA-Puno. Aplicando la metodología: de una investigación experimental. Llegando a los resultados: donde el 40% del activo de base de datos presentan un rango de 3-5 de confidencialidad, integridad y disponibilidad de la información. Concluyendo que existen 12 riesgos de nivel alto, 28 riesgos de nivel medio y 151 riesgos de nivel bajo, siendo varios los criterios respecto a las amenazas que vulneran la información que administra la OTI. Así mismo, las existencia de políticas de seguridad de la información coadyuvará con los controles de seguridad del manejo, almacenamiento y distribución de la información (p. 81).

De otra parte en la investigación realizada por Ancajima (2019), titulada: *"Propuesta de implementación de seguridad informática en las TIC de la I.E. San Miguel Arcángel, Catacaos-Piura; 2016"*. Universidad Católica los Ángeles Chimbote, Piura –Perú. Planteando el objetivo: Estudiar los riesgos que se tiene en la institución y proponer la implementación de Seguridad Informática de la I.E estudiado. Utilizó la metodología: investigación fue cuantitativa, de nivel descriptivo, con diseño no experimental - transversal. Donde los resultados fueron: el 75.00% manifestaron encontrarse satisfechos con las TIC en el proceso de enseñanza, el 73.00% están satisfechos con la formación y capacitación de las TIC y el 73.00% señalan satisfacción con la seguridad Informática en las TIC de la entidad. Concluyendo: que las políticas de seguridad y manejo de los datos permitirán mayor seguridad informática, donde docentes, alumnos y personal administrativo se encuentren satisfechos en el momento de utilizarlas (p. 119).

Por su parte Salazar (2019), en su investigación *"Gestión de calidad con el uso de tecnología de información y comunicación y propuesta de mejora en las micro y pequeñas empresas, sector comercio, rubro ferretería, ciudad de Juanjui 2019"*.

Universidad Católica los Ángeles Chimbote, Perú. Con el objetivo: determinar las principales características de Gestión de calidad con el uso de Tecnologías de información y comunicación en las instituciones en estudio. Aplicando la metodología: investigación de diseño no experimental-transversal. Arribando a los resultados: el 46.15% no conocen el término gestión de calidad, y que el 53.85% no conocen el significado de las TIC, por cuanto la mayoría de las Micro y pequeñas empresas no aplican la gestión de calidad con el uso de las TIC, tan solo se limitan a usar el teléfono para coordinar las actividades de las empresas (p. 37).

En la investigación de Ortiz (2018), titulado *"Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de seguridad de la información en la universidad nacional Agraria de la Selva"*. Universidad Nacional Agraria de la Selva, Tingo María-Perú. Cuyo objetivo fue: Implementar de forma incremental la Norma Internacional ISO/IEC 27002:2013 en la universidad objeto de estudio. Aplicando la metodología: bajo la investigación aplicada, de diseño cuasi-experimental, de carácter prospectivo longitudinal. Arribando a los resultados: que el 15% los controles que se encuentran en un nivel de madurez inicial, el 51% de madurez repetible, el 26% con un nivel de madurez definido, solo 8% con controles de madurez gestionado. Al final concluye: que existe un 95% de nivel de confianza producto de la implementación de controles de seguridad de la norma ISO/IEC 27002:2013, las mismas que permitirán mejorar la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva.

Por su parte Guaylupo (2017), en la investigación de posgrado titulado *"Solución holística de seguridad informática para mejorar la gestión de las tecnologías de la información y comunicación, en la dirección regional de educación de Piura, departamento de Piura en el año 2016"*. Universidad Católica los Ángeles de Chimbote, Piura-Perú. El objetivo fue: implementar una solución holística de seguridad informática para mejorar la gestión de las tecnologías de información y comunicación. Cuya Metodología utilizada: bajo una investigación aplicada, descriptiva, de diseño no experimental, de enfoque cuantitativo. De donde los resultados se tiene: que la seguridad informática un 42,9 % se encuentra en desacuerdo sobre la existencia de políticas de seguridad de la información en la DREP, por otro lado, un 14,3 % se encuentra de

acuerdo, de donde se determina que la políticas de seguridad informática no son conocidas por los funcionarios o no existe una declaración formal. Además se aprecia que el 57,1 % se encuentra en desacuerdo; respecto a si se cumplen las políticas de seguridad de información en la DREP; además un 14,3 % manifiesta no estar ni de acuerdo ni en desacuerdo, deduciendo que en la DREP no se cumplen las políticas de seguridad, quizá por falta de conocimiento. Llegando a la conclusión: que la entidad objeto de estudio contiene variados inconvenientes para el manejo de su información, a consecuencia de la falta de identidad y conocimiento sobre la importancia de asegurar la información existente, la carencia de políticas que normen las prácticas adecuadas en cada uno de los procesos, transacciones y recursos asociados con el manejo de la información (p. 95).

2.1.3 A nivel regional y local

Huamán (2018), en el estudio titulado *"Modelo de gestión de seguridad de la información con ISO/IEC 27001 para minimizar la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2018"*. Universidad Nacional José María Arguedas, Andahuaylas-Perú. Planteo el objetivo: minimizar la vulnerabilidad de la información a la que está expuesta la institución estudiada. Aplicando la metodología: de enfoque cuantitativo, pre experimental, tipo aplicada y nivel explicativo. Llegando a los resultados: que el estado de la divulgación de la información minimizó significativamente en un 78.64% después de la aplicación del MGSI en la entidad municipal, el 16.67% sostienen que la divulgación de la información es alta antes de la aplicación del MGSI. Concluyendo: que hay una minimización de la vulnerabilidad de la información de manera significativa, ya que se determinó una variación positiva de 56,04% respecto a la disminución de la vulnerabilidad de la información, además existe una variación positiva de 62,07%, afirma que la divulgación de la información se minimizó significativamente, por otro lado en la minimización de la alteración de la información con la implementación del MGSI se obtuvo un resultado significativo positivo de 53,03%, lo cual indica que la alteración de la información minimizó significativamente, y por último, en la minimización de las amenazas de la información también se obtuvo una variación positiva de 53,12%, lo cual indica que la

aplicación del MGSI para la minimización de las amenazas de la información es importante (p. 50).

2.2 Bases Teóricas

2.2.1 Gestión de tecnologías de información y comunicación

La gestión de tecnologías de información y comunicación (GTIC), "son aquellas herramientas de gestión computacional e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información variada, a través de un conjunto de herramientas, soportes y canales para el tratamiento eficiente al interior de las organizaciones". (Huidobro, 2007, p. 2)

De otra parte de acuerdo a las manifestaciones de Jiménez (2019):

> La tecnología de información y comunicación (TIC) son "el resultado de poner en interacción la informática y las telecomunicaciones, todo con el fin de mejorar el procesamiento, almacenamiento y transmisión de la información" (párr. 1)

Por cuanto la GTIC, "son las tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información". (Daccach, s.f., p. 1)

2.2.1.1 Importancia de las tecnologías de información y comunicación.

La importancia que tiene las TIC para las empresas y sobre todo para la toma de decisiones los gerentes debe tener conocimientos sobre las tecnologías. Tal es así que para Martín (s.f.), las TIC presentan una gran importancia para las empresas:

- Están cambiando la forma de realizar las actividades y administrar sus recursos.
- Presenta elementos clave, para que el trabajo y desarrollo empresarial sea más productivo.
- Tiende agilizar la comunicación de la organización.
- Sostiene el trabajo sinérgico.
- Promociona en el mercado los productos.

- Incrementa la productividad empresarial.
- Presencia de la comunicación asertiva mediante las redes sociales (párr. 1).

2.2.1.2 Componentes de las tecnologías de información y comunicación

Según Cortés (2018), las tecnologías de información y comunicación (TIC), derivan de tres hechos fundamentales (párr. 1), las mismas son:

- Un soporte físico común compuesta por la microelectrónica; denominada hardware, se encuentra en todos las funcionalidades del proceso de información, la comunicación, almacenamiento y registro.
- Del software (SW); por su gran componente es incorporado a los productos, se encuentra en todas las funcionalidades del proceso de la información, sobre todo en el tratamiento de la misma.
- De la infraestructura de comunicaciones; permiten la distribución (deslocalización) de los distintos elementos de proceso de la información y asegurar la seguridad, calidad, inexistencia de errores, rapidez, etc. (Cortés, 2018, párr. 1)

2.2.1.3 Clasificación de las tecnologías de información y comunicación.

Marqués (2000), llega a señalar que se debe contemplar a todas las redes de comunicación sociales interpersonales (teléfono o el fax y entre otros) dentro de la clasificación de las tecnologías de información y comunicación. (párr. 1). Siendo la base posible de tres grandes grupos:

- Las redes: comprenden telefonía fija y móvil, televisión (digital, satélite…), banda ancha y otros.
- Las terminales: engloban equipos informáticos, vídeos, bluray, mp3-4-5, terminales móviles, televisores, las consolas, entre otras.
- Los servicios TIC: comprenden los buscadores, navegadores, banca y comercio electrónico, administraciones públicas, servicios de educación y salud, los blogs, entre otras. (Marqués, 2000, párr. 1)

2.2.1.4 Las tecnologías de información y comunicación en las empresas.

Ca' Zorzi (2011), señala a nivel empresarial se advierten aplicaciones basadas en las TIC que permiten sostener servicios de inteligencia de mercados, sistemas de posicionamiento e información geo-referenciada, procesos de gestión de la relación con usuarios-clientes, sistemas de control, tecnologías para certificar la calidad, inteligencia competitiva, automatización industrial, sistemas para la toma de decisiones y entre otros elementos y herramientas implementadas en las organizaciones con la finalidad de ser cada vez más competitiva (p. 16).

De donde, la manera que son aplicadas las TIC por las organizaciones se las puede diferenciar entre un uso infraestructural o genérico y/o el especializado. (Ca' Zorzi, 2011, p. 16), de donde:

a. Uso infraestructural o genérico: referida a la tecnología que maneja funciones de comunicación audio-visual (telefonía fija, móvil o VOIP), la comunicación escrita (e-mail, SMS, chat). (Ca' Zorzi, 2011, p. 16)

b. El uso especializado: producto de las TIC las organizaciones se benefician, gracias a las soluciones de apoyo a los diferentes procesos internos y externos de negocio relacionados a su cadena de valor. Como ser: a). en la gestión estratégica, b) en el soporte a la gestión empresarial y/o (BI), c) en la gestión financiera y/o (ERP), d) en la producción y/o RPM, e) en la gestión de la cadena de suministro (SCM), e) en la gestión de clientes, f) en la promoción de la empresa por la web, g) en los canales de venta por internet (B2C) o (B2B), h) en la distribución, i) en el comercio exterior, j) en el área de recursos humanos, y k) en la infraestructura tecnológica de la organización**.** (Ca' Zorzi, 2011, p. 17-18)

2.2.1.5 Dimensiones de tecnología de información y comunicación.

De acuerdo a las experiencias de Rodríguez y Peña (2012), quienes expresan que el constructo de las TIC se examina de manera integral en cinco dimensiones (p. 54), conformado por:

> Objetos de las TIC como el hardware, software y personal de soporte; conocimiento en TIC como la comprensión de la organización sobre los

> objetos y las operaciones de las TIC, como la medida en la cual la organización utiliza la tecnología de información y comunicación para la gestión del mercado y de la información de sus clientes (Rodríguez y Peña, 2012, p. 54).

De otra parte y desde otra perspectiva los recursos humanos se consideran como una dimensión separada de los objetos agrupándose con el conocimiento de las TIC y resaltando el aspecto de las relaciones de la TIC dentro y fuera de la organización. (Zhang, Sarker y McCullough, 2008) citado por (Rodríguez y Peña, 2012, p. 54)

Donde los anteriores autores manifiestan:

a. Dimensión de infraestructura; comprende el hardware, software y las tecnologías de comunicación que se encuentran implementadas en la empresa, incluyendo el colaborador técnico y humano de las TIC. De donde toda infraestructura sostiene los elementos sustanciales para la edificación de los procesos de negocio y la capacitación al talento humano, basados en la conectividad, compatibilidad y modularidad de los recursos físicos y la competencia del talento humano de la TIC. (Zhang, Sarker y McCullough, 2008) citado por (Rodríguez y Peña, 2012, p. 55)

b. **Dimensión de arquitectura;** constituye las exigencias de la TIC, incluyéndose a los dispositivos de datos, las aplicaciones, la conectividad y la compatibilidad de los equipos de cómputo. (Zhang, Sarker y McCullough, 2008) citado por (Rodríguez y Peña, 2012, p. 55).

c. **Dimensión de talento humano;** comprende al equipo de trabajo de la TIC, donde las habilidades de los mismos permitirá resolver contingencias del negocio integrales con la participación de las TIC y llegara a dirigir las oportunidades para el crecimiento competitivo y activos clave organizacionales. (Zhang, Sarker y McCullough, 2008) (Rodríguez y Peña, 2012, p. 55)

d. **Dimensiones de conocimiento;** comprende el nivel de entendimiento de las TIC, partiendo de los procesos operativos y objetivos estratégicos de la organización, así como entender las necesidades, habilidades y capacidades de las tecnologías de información y comunicación latentes y emergentes integrales con el negocio. (Crawford et al., 2011) citado por (Rodríguez y Peña, 2012, p. 56)

e. **Dimensión a las relaciones de la TIC con el negocio;** la concatenación de las TIC con el negocio, donde debe existir una agradable comunicación entre las dos partes en la organización, quienes deben compartir los riesgos y la responsabilidad en el tratamiento de la TIC. (M. Zhang, Sarker y McCullough, 2008) citado por (Rodríguez y Peña, 2012, p. 56)

2.2.2 Seguridad informática

Para la Universidad internacional de Valencia (VIU, 2018), la seguridad informática constituye:

> "El proceso de prevenir y detectar el uso no autorizado de un sistema informático" (párr. 1).

Por su parte Gómez (2017), señala que la seguridad informática se la puede considerar como:

> "Las medidas que impiden la ejecución de operaciones no autorizadas sobre un sistema o red informática, para evitar posibles daños a la información y comprometer su confidencialidad, autenticidad, disponibilidad o integridad" (p. 40).

De otro lado, según la norma ISO 7498, la seguridad informática consiste en "una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización". (Gómez, 2017, p. 42)

Según Aguilera (2011), la seguridad informática es la disciplina encargada de:

> "Plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad" (p. 15).

2.2.2.1 Importancia de la seguridad informática.

Muchas acciones del día a día en el uso de la tecnología obedecen a garantizar la seguridad informática en todo el proceso y canal que siguen los datos, de ahí la significativa importancia de la seguridad informática en los procesos del manejo de la información (VIU, 2018, párr. 1), como:

- Los datos deben permanecer seguros y protegidos confidencialmente

- La prevención del robo de información; las bases de datos, números de cuentas bancarias, tarjetas de crédito, contraseñas, entre otras.
- En la comunicación; por medio de las comunicaciones los datos presentes en un computador puede ser utilizados de mala manera por usuarios sin la autorización respectiva.
- Contra intrusos; estos pueden llegar a cambiar y/o modificar los códigos fuente de los programas, así como utilizar imágenes o cuentas de correo electrónico no verídicas para crear contenido perjudicial al usuario propietario.
- Contra los ciber-delincuentes; quienes pueden acceder a las computadoras con maliciosas intenciones y/o dañar otros equipos o sitios web o redes para generar caos.
- Contra hackers; quienes llegaran a paralizar la operatividad del sistema informático, propiciando pérdida de información, las fallas de servidores y por ende no poder acceder a la Web.
- Contra el ataque de los virus como troyanos, gusanos, etc.
- Contra suplantación y/o espionaje por medio de las redes sociales. (VIU, 2018, párr. 1)

2.2.2.2 Clasificación de la seguridad informática.

Lo que debe contemplar la seguridad informática se puede clasificar en tres partes (Romero et al., 2018, p. 14), como:

- Usuarios; son las personas que muchas veces es imposible de controlar, toda vez que estos pueden cometer un error y olvidar algo o tener un accidente, donde este acontecimiento puede generar perdida del trabajo desarrollado por mucho tiempo.
- Información; es la más significativa de toda seguridad informática, la misma que debe que debe garantizar su protección para que este a salvo de terceros y ajenos a esta.

- Infraestructura; es uno de los elementos más controlados y dependerá de los procesos que se manejan. (Romero et al., 2018, p. 14)

2.2.2.3 Objetivos de seguridad informática.

Para Gómez (2017), los objetivos de la seguridad informática se encuentran basados en buscar:

- Minimizar y gestionar riesgos, la detección de probables contingencias y amenazas a la información.
- Llegar a garantizar el adecuado uso de los recursos y aplicaciones de todo sistema informático.
- Llegar a limitar las pérdidas y conseguir satisfactoriamente la recuperación del sistema informático cuando se produzca una contingencia en la se seguridad.
- Cumplimiento del marco legal y requisitos asignados por los clientes en sus respectivos contratos. (Gómez, 2017, p. 44)

2.2.2.4 Factores de seguridad informática.

La seguridad informática para un sistema informático dependerá de diversos factores según Gómez (2017), entre ellos se tiene:

- La sensibilidad de las autoridades y/o responsables de la empresa; los que deben considerar y ser conscientes de la gran necesidad de presupuestar recursos para este fin.
- La formación y asunción de responsabilidades; de los usuarios y/u operadores de las aplicaciones informáticas.
- Las limitaciones de asignación de permisos y privilegios a los usuarios.
- La adecuada instalación, configuración y mantenimiento de los equipos tecnológicos e informáticos.
- El soporte técnico por parte de los fabricantes de hardware y software (p. 43).

2.2.2.5 Tipos de seguridad informática.

Para Molinetti (2019), existen distintos tipos de seguridad informática, de cómo se emplean e importancia para las organizaciones (párr. 1), siendo los tipos siguientes:

a. La seguridad de la red; es la protección de información -como documentos, datos personales, bancarios y contraseñas- en Internet, evitando vulneraciones como -suplantación de identidad, de software espía, phishing, virus, etc.

Por cuanto la seguridad en la red más usados en las empresas, estos son algunos mecanismos:

- Los antivirus: son programas para proteger la información de las computadoras de ataques de virus, troyanos y/o worms.
- Los antispyware: son programas para que un tercero no robe la información confidencial del ordenador.
- Las redes privadas (VPN): es toda estructura de red que posibilita la extensión de la red interna (LAN) hasta la red pública (Internet). (Molinetti, 2019, párr. 1)

b. La seguridad del software; la protección de las aplicaciones de ataques maliciosos pueda ser por un antivirus una opción adecuada, pero la seguridad informática exige soluciones más precisas y específicas, como:

- Los cortafuegos (firewall): controla el tráfico de datos en una red. Por ejemplo: Application Gateway, Packet Filter, Proxy Server, etc.
- El software de filtración de contenidos: opera como tamiz para los usuarios que tienen acceso a Internet, asistiendo a la protección de amenazas de phishing.

c. La seguridad de hardware; se llega considerar:

- Los cortafuegos de hardware: dispositivo físico que se conecta al router, permitiendo el bloquea de las conexiones potencialmente dañinas.

- Los servidores proxy: es un equipo dedicado (puede ser un SW) actuando de canal entre el computador y un servidor determinado.
- El Sistema de Alimentación Ininterrumpida (SAI) o UPS; suministra electricidad a los equipos tecnológicos cuando existe falencias en el suministro para utilizar durante un tiempo determinado y poder almacenar adecuadamente los datos. (Molinetti, 2019, párr. 1)

2.2.2.6 Dimensiones de la seguridad informática.

Es fundamental hacer notar y de mucha significancia que tanto los datos, equipos y toda la tecnología implementada deben permanecer seguros y protegidos contra diferentes escenarios adversos en toda empresa (VIU, 2018, párr., 1), de ahí se consideran cuatro dimensiones principales que cubre la seguridad informática:

De donde para la VIU (2018), las dimensiones principales son:

a. Los procesos: Son operaciones de seguridad apropiados para gestionar el riesgo y mejorar la seguridad informática. Al mismo son medidas técnicas que garanticen el material de seguridad de información con el objetivo de mitigar riesgos tales como pérdida o filtración de información.
b. La confidencialidad: donde todos los usuarios y/u operadores que son autorizados tienen derecho a acceder a los recursos, datos e información de la organización.
c. La integridad: consiste en que los usuarios autorizados son los únicos que pueden llegar a modificar los datos siempre y cuando sea necesario.
d. La disponibilidad: cuando los datos se encuentran disponibles sólo para los usuarios autorizados y cuando estos lo requieran (párr. 1).

2.3. Marco conceptual

Gestión de tecnología de información y comunicación (TIC)

Son “herramientas de gestión computacional e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información de la más variada, a través de un conjunto de herramientas, soportes y canales para el tratamiento eficiente de la información al interior de las organizaciones”. (Huidobro, 2007, p. 2)

Seguridad informática

"Es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática". (Gómez, 2017, p. 40)

Almacenamiento de datos

Kilburn (2015), considera que el almacenamiento de datos se refiere "al uso de medios de grabación para conservar los datos utilizando PC y otros dispositivos, estos pueden estar en archivos, en bloque y el almacenamiento de objetos, cada uno de los cuales resulta adecuado para un fin diferente".

Base de datos

Es un conjunto de contenidos de información estructurados y organizados sistemáticamente para su almacenamiento. (Blázquez, 2014, p. 54)

Datos de usuarios

Son caracteres y/o información procesada por aplicaciones.

Datos de sistema

Son caracteres utilizados para su respectiva gestión por una base de datos.

Sistema

Según Kendall (2011), es "un conjunto de elementos relacionados entre sí funcionalmente de modo que cada elemento del sistema es función de algún otro elemento, no habiendo ningún elemento aislado" (p. 2).

Licencia de software

"Es la autorización o el permiso concedido por el titular del derecho de autor, en cualquier forma contractual, al usuario de un programa informático, para utilizarlo en forma determinada y de conformidad con las condiciones convenidas". (Romero, 2015, p. 9)

Software libre

Para Romero (2015), "es cuando el software llega a brindar libertad a los usuarios sobre su producto adquirido y, por lo tanto, una vez obtenido, puede ser usada, copiada, estudiada, modificada y distribuida con libertad" (p. 10).

Shareware

"Es una modalidad de distribución de software, donde el usuario llega a evaluar de manera gratuita el producto, pero con limitaciones en el periodo de uso y restricciones den las capacidades finales". (Romero, 2015, p. 10)

Software propietario

Según Romero (2015), "es aquel software que es comercializado, donde las organizaciones o individuos que lo producen cobran dinero, tanto por su distribución y soporte" (p. 11).

Freeware

"Tipo de software que se distribuye sin costo alguno, disponible para ser utilizado por tiempo ilimitado, la misma es una variante gratuita del shareware, para que el cliente pruebe el producto durante un tiempo limitado, si este lo satisface lo cancele por él". (Romero, 2015, p. 11)

Internet

Para Romero (2015), "es una red mundial de computadoras que están conectadas entre sí y que pueden intercambiar información" (p. 12).

Virus informático

Es "un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos". (Vieites, 2013, citado por Romero et al., 2018, p. 15)

Bloqueo automático

"Es un mecanismo de emergencia que permite bloquear de manera automática el sistema informático contra riesgos y ataques para evitar hacer lo que querían". (Romero et al., 2018, p. 21)

Encriptación

"También conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada". (Romero et al., 2018, p. 21)

Encriptación simétrica

Santos (2014), sostiene que "está basado en métodos criptográficos que usan una misma clave para cifrar y descifrar el mensaje" (p. 47).

Encriptación asimétrica

"Se basa en que si el emisor cifra la información el receptor lo puede descifrar o viceversa, en este caso cada usuario del sistema debe poseer una pareja de claves". (Santos, 2014, p. 47)

Clave privada

Se encuentra bajo la custodia del propietario, solo él tiene conocimiento y acceso a ella.

Clave pública

Se caracteriza por tener acceso o conocida por uno o todos los usuarios

Riesgos informáticos

Para Romero (2018), "es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional" (p. 28).

Amenazas informáticas

"Son esos sucesos que pueden dañar los procedimientos o recursos de hardware, software e información". (Romero, 2018, p. 28)

Vulnerabilidades informáticas

"Consisten en los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema". (Romero, 2018, p. 28)

Privilegios

"Son permisos de actuación que un usuario, sea una persona o un sistema tiene para actuar sobre otros recursos".

Ataque pasivo

“Consiste en monitorear al sujeto atacado, es un ataque no invasivo ya que no afecta a la infraestructura, pero monitoriza lo que esta puede almacenar o transmitir, incluso información que es directamente pública” (Romero, 2018, p. 37)

Ataque activos

“Se caracterizan por acciones directas que tratan de penetrar la infraestructura, e incluso de hacerse estables dentro de ella de forma permanente”. (Romero, 2018, p. 37)

Descifrado de contraseñas

“Es el proceso de validar cuan robusta puede ser una clave, a través del uso de herramientas de recuperación de contraseñas de manera automática”. (Romero, 2018, p. 54)

Sondeo de red

“Consiste en analizar nombres de dominio, nombres de servidores, direcciones IP, mapas de red, información del proveedor de internet, propietarios de sistema y servicios”. (Romero, 2018, p. 56)

Testeo de aplicaciones de internet

De acuerdo a Romero (2018), “consiste en emplear diferentes técnicas de análisis de software para encontrar fallos de seguridad en aplicaciones cliente, como se está realizando un análisis externo, se pueden utilizar en este módulo los test de caja negra” (p. 56).

Antivirus

“Esencialmente son programas que se basan en la detección de malware en la fase de pre-ejecución”.

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1 Hipótesis

3.1.1 Hipótesis General

Existe relación significativa de la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021.

3.1.2 Hipótesis Específicas

1. Existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021.
2. Existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021.
3. Existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021.
4. Existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.

3.2 Método

Para la presente investigación en base a las características de cada una de las variables y sus respectivas dimensiones se aplicó el método deductivo y analítico:

Donde el método deductivo, permitió realizar las examinaciones de los fenómenos y se originaran a partir del marco teórico, referente a la caracterización de las dos variables objeto de investigación.

Es así, por intermedio del presente método se utilizaron y emplearon principios reveladores de objetos y fenómenos generales a aspectos peculiares y particulares, partiendo de una vinculación de criterios y conocimiento propios (Madé, 2006, p. 69).

El método analítico, permitió identificar e inspeccionar cada variable, que señaló y determinó la realidad problemática en la organización objeto de estudio, analizando las correlaciones existentes entre las dimensiones que las integran.

De donde los procesos analíticos, permiten reconocer los componentes de un objeto y/o fenómeno para proceder con la revisión sistemática de cada elemento e independientemente una de otra. (Abad, 2009, p. 94)

3.3 Tipo investigación

El estudio es de enfoque cuantitativo según la naturaleza de las variables investigadas, donde la información obtenida se operó numéricamente y objetivamente gracias a la estadística descriptiva.

La investigación es de un estudio de tipo básica o fundamental, por cuanto la presente investigación se enmarcó en el manejo de las teorías y conocimientos asociados a los fenómenos objeto de estudio para posteriormente suministrar y aportar a las teorías existentes.

Para Valderrama (2013), las investigaciones básicas o puras:

> "Tiene por finalidad de generar conocimientos sin producir respuestas o resultados para su aplicación inmediata, se interesa por captar datos de la realidad de tal modo pueda alimentar los conocimientos teóricos-científicos" (p.164).

3.4 Nivel o alcance de investigación

El presente estudio pertenece a un nivel de investigación correlacional-descriptivo, donde se llegó a determinar, puntualizar y relatar los contextos y sucesos que se encuentran relacionados en un momento determinado de las variables, es decir como son y de qué manera se comportaron determinados fenómenos y/o componentes de las variables estudiadas, además se llegó a describir la realidad problemática de los fenómenos tal y como se presentaron en los diversos escenarios y que están sumidos con la gestión de las TIC, y los procesos de seguridad informática del gobierno regional de Apurímac, 2021.

Para Hernández, Fernández y Baptista (2014), la investigación de nivel correlacional:

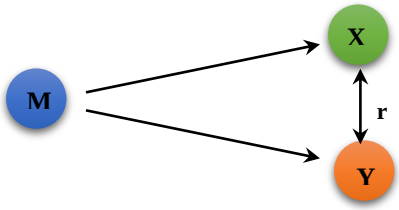
> "Permitirá identificar y anunciar las relaciones existentes a partir de dos o más variables, donde los datos se tomaran directamente de la realidad para ser interpretados y dar explicación a sus concordancias" (p. 93).

De otra parte las investigaciones de carácter descriptivo "examinan y especifican las propiedades sustanciales de los fenómenos y/o objetos que son sujetos para su análisis". (Hernández et al, 2014, p. 92)

3.5 Diseño de investigación

El presente estudio es de diseño no experimental – transeccional, donde la información se llegó a obtener en un momento único en su ambiente natural, sin realizar ninguna manipulación, para luego especificar y describir de manera real cada fenómeno en estudio, escenario que permitió analizar el nivel de relación entre la gestión de las TIC, y el proceso de la seguridad informática del gobierno regional de Apurímac, 2021.

Por cuanto el diagrama a sostener fue:



Dónde:

M = Muestra de las unidades de análisis.

X = Variable gestión de tecnología de información y comunicación.

Y = Variable seguridad informática.

r = Relación entre las variables en estudio.

Por cuanto las investigaciones no experimentales son "estudios que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural para analizarlos". (Hernández et al, 2014, p. 152)

A su vez, es una investigación transeccional, toda vez que los datos se acopiaron en un tiempo único. (Hernández et al, 2014, p. 154)

3.6 Operacionalización de Variables

Variable de investigación	Definición conceptual	Dimensiones	Definición Operacional	Indicadores
Variable X: Gestión de Tecnologías de Información y Comunicación	son aquellas "herramientas de gestión computacional e informática que procesan, almacenan, sintetizan, recuperan y presentan información de la más variada, a través de un conjunto de herramientas, soportes y canales para el tratamiento eficiente de la información al interior de las organizaciones" (Huidobro,2007, p:2	Infraestructura	En el conjunto de procesos de tecnología conformadas por la infraestructura, Arquitectura, conocimiento, relaciones y del personal desde la adquisición, producción y almacenamiento, tratamiento, comunicación, registro y presentación de la información en la empresa, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnético	Hardware Software Tecnología de comunicación Plataforma de aplicación Conectividad Compatibilidad Modularidad
		Arquitectura		Planificación Datos Conectividad Seguridad Política Riesgo Ambientes Compatibilidad
		Talento Humano		Atención Capacidad Oportunidades Recursos Resultados Liderazgo
		Conocimiento		Apalancamiento Respaldo Impacto Procesos Evaluación Actitud Operación
		Relaciones de la TIC con el negocio		Adecuada comunicación Normativas Conocimiento Efectividad Producción Responsabilidad Adaptación al cambio

Variable de investigación	Definición conceptual	Dimensiones	Definición Operacional	Indicadores
Variable Y: Seguridad Informática (SI)	Es cualquier medio que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevarse a daños sobre la información comprometer su confidencialidad, autenticidad, disponibilidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (Gomez,2017, p,40)	Proceso	Son procedimientos y técnicas desarrolladas para proteger los equipos informáticos y la información de daños accidentales o intencionados, por intermedio de su confidencialidad, disponibilidad, autenticidad e integridad.	Políticas Manejo de actividad Aseguramiento e identidad Intercambio de datos y otros Elementos Control Identificación y envió Reportes
		Confidencialidad		Acceso Cuentas Roles Resguardo Codificación Fugas y filtraciones Custodia Gestión
		Integridad		Ataques Validación Consistencia Exactitud Resguardo de la información Vulnerabilidad Medidas Protección Modificación
		Disponibilidad		Información Metodología Roles del Usuario Flujo de datos Sistema comunicativo Requerimientos Usuarios Almacenamiento Requerimientos

3.7 Población, muestra y muestreo

3.7.1 Población

Para el presente estudio la población estuvo constituida por los talentos humanos que se encontraban laborando en las diferentes unidades y/o dependencias del gobierno regional de Apurímac, como: la subgerencia de desarrollo institucional, estadística e informática y el área de las tecnologías de información, la dirección regional de administración, la gerencia de planeamiento de presupuesto y acontecimientos territoriales, la gerencia regional de desarrollo económico del gobierno regional de Apurímac. La misma estuvo conformada por ochenta y dos (82) talentos humanos en total.

Toda vez que la población "Es el conjunto de todos los elementos (unidades de análisis) que pertenecen al ámbito espacial donde se desarrolla el trabajo de investigación". (Carrasco, 2006, p. 236)

3.7.2 Muestra

La muestra para la presente investigación estaba conformada por las unidades de análisis del talento humano de las diferentes unidades funcionales del gobierno regional estudiada, donde el tamaño de muestra se llegó a obtener por intermedio del método de muestreó probabilístico, debido a que las unidades muéstrales en su gran mayoría se encontraban realizando trabajo remoto y no se tenía acceso a las mismas de manera presencial a consecuencia del aislamiento social y el estado de emergencia sanitaria que el país se encuentra viviendo a efecto del COVID-19, así como del factor tiempo para la conclusión del estudio dentro los plazos respectivos; es así que todos los empleados tuvieron la misma probabilidad de ser considerados para la observación respectiva y acopio de la información.

El tamaño de la muestra se llegó a obtener por intermedio de la formula estadística de Cochran:

$$n = \frac{NZ^2S^2}{d^2(N-1) + Z^2S^2}$$

Siendo:

n: el tamaño de la muestra

N: el tamaño de la población

Z: el coeficiente de confianza o valor de Z critico

S: la varianza de la población en estudio

d: el nivel de precisión absoluta

Desarrollando:

n = ?

N = 82 talentos humanos.

Z = el coeficiente de confianza, por la tabla al 95 % = 1.96

S = la varianza de la población: considerado un 0.5

d = el nivel de precisión absoluta; según la tabla al 95 % = 0.05

$$n = \frac{82 * 1.96^2 * 0.5^2}{0.05^2 * (82 - 1) + 1.96^2 * 0.5^2}$$

$$n = \frac{78.7528}{1.1629} = 67.72$$

$\boldsymbol{n = 68}$ Unidades muéstrales

Por cuanto la muestra para el presente estudio fue de 68 trabajadores de las unidades funcionales consideradas para el presente estudio del gobierno regional de Apurímac.

3.7.3 Muestreo

El método que se aplicó para determinar las unidades de análisis estuvo basado en el muestreo aleatorio simple, partiendo de la realidad donde todos los actores tuvieron la misma probabilidad de participar y obtener los datos para arribar a los objetivos señalados y la contrastación de las hipótesis de investigación. De donde los resultados obtenidos producto de la muestra manejada refleja la realidad total de la población de los empleados del gobierno regional de Apurímac.

3.8 Técnicas e instrumentos

3.8.1 Técnica

Para el presente estudio la técnica establecida fue la encuesta, en las mismas se consideraron una sucesión de elementos, indicadores y valoraciones de cada una de los fenómenos en estudio a partir de sus respectivas dimensiones, que permitió observar las características de la gestión de las TIC y los procesos de la seguridad informática del gobierno regional de Apurímac, 2021.

3.8.2 Instrumentos

Para la investigación se diseñó instrumentos basado en dos cuestionarios, las mismas estaban estructuradas de manera propia para cada una de las variables objeto de estudio, partiendo de sus respectivas dimensiones, indicadores y valoraciones pertinentes, la mismas que se aplicaron en los talentos humanos de las unidades funcionales de la entidad estudiada, acopiando los datos y describir una aproximación psicométrica de la gestión de la TIC, así como de los procesos de la seguridad informática, basada en la escala valorativa de opción múltiple tipo Likert.

De donde Hernández, et al. (2014), manifiesta que un cuestionario es:

> "Un conjunto de preguntas respecto de una o más variables que se van a medir" (p. 217).

3.9 Consideraciones éticas

Para abordar el estudio se procedió con la instauración de los mecanismos prácticos de toda investigación científica, partiendo de toda actitud ética personal y profesional, con un compromiso sincero con los empleados y/o unidades de análisis del gobierno regional de Apurímac, partiendo del consentimiento informado, protección y motivación sobre la significancia de la presente investigación para la entidad objeto de estudio en relación a la gestión de la tecnología de información y comunicación y su concordancia con los procesos de seguridad informática, así como para futuros estudios a ser desarrollados.

3.10 Procedimientos estadísticos

3.10.1 Procesamiento y presentación de datos

Para una oportuna obtención de los datos, se procedió con enviar un documento ante el ápice estratégico del gobierno regional de Apurímac para el inicio, autorización y ejecución de la investigación y aplicar los cuestionarios en los talentos humanos de las diferentes unidades funcionales consideradas de la entidad en estudio.

Los datos e información captados durante la ejecución del presente trabajo de investigación fueron estimados, procesados y estructurados en sus respectivas bases de datos de cada fenómeno, posteriormente presentados de manera numérica en tablas distribuidas en frecuencias y porcentajes, para luego reflejarlas en sus figuras correspondientes a partir de las dimensiones e indicadores de cada variable, tales como la gestión de la tecnología de información y comunicación, y los procesos de la seguridad informática, para los cuales se llegó a aplicar el software estadístico IBM SPSS 26, Microsoft Excel y Word.

3.10.2 Análisis e interpretación de datos

Capturado la información fueron tabulados, procesados y presentados en tablas y figuras, para luego proceder con el análisis, interpretación y las discusiones respectivas de manera práctica, concreta, seria y la rigurosidad del caso, aplicando para el mismo la estadística descriptiva e inferencial, la misma que permitió evidenciar la realidad de los fenómenos en un momento único y determinar el nivel de asociación que existe entre la gestión de la tecnología de información y comunicación y el proceso de seguridad informática en la organización en estudio.

Así mismo para llegar a contrastar las hipótesis de investigación del presente trabajo, se plantearon las hipótesis estadística respectivas producto de los datos e información obtenida en los resultados, la misma que estuvo sujeto a la estadística inferencial por el coeficiente de correlación *r* de Pearson y medir la magnitud del grado de relación que existe entre ambas variables objeto de investigación en el gobierno regional de Apurímac.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1 Resultados

Tabla 1

Aspectos sociodemográficos del talento humano

Aspectos Sociodemográficos	Afirmación	F	%	Porcentaje Acumulado
Genero	Masculino	41	60.29	60.29
	Femenino	27	39.71	100
	Total	68	100	
Edad	De 21 a 30 años	26	38.24	38.24
	De 31 a 40 años	29	42.65	80.89
	De 41 años a más	13	19.12	100
	Total	68	100	
Estado civil	Soltero (a)	41	60.29	60.29
	Casado (a)	10	14.71	75.00
	Conviviente	17	25.00	100
	Total	68	100	
Formación profesional	Técnico	3	4.41	4.41
	Bachiller	16	23.53	27.94
	Profesional	45	66.18	94.12
	Magister	4	5.88	100
	Total	68	100	
Tiempo de servicio	De 1 a 2 años	14	20.59	20.59
	De 3 a 6 años	39	57.35	77.94
	Más de 6 años	15	22.06	100
	Total	68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

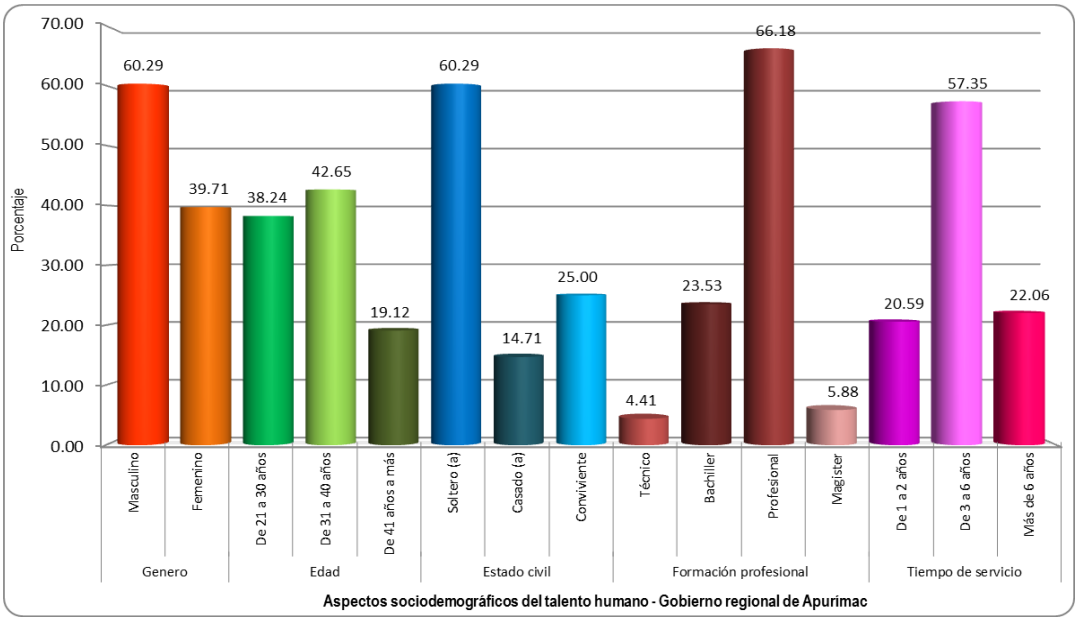


Figura 1: Aspectos sociodemográficos del talento humano del gobierno regional de Apurímac

Al observar la tabla y figura anterior, se aprecia que el 60.29% del talento humano del gobierno regional es del sexo masculino y el 39.71% son femeninos, de donde el 42.65% presentan edades entre 31 a 40 años, el 38.24% de 21 a 30 años de edad, además el 60.29% son solteros, así como el 66.18% son profesionales y al final el 57.35% presentan un tiempo de servicio de 3 a 6 años en la entidad objeto de estudio.

Tabla 2

Infraestructura-gestión de tecnologías de información y comunicación

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Infraestructura	Casi nunca	5	7.35	7.35
	A veces	29	42.65	50.00
	Casi siempre	24	35.29	85.29
	Siempre	10	14.71	100
Total		68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

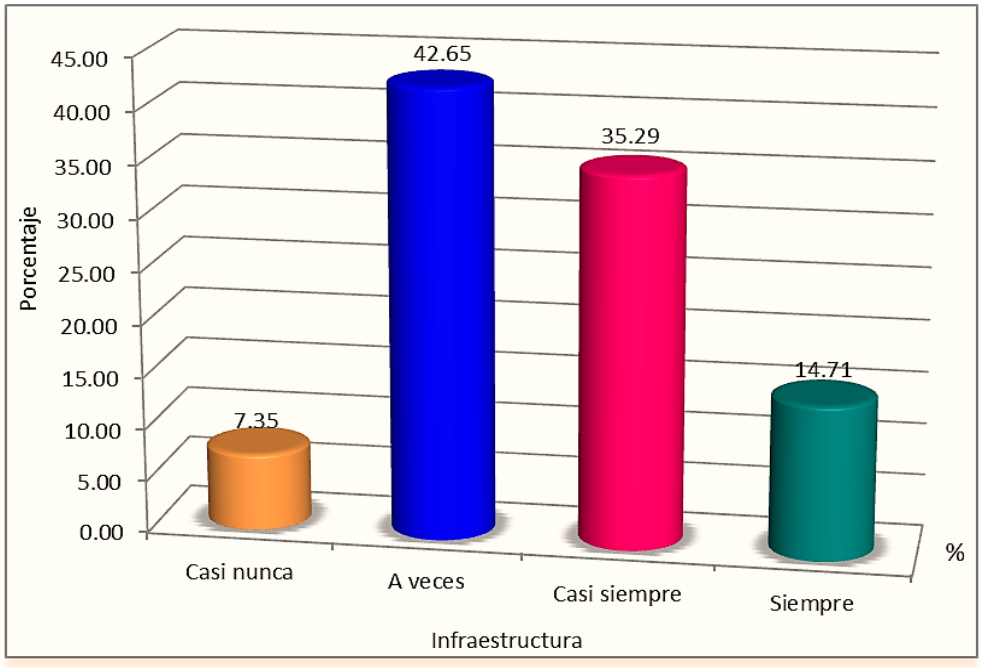


Figura 2: Infraestructura-gestión de tecnologías de información y comunicación

La tabla y figura 2, se aprecia datos de la infraestructura de las TIC de la entidad objeto de estudio, donde el 42.65% de los empleados manifestaron a veces, seguido del 35.29% que afirmaron casi siempre, luego el 14.71% que señaló siempre y tan sólo el 7.35% indicó casi

nunca contar con una adecuada infraestructura de las TIC en el gobierno regional de Apurímac.

Tabla 3

Arquitectura-gestión de tecnologías de información y comunicación

Dimensión	Afirmación	F	%	Porcentaje Acumulado
Arquitectura	Nunca	1	1.47	1.47
	Casi nunca	4	5.88	7.35
	A veces	33	48.53	55.88
	Casi siempre	26	38.24	94.12
	Siempre	4	5.88	100
Total		68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

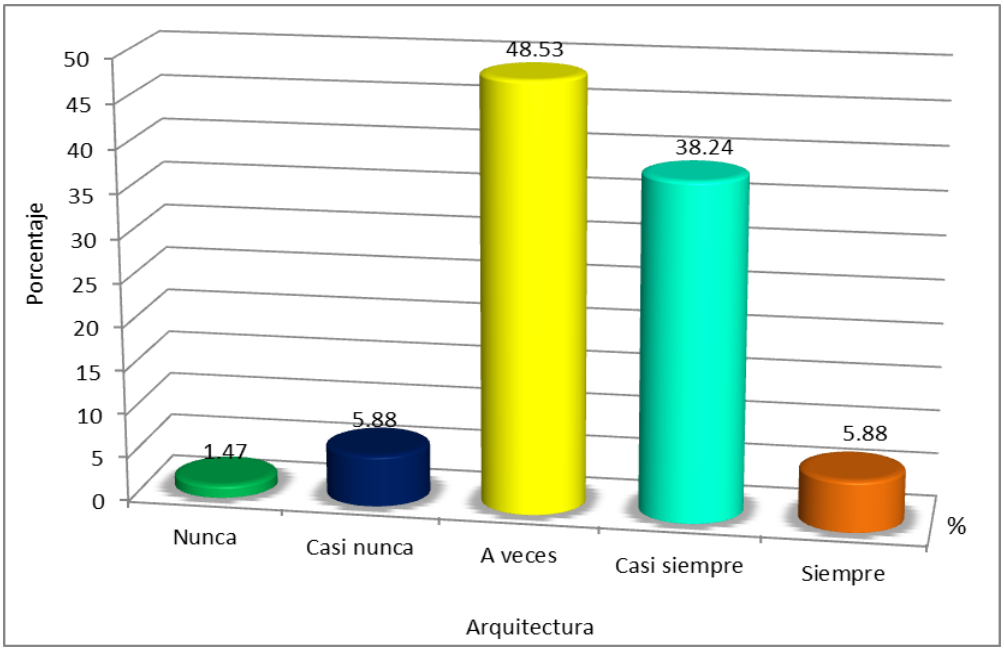


Figura 3: Arquitectura-gestión de tecnologías de información y comunicación

Considerando la tabla y figura que antecede, presenta información sobre la arquitectura, de donde el 48.53% del talento humano sostuvieron a veces, además el 38.24% afirmaron casi siempre, luego el 5.88% de manera igualada imprimieron siempre y casi nunca respectivamente, y al final tan sólo el 1.47% supieron señalar nunca existe una arquitectura adecuada en cuanto a la tecnología de información y comunicación en la entidad investigada.

Tabla 4

Talento humano-gestión de tecnologías de información y comunicación

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Talento humano	Casi nunca	4	5.88	5.88
	A veces	28	41.18	47.06
	Casi siempre	31	45.59	92.65
	Siempre	5	7.35	100
	Total	68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

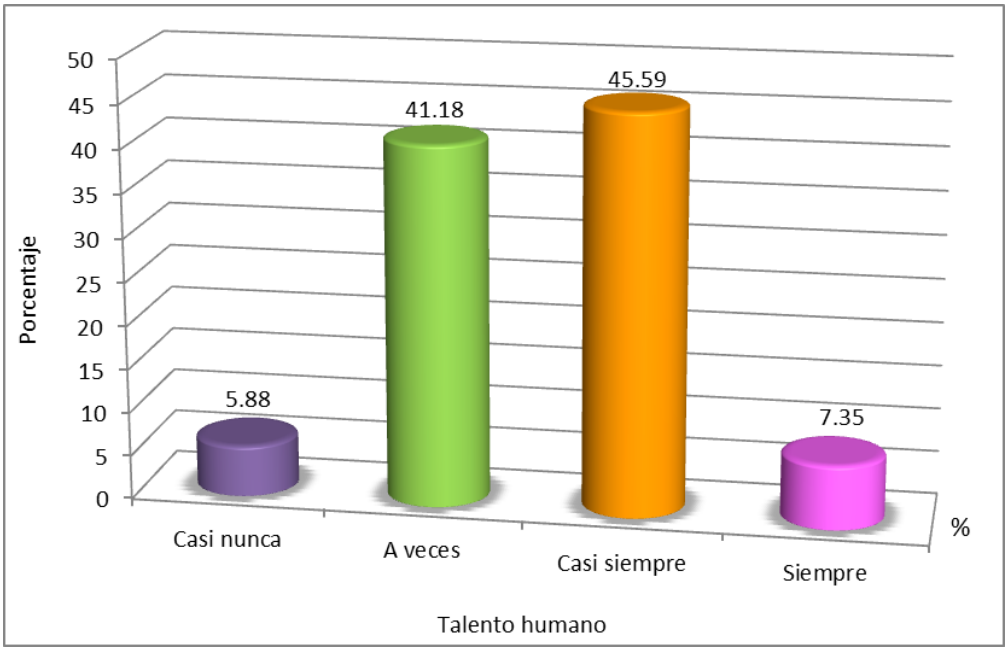


Figura 4: Talento humano-gestión de tecnologías de información y comunicación

Visualizando la anterior tabla y figura, se distingue que el 45.59% del talento humano manifestaron casi siempre, seguido del 41.18% que afirmaron a veces, además del 7.35% que indicó siempre y al final el 5.88% señalaron casi nunca la institución brindan oportunidades, motivaciones y estímulos a los responsables de administrar la tecnología de información y comunicación de la entidad.

Tabla 5

Conocimiento-gestión de tecnologías de información y comunicación

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Conocimiento	Nunca	1	1.47	1.47
	Casi nunca	3	4.41	5.88
	A veces	27	39.71	45.59
	Casi siempre	33	48.53	94.12
	Siempre	4	5.88	100
Total		68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

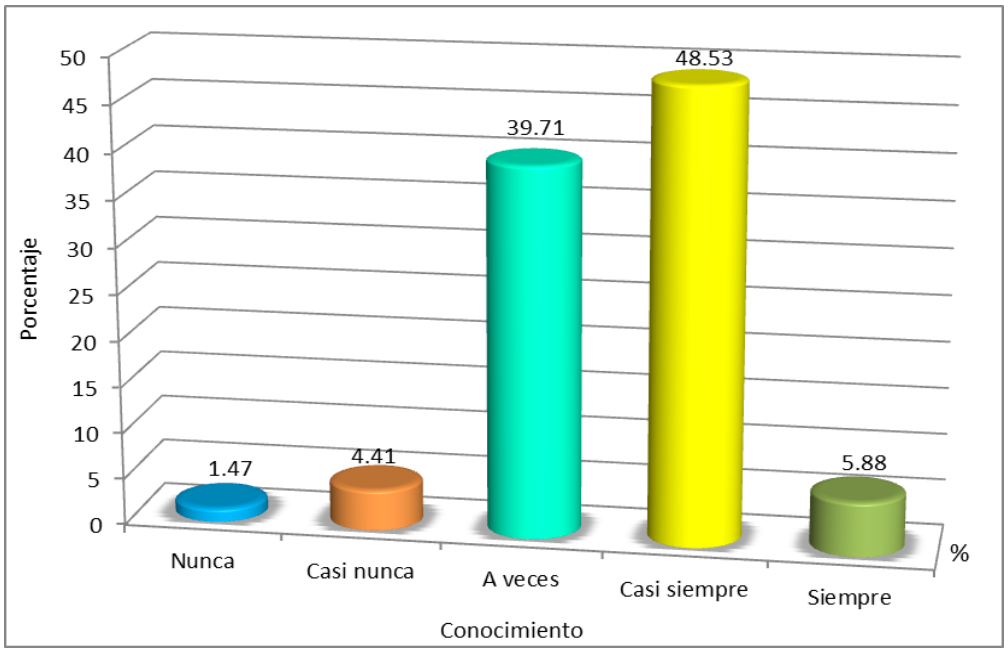


Figura 5: Conocimiento-gestión de tecnologías de información y comunicación

Observando la tabla y figura anterior presenta datos de la dimensión conocimientos del trabajador, de donde el 48.53% afirmaron casi siempre, así mismo el 39.71% manifestó a veces, además el 5.88% sostuvo siempre, luego el 4.41% imprimió casi nunca y sólo el 1.47% declaró nunca los altos directivos tener conocimientos sobre la realidad de las TIC, así como el talento humano que labora en la unidad objeto de estudio cuentan con conocimientos de operación y procedimientos de seguridad informática.

Tabla 6

Relaciones de las TIC con el negocio-gestión de tecnologías de información y comunicación

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Relaciones de las TIC con el negocio	Casi nunca	3	4.41	4.41
	A veces	30	44.12	48.53
	Casi siempre	31	45.59	94.12
	Siempre	4	5.88	100
Total		68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

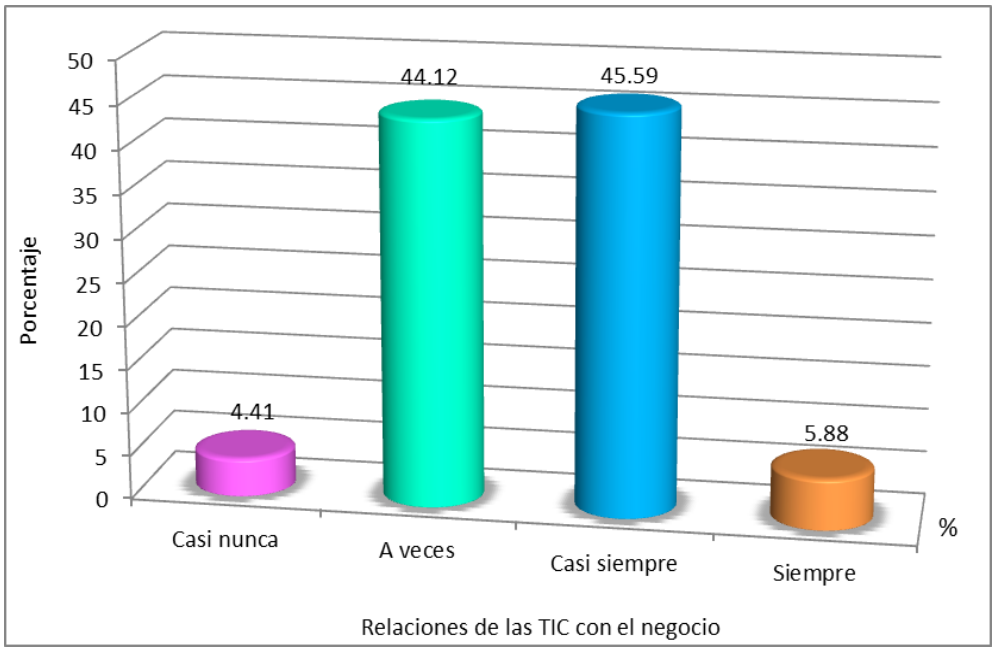


Figura 6: Relaciones de las TIC con el negocio-gestión de tecnologías de información y comunicación

Considerando la tabla y figura 6, se distingue que el 45.59% de los empleados supieron señalar que casi siempre, seguido del 44.12% que apuntaron a veces, luego el 5.88% que dijeron siempre y al final un 4.41% aseveraron casi nunca existe una política clara y coherente en las relaciones de las TIC con el proceso de negocio de la entidad en cuanto a su seguridad informática para el cambio organizacional.

Tabla 7

Gestión de tecnologías de información y comunicación

Variable	Afirmación	f	%	Porcentaje Acumulado
Gestión de tecnologías de información y comunicación	A veces	3	4.41	4.41
	Casi siempre	59	86.76	91.17
	Siempre	6	8.82	100
Total		68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

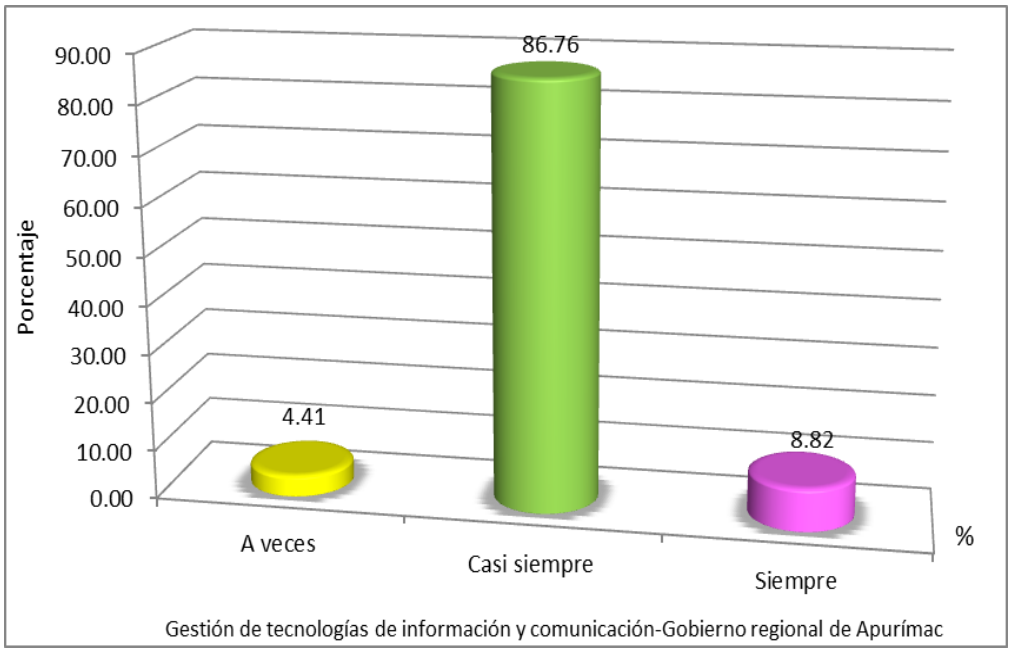


Figura 7: Gestión de tecnologías de información y comunicación

La anterior tabla y figura 7, reflejan información sobre la realidad latente de la variable estudiada, de donde el 86.76% de los sujetos manifestaron casi siempre, luego el 8.82% alegaron siempre y un 4.41% declararon a veces existe una adecuada gestión de las TIC del gobierno regional de Apurímac.

Tabla 8

procesos-seguridad informática

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Procesos	Nunca	1	1.47	1.47
	Casi nunca	8	11.76	13.23
	A veces	29	42.65	55.88
	Casi siempre	26	38.24	94.00
	Siempre	4	5.88	100
	Total	68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

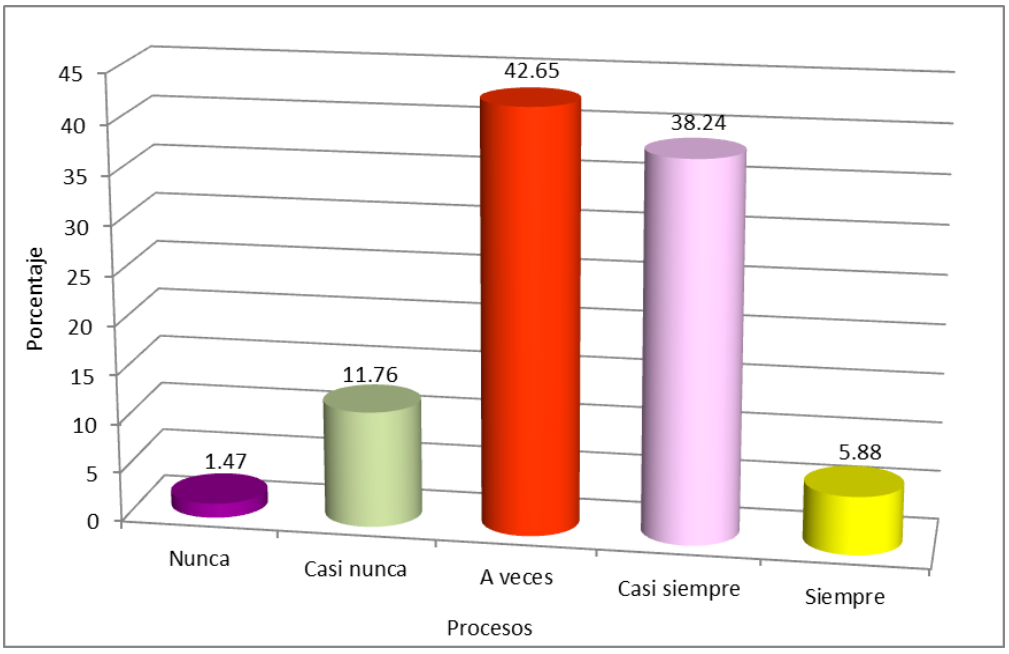


Figura 8: procesos-seguridad informática

Observando la tabla y figura que antecede se aprecia que el 42.65 de los empleados afirmaron a veces, seguido del 38.24% que aseguraron casi siempre, posteriormente el 11.76% imprimieron casi siempre, además del 5.88% que registraron siempre y al final el 1.47% registraron nunca es apropiada los procedimientos, aseguramiento e identidad de la seguridad informática en la institución.

Tabla 9

Confidencialidad-seguridad informática

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Confidencialidad	Casi nunca	5	7.35	7.35
	A veces	33	48.53	55.88
	Casi siempre	26	38.24	94.00
	Siempre	4	5.88	100
	Total	68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

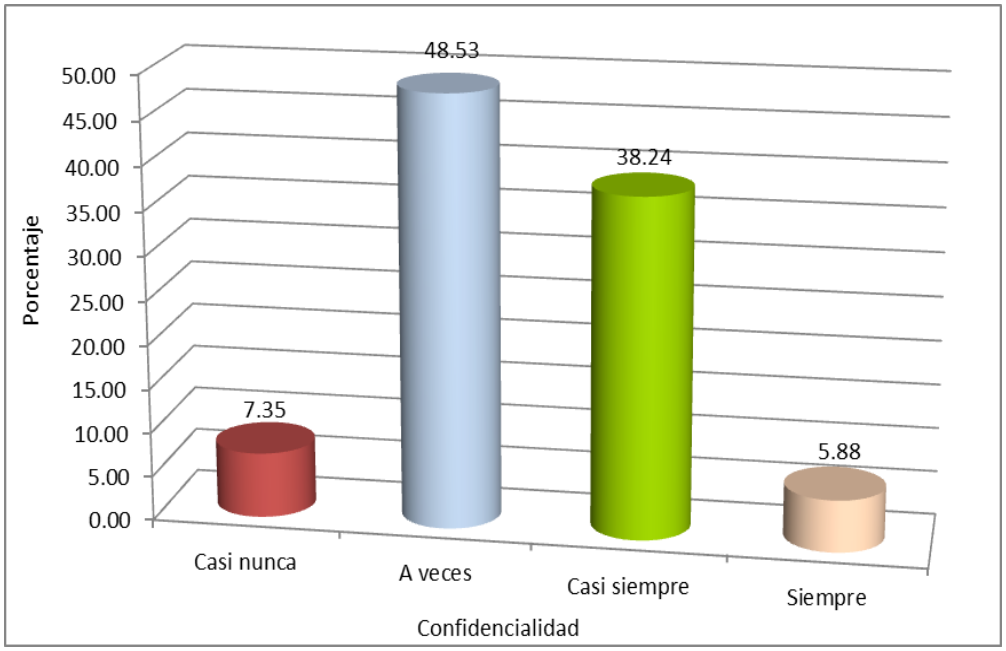


Figura 9: Confidencialidad-seguridad informática

En la tabla 9 se puede distinguir los datos de la dimensión confidencialidad de a seguridad informática la misma que se refleja en la figura 9, en donde el 48.53% de los empleados manifestaron a veces, además del 38.24% que señalaron casi siempre, luego el 7.35% especificaron casi siempre y sólo el 5.88% suscribieron siempre existen directivas, procedimientos u otros documentos de confidencialidad que normen la gestión de accesos a la información en la institución.

Tabla 10

Integridad-seguridad informática

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Integridad	Casi nunca	5	7.35	7.35
	A veces	34	50.00	57.35
	Casi siempre	25	36.76	94.11
	Siempre	4	5.88	100
	Total	68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

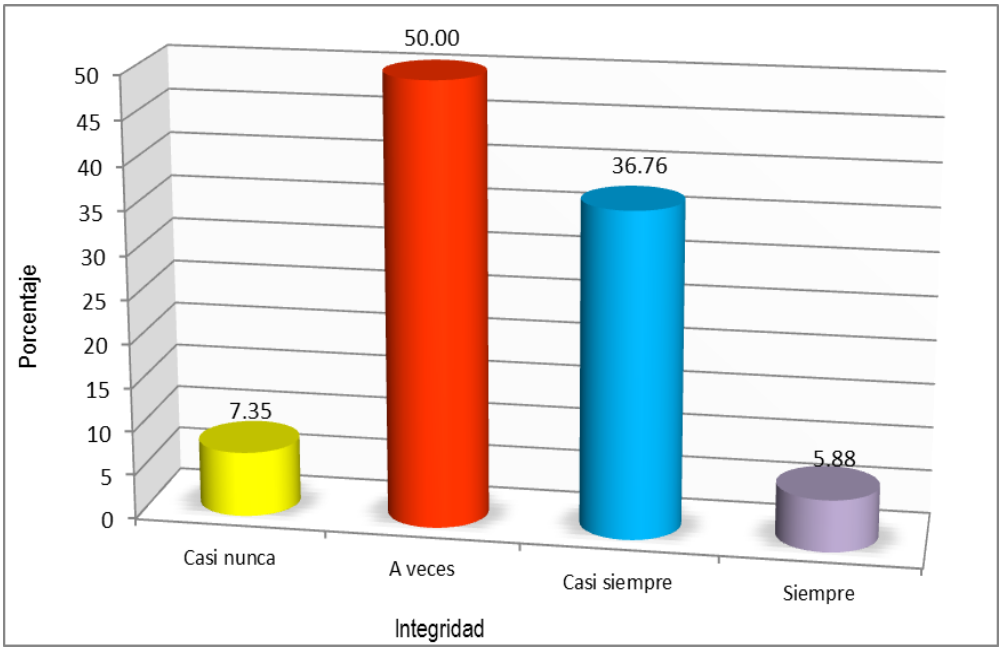


Figura 10: Integridad-seguridad informática

Considerando la tabla y figura precedente donde se advierte que el 50.00% del talento humano de la entidad en estudio manifestaron a veces, seguido del 36.76% que indicaron casi siempre, además del 7.35% que anunciaron casi nunca y al final sólo el 5.88% mencionaron siempre al integridad de la seguridad informática se toma en cuenta en la institución para la protección de los datos contra el acceso no autorizado e inapropiado.

Tabla 11

Disponibilidad-seguridad informática

Dimensión	Afirmación	f	%	Porcentaje Acumulado
Disponibilidad	Casi nunca	1	1.47	1.47
	A veces	36	52.94	54.41
	Casi siempre	28	41.18	95.59
	Siempre	3	4.41	100
	Total	68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

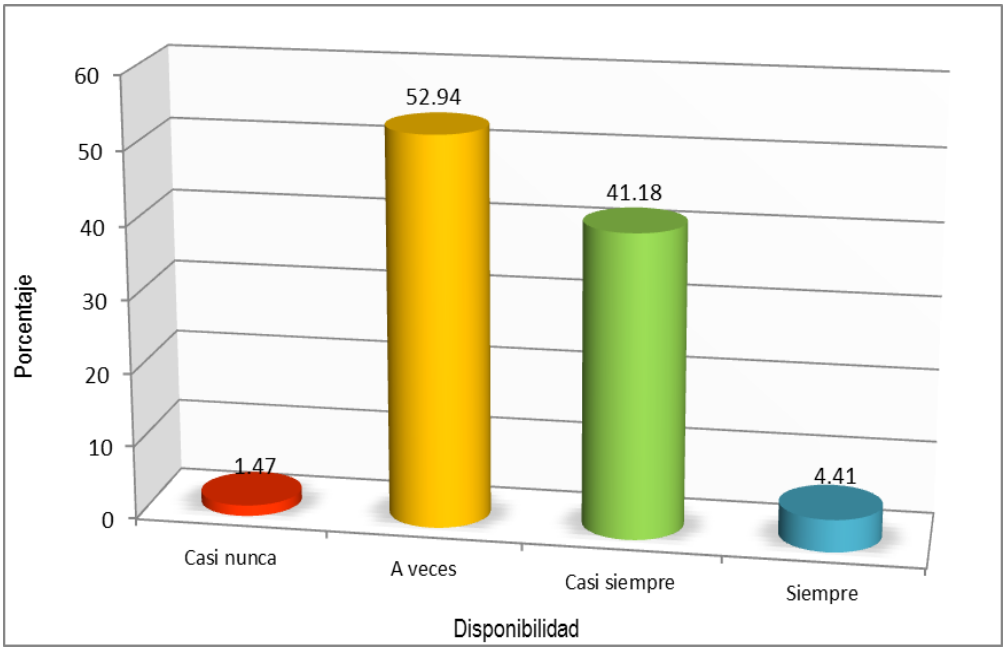


Figura 11: Disponibilidad-seguridad informática

En la tabla y figura que antecede se puede llegar a distinguir los datos de la dimensión disponibilidad del fenómeno seguridad informáticas, donde el 52.94% de los empleados afirmaron a veces, el 41.18% señalaron casi siempre, así mismo el 4.41% indicaron siempre y el 1.47% declararon si nunca no está disponible la información cuando el usuario o sistema necesite realizar una consulta para la toma de decisiones en la institución regional.

Tabla 12

Seguridad informática

Variable	Afirmación	F	%	Porcentaje Acumulado
Seguridad informática	A veces	14	20.59	20.59
	Casi siempre	52	76.47	97.06
	Siempre	2	2.94	100
Total		68	100	

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado

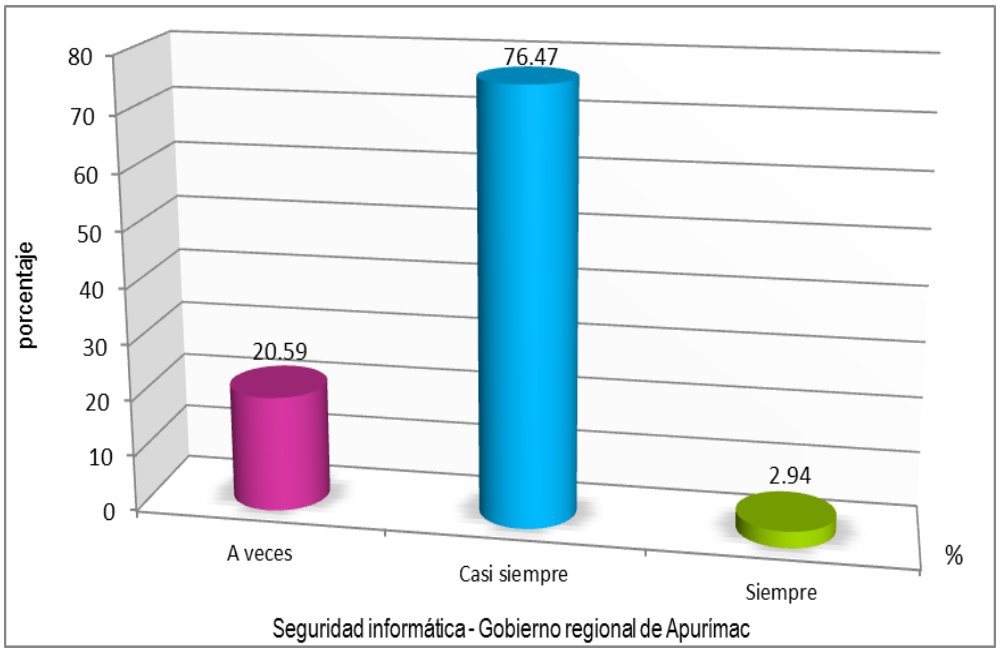


Figura 12: Seguridad informática

Se puede divisar en la tabla y figura 12 datos relacionados al fenómeno seguridad informática, de donde el 76.47% del talento humano manifestaron casi siempre, seguido del 20.59% que indicó a veces y un 2.94% sostuvieron siempre se establecen políticas y tareas de la seguridad informática que repercuten en los objetivos de la seguridad de los datos en la institución regional de Apurímac.

4.2 Discusiones de resultados

De los resultados conseguidos se desarrolla las discusiones pertinentes y precisas en el presente estudio:

1. En consideración a nivel de concatenación de la variable gestión de las TIC con la seguridad informática en el gobierno regional de Apurímac, 2021. Se sostiene de forma precisa y validar la hipótesis general a partir del coeficiente de correlación *r* de Pearson de 0.663** que señala de la existencia de un nivel de relación positiva alta, además el *p*-valor alcanzado fue α=0.000 siendo inferior al nivel de significancia de 0.01, determinando de manera categórica que existe relación significativa, positiva, consistente y alta entre la gestión de las TIC y la seguridad informática, toda vez que el 86.76% de los sujetos manifestaron casi siempre se cumplen con todos los procesos operacionales tendientes a una efectiva gestión de las tecnologías, basadas a partir de la infraestructura, la arquitectura, el talento humano y las relaciones de las Tic con las actividades de negocio organizacional, además por el 76.47% de los empleados que sostuvieron que casi siempre se toman en cuenta los elementos necesarios para el manejo adecuado de la seguridad informática la misma que repercuten en la políticas, seguridad, protección y la garantía para el intercambio de datos en las diferentes unidades a partir de los procesos de confidencialidad, integridad y disponibilidad de los datos en la toma de decisiones oportunas y efectivas. Tal como señala Ancajima (2019), en su investigación de pregrado en donde concluye; que la implementación de políticas a los procesos operativos favorecerán a la seguridad informática de la entidad educativa, donde docentes, alumnos y personal administrativo estén conformes, felices y complacidos con la información utilizada, muy seguros de las mismas y de su facilidad de manejo (p. 119).
2. Por otro lado en referencia a la relación de la gestión de las Tic con los procesos de la seguridad informática, se reconoce y valoriza la primera hipótesis específica en base al coeficiente de correlación de *r* de Pearson igual 0.490** que específica de la existencia de una relación positiva moderada y el *p*-valor brindado de α=0.000 misma que es inferior al grado de significancia de 0.01, determinando la existencia de una asociación, positiva media y consistente entre la gestión de las Tic con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021; contexto exhibido por el 86.76% del talento humano que señalaron que casi siempre cuentan con los componentes adecuados de hardware y las aplicaciones de software que forman el sostén de los sistemas, desarrollo de las actividades, funcionamiento de tareas y las comunicaciones necesarias y suficientes que repercute positivamente en la gestión de las Tic en la organización, basadas en la integración del 42.65% que afirmaron que a veces los procesos de la seguridad informática cuenta con

políticas para los procedimientos, aseguramiento e identidad actualizados para efectuar la identificación, envió, almacenamiento de la información y reportar eventos e incidencias sobre seguridad informática por parte de la unidad de seguridad informática de la entidad. Situación concordante con la investigación de Guevara (2017), en la que concluye; que el distrito educativo carece de documentos específicos relacionados a las políticas de seguridad informática, cuyos procesos operativos de la información llevados a cabo, no se realizan en base a lineamientos establecidos, tan sólo se aplican ciertas normativas para administrar y manejar la información, donde las mismas lamentablemente son rutinarias y básicas, siendo las mismas insuficientes para garantizar las seguridad de la información de la entidad educativa (p. 86).

3. De otra parte en consideración a la relación de la gestión de las Tic y la confidencialidad de la seguridad informática; se establece contrastando la hipótesis específica segunda a partir del coeficiente *r* de Pearson que dio 0.467** que fija una relación positiva media, donde además el *p*-valor calculado de α=0.000 siendo inferior al nivel de significancia de 0.01, llegando a determinar que existe una asociación significativa, media positiva de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en la entidad regional de Apurímac, 2021; ambiente expuesto por el 86.76% de los trabajadores quienes manifestaron que casi siempre los responsables de la unidad de tecnologías de información cuenta con la capacidad, habilidad y conocimientos para cumplir con la atención, el papel, las funciones y procedimientos para una adecuada gestión de las Tic que se concatenan con el 48.53% de los empleados que indicaron a veces la confidencialidad de la seguridad informática cuenta con accesos que son otorgados en mérito a la función autorizada, producto del constante cambio de talento humano que se ve reflejada en las cuentas asignadas, en el resguardo y la duplicidad de roles que se dan por la poca o nula actualización de la matiz funcional, las directivas, reglamentos, procedimientos u otros documentos que norme la gestión de accesos a los sistemas que afecta la operatividad del servicio por las fugas y filtraciones de información en la institución. Realidad contrastada con la investigación de Camargo (2017), quien concluye; que no existe documentación referente a los procesos de la información, donde la situación latente de seguridad de la información está en un nivel medio, debido a que el talento humano realiza las actividades utilizando sus buenas prácticas de ellos, por la no existencia de procesos claros que les

lleguen a permitir, establecer roles y responsabilidades para cada uno de ellos, en especial del área informática donde tienen procesos establecidos, políticas implementadas para los activos de la información, pero estas no cuentan con la respectiva documentación y de una divulgación acertada sobre la seguridad informática (p. 102).

4. Así mismo en lo referente al grado de asociación de la gestión de las Tic con la integridad de seguridad informática; se inicia validando la tercera hipótesis específica en base a la prueba *r* de Pearson que arrojo 0.625** que establece una asociación positiva moderada y que el *p*-valor obtenido de α=0.000 es menor al nivel de significancia de 0.01, estableciendo que existe un grado de asociación significativa, fuerte, positiva y consistente de la gestión de la Tic con la integridad de seguridad informática en el gobierno regional de Apurímac, 2021; contexto reflejado por el 86.76% de los empleados que afirmaron casi siempre el área de las tecnologías de información cuenta con el respaldo y apoyo de la alta dirección y demás dependencias de la organización regional, toda vez que las Tic y los proceso de las operaciones informáticas con que cuentan favorecen al cumplimiento de los objetivos establecidos en el POA, favoreciendo la gestión de los procedimientos técnicos operativos de las Tic además a la seguridad informática, las mismas que se anidan por el 50.00% del talento humano que indicaron a veces la integridad de la seguridad informática presentan usuarios de las distintas dependencias de la entidad que son afectados por ataques de phishing, la realización de acciones para la protección de los datos contra el acceso y la modificación no autorizado e inapropiado con la finalidad de mantener las cualidades de validez, consistencia y exactitud de la información de manera apropiada. Ambiente latente tratada en la investigación de Ochoa (2015), en donde llega a la conclusión; que existe ausencia de una estructuración y la sistematización de los procesos operativos informáticos, siendo necesarios para la organización la puesta en marcha de las TIC, toda vez que en el departamento de contabilidad es deficiente, donde el empleado no recibe la información de la diferentes unidades de manera oportuna, al no existir funciones definidas de trabajo que deben desarrollar en ningún departamento, causando una mala organización y por ende no hay responsabilidad del personal (p. 89).
5. Al final en referencia al grado de relación de la gestión de las Tic con la disponibilidad de la seguridad informática; se considera y contrasta la cuarta hipótesis específica a partir del coeficiente *r* de Pearson igual a 0.591** que señala una relación positiva fuerte, además el

p-valor calculado α=0.000 siendo inferior al nivel de significancia de 0.01, de donde se determina que existe un nivel de relación significativa, consistentes, positiva fuerte entre la gestión de la Tic y la disponibilidad de la seguridad informática en la institución regional pública de Apurímac, 2021; entorno irradiado por el 86.76% del talento humano que aseveraron casi siempre la institución cuenta con directivas para la sistematización de los activos y de la información de las diferentes unidades orgánicas, y de la existencia de herramientas y normativas que apoyan con efectividad a la gestión de las aplicaciones de tecnologías de información, comunicación y de la seguridad informática para el cambio organizacional, las que se correlacionan con el 52.94% de los colaboradores que sustentaron que a veces la disponibilidad de la seguridad informática presenta alguna metodología para realizar la gestión de roles de las diferentes unidades y que la información se encuentre disponible cuando el usuario o sistema lo requiera para realizar las consultas respectivas, además los requerimientos enviados fuera del plazo por obstáculos presentados en los elementos de las TI y la seguridad informática inciden en la operatividad institucional. Panorama reflejado en la investigación de Machicao (2019), donde concluye; que existen diferentes niveles de riesgos, considerando diversos criterios para detectar las amenazas que puedan vulnerar la información que maneja la OTI, quienes deben garantizar su confidencialidad, integridad y disponibilidad de la misma a todas las unidades y que las políticas de seguridad de la informática coadyuvará con los controles para mejorar de forma técnica, práctica y precisa la operatividad de los datos al ser un documento de jerarquía y de uso para la seguridad de la información (p. 81).

4.3 Prueba de hipótesis

Hipótesis general

Tabla 13

Relación de la gestión de tecnología de información y comunicación con la seguridad informática

Correlaciones			
		Gestión de tecnologías de información y comunicación	Seguridad informática
Gestión de tecnologías de información y comunicación	Correlación de Pearson	1	,663**
	Sig. (bilateral)		,000
	N	68	68
Seguridad informática	Correlación de Pearson	,663**	1
	Sig. (bilateral)	,000	
	N	68	68
**. La correlación es significativa en el nivel 0,01 (2 colas).			

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 14

Análisis e interpretación

Hipótesis estadísticas	Ho: No existe relación significativa de la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021.
	Ha: Existe relación significativa de la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021.
Nivel de significación	$\alpha = 0{,}01$
Coeficiente de correlación r de Pearson	0,663**
Valor p calculado	$p = 0{,}000$
Conclusión	Por tanto $p < 0{,}01$, se rechaza hipótesis nula y se acepta la hipótesis alterna, concluyendo que existe relación significativa de la gestión de tecnología de información y comunicación con la seguridad informática en el gobierno regional de Apurímac, 2021.

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Hipótesis específicas

Tabla 15

Relación de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática

Correlaciones			
		Gestión de tecnologías de información y comunicación	Procesos -SI
Gestión de tecnologías de información y comunicación	Correlación de Pearson	1	,490**
	Sig. (bilateral)		,000
	N	68	68
Procesos-SI	Correlación de Pearson	,490**	1
	Sig. (bilateral)	,000	
	N	68	68
**. La correlación es significativa en el nivel 0,01 (2 colas).			

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 16

Análisis e interpretación

Hipótesis estadísticas	Ho: No existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021.
	Ha: Existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021.
Nivel de significación	$\alpha = 0{,}01$
Coeficiente de correlación r de Pearson	0,490**
Valor p calculado	$p = 0{,}000$
Conclusión	Por tanto $p < 0{,}01$, se rechaza hipótesis nula y se acepta la hipótesis alterna, concluyendo que existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021.

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 17

Asociación de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática

Correlaciones			
		Gestión de tecnologías de información y comunicación	Confidencialidad-SI
Gestión de tecnologías de información y comunicación	Correlación de Pearson	1	,467**
	Sig. (bilateral)		,000
	N	68	68
Confidencialidad-SI	Correlación de Pearson	,467**	1
	Sig. (bilateral)	,000	
	N	68	68
**. La correlación es significativa en el nivel 0,01 (2 colas).			

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 18

Análisis e interpretación

Hipótesis estadísticas	Ho: No existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021.
	Ha: Existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021.
Nivel de significación	$\alpha = 0{,}01$
Coeficiente de correlación r de Pearson	0,467**
Valor p calculado	$p = 0{,}000$
Conclusión	Por tanto $p < 0{,}01$, se rechaza hipótesis nula y se acepta la hipótesis alterna, concluyendo que existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021.

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 19

Relación de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática

Correlaciones			
		Gestión de tecnologías de información y comunicación	Integridad-SI
Gestión de tecnologías de información y comunicación	Correlación de Pearson	1	,625**
	Sig. (bilateral)		,000
	N	68	68
Integridad-SI	Correlación de Pearson	,625**	1
	Sig. (bilateral)	,000	
	N	68	68
**. La correlación es significativa en el nivel 0,01 (2 colas).			

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 20

Análisis e interpretación

Hipótesis estadísticas	Ho: No existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021.
	Ha: Existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021.
Nivel de significación	$\alpha = 0{,}01$
Coeficiente de correlación r de Pearson	0,625**
Valor p calculado	$p = 0{,}000$
Conclusión	Por tanto $p < 0{,}01$, se rechaza hipótesis nula y se acepta la hipótesis alterna, concluyendo que existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021.

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 21

Asociación de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática

Correlaciones			
		Gestión de tecnologías de información y comunicación	Disponibilidad-SI
Gestión de tecnologías de información y comunicación	Correlación de Pearson	1	,591**
	Sig. (bilateral)		,000
	N	68	68
Disponibilidad-SI	Correlación de Pearson	,591**	1
	Sig. (bilateral)	,000	
	N	68	68
**. La correlación es significativa en el nivel 0,01 (2 colas).			

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

Tabla 22

Análisis e interpretación

Hipótesis estadísticas	Ho: No existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.
	Ha: Existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.
Nivel de significación	$\alpha = 0{,}01$
Coeficiente de correlación r de Pearson	0,591**
Valor p calculado	$p = 0{,}000$
Conclusión	Por tanto $p < 0{,}01$, se rechaza hipótesis nula y se acepta la hipótesis alterna, concluyendo que existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.

Fuente: Elaboración propia de las investigadoras, cuestionario aplicado en SPSS 26.

CONCLUSIONES

Primera.- Que existe un nivel de relación significativa, positiva y consistente entre la gestión de las Tic y la seguridad informática en el gobierno regional de Apurímac, 2021, toda vez que *r* de Pearson presentó un índice de 0.663** y que *p*-valor de α=0.000 la misma es menor al nivel de significancia de 1% (*p*=0.000<0.01), ambiente presentado, latente y frecuente por las inquietudes intrínsecas de los elementos, componentes y factores que sostienen a la gestión de las TIC basadas en la infraestructura, arquitectura, talento humano, conocimientos y las relaciones de las Tic con el negocio organizacional, que se encuentran anidadas a las estrategias de afrontamiento manejadas para emprender las situaciones, escenarios y contextos de los procesos de confidencialidad, integridad y disponibilidad que exige la seguridad informática en el intercambio, identificación, almacenamiento y envió de información para la toma de decisiones oportunas en cumplimiento a las políticas de seguridad de la información y el cambio organizacional regional apurimeña.

Segunda.- También se concluye partiendo del coeficiente *r* de Pearson que dio 0.490** de índice y el *p*-valor logrado de α=0.000 siendo inferior al nivel de significancia de 1% (*p*=0.000<0.01), que determina que existe un grado de asociación significativa, positiva moderada de la gestión de las Tic y los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021, contexto reflejado por la existencia de los componentes adecuados de hardware, aplicaciones de software y talento humano que forman el desarrollo de las actividades, el funcionamiento de las tareas, el sostén de los sistemas y de las comunicaciones necesarias y suficientes que repercute positivamente en la gestión de las Tic anidadas de manera sostenida con las políticas de procedimientos, aseguramiento e identidad actualizadas que permiten efectuar la identificación, envió, almacenamiento de la información y reportar eventos e incidencias de seguridad informática e información de la entidad.

Tercera.- Además se concluye que existe un grado de asociación significativa, positiva media de la gestión de la Tic y la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021, evento establecido por la prueba de correlación *r* de Pearson que brindó un índice de 0.467** y un *p*-valor calculado de α=0.000 que es menor al nivel de significancia de 1% (*p*=0.000<0.01); escenario concebido en la unidad de tecnologías de información, donde el talento humano presenta la capacidad, habilidad y conocimientos exigidos para cumplir con la

atención, papel, funciones y procedimientos para una efectiva gestión de la Tic, las mismas se encuentran concatenadas con los accesos que son otorgados a los sistemas, a la función autorizada y reflejada en las cuentas asignadas, en el resguardo y la duplicidad de roles que se dan por la poca o nula actualización de la matiz funcional y confidencialidad de la seguridad informática que incide en la operatividad del servicio por las fugas y filtraciones de información en la institución.

Cuarta.- De otra parte se llega a la conclusión en base al coeficiente *r* de Pearson donde el índice fue 0.625** y el *p*-valor calculado de α=0.000 siendo menor al nivel de significancia de 1% (*p*=0.000<0.01), determinando que existe un nivel de relación significativa, positiva y contundente entre la gestión de la Tic con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021; espacio manifestado por el respaldo y apoyo de las autoridades y demás dependencias de la organización que recibe la unidad de tecnología de información y servicios informáticos que permiten apalancar los objetivos establecidos en los planes operativos anuales y la gestión de los procedimientos técnicos operativos de las Tic alojadas en la integridad para la seguridad informática, donde los usuarios de las distintas dependencias de la entidad no sean afectados por ataques de phishing para la protección de los datos contra el acceso y la modificación no autorizado e inapropiado en busca de mantener las cualidades de validez, consistencia y exactitud de los datos en la organización.

Quinta.- Al final se concluye que existe un grado de asociación significativa, positiva y fuerte entre la gestión de la Tic con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021; basado por la prueba *r* de Pearson que proporcionó 0.591** de índice y el *p*-valor calculado de α=0.000 siendo inferior al nivel de significancia de 1% (*p*=0.000<0.01); entorno sostenido por la normativa existente para la clasificación de los activos de la información de las diferentes unidades orgánicas, y de la existencia de instrumentos que ayudan con efectividad a la gestión de las Tic que se encuentran entrelazadas con las metodologías aplicadas en la gestión de roles de las diferentes unidades para que la información se encuentre disponible cuando el usuario o sistema lo requiera y puedan realizar las consultas respectivas toda vez que los requerimientos enviados fuera de los tiempos sea por contingencias de los elementos de las Tic y/o en la seguridad informática inciden de manera negativa en la operatividad institucional.

RECOMENDACIONES

Primera.- A la alta gerencia y a los responsables de la unidad de tecnologías de información y comunicación del gobierno regional de Apurímac deben diseñar acciones base para innovar los procesos, herramientas y roles de las diferentes unidades de la entidad, toda vez que al determinar que la gestión de las Tic se encuentra relacionado de manera consistente y sólida a la seguridad informática, entorno que refleja que se debe abordar cada problemática de manera asociada, anidada e integral, concibiendo que las mismas actúan como fenómenos correlacionados a consecuencia de sus elementos y hechos extrínsecos e intrínsecos que expresan las características y naturaleza enmarañada para la validez, consistencia, almacenamiento, exactitud, seguimiento, monitoreo y resguardo de los datos e información para toma de decisiones oportunas y efectivas, donde en el abordaje se deben englobar acciones, actividades y tareas puntualizadas que deben ser previstas en su plan estratégico institucional y en su plan operativo anual de la unidad de tecnologías de información y de toda la entidad regional de Apurímac.

Segunda.- A las distintas unidades, la oficina de tecnologías de información o a los que hagan las veces del gobierno regional de Apurímac, deben establecer y contar con una línea sería de acciones base respecto a la gestión de las tecnologías de información y comunicación que están interrelacionadas con los procesos de la seguridad informática en la organización para continuar manteniendo y/o innovar de manera oportuna los componentes y accesorios de hardware, software, redes y comunicación tecnológica, en busca del funcionamiento, sostén, seguridad de los sistemas e información y su consecuente priorización dentro las políticas de procedimientos, aseguramiento, identificación, envió, almacenamiento oportuno de la información en busca de la toma de decisiones efectivas por parte de los responsables de la vigente gestión regional.

Tercera.- A los integrantes de la toma de decisiones, talento humano de la unidad de tecnología o al que haga de sus veces del gobierno regional de Apurímac, deben estructurar planes de acciones concretas para mantener y/o modernizar la gestión de las tecnologías de información y comunicación asociando a la confidencialidad de la seguridad informática por parte del talento humano, quienes deben presentar dominio, capacidad, habilidad, actitudes y conocimientos tendientes a cumplir la función, atención y los roles asignados a los usuarios de modo que se encaminen, desarrollen decisiones precisas en la otorgación de accesos y asignación de cuentas

de los sistemas y tecnologías de información, para revertir la poca o nula actualización de la matiz funcional, operacional y confidencialidad de la información, y llegar a eliminar y/o evitar fugas, filtraciones, modificaciones, hackers y entre otros ataques cibernéticos internos y externos en la organización que incide la operatividad de los servicios organizacionales de manera desfavorable.

Cuarta.- Al talento humano de la oficina de tecnologías de información y de otras dependencias del gobierno regional de Apurímac; deben establecer acciones estratégicas, sobrias y confiables de mejora continua para una satisfactoria gestión de las Tic enmarcadas, sumidas en una articulación, ejecución y operatividad eficiente de integridad de la información, para evitar que los usuarios de los sistemas automatizados sean atacados por phising, la protección de los bancos y bases de datos frente a accesos y modificaciones no autorizadas e inapropiadas para fortalecer las cualidades de oportunidad, validez, consistencia y exactitud de la información en la toma de decisiones por los ejecutivos de la organización regional.

Quinta.- A los gerentes, directivos, responsables y operadores de tecnologías de información, comunicación y de la seguridad informática del gobierno regional de Apurímac, así como de las organizaciones estatales y privadas, investigadores e individuos conmovidos en la problemática abordada; deben reflexionar y ahondar profundamente de estos y otros factores de éxito en próximas investigaciones, especialmente en el interés de contar, orientar y poner en práctica acciones estratégicas tendientes al mejoramiento continuo de la gestión de las Tic con la unificación directa e integrada a la disponibilidad efectiva de la información como factor categórico de la seguridad informática, en vista que las metodologías aplicadas para realizar las consultas respectivas deben estar basadas en los requerimientos pertinentes y enviados de manera oportuna para la toma de decisiones oportunas y la operatividad institucional efectiva.

ASPECTOS ADMINISTRATIVOS

Recursos: potencial humano

- Br. ALEJANDRINA HUAYLLA QUISPE; Bachiller en Ingeniería de Sistemas e Informática, Facultad de Ingeniería, Universidad Tecnológica de los Andes, sede Abancay (Tesista).
- Br. MARINA VARGAS PANCORBO; Bachiller en Ingeniería de Sistemas e Informática, Facultad de Ingeniería, Universidad Tecnológica de los Andes, sede Abancay (Tesista).

- Asesor interno y externo de la Tesis: temático y metodológico.
- Directivos del gobierno regional de Apurímac.
- Empleados o unidades muéstrales del gobierno regional de Apurímac.
- Dictaminantes y jurados de grado.

Recursos materiales

- PC´s (Computadora personal).
- Impresora
- DVD´s.
- Flas memory (USB).
- Libros y textos.
- Fotocopias.
- Hojas
- Internet
- Otros.

Cronograma de actividades

N°	DETALLES	CRONOGRAMA AÑO 2021																				RESPONSABLES
		May.				Jun.				Jul.				Ago.				Sep.				
1	Planteamiento, diseño y construcción del problema.																					Tesista - Asesor.
2	Analisis y confección del marco teórico.																					Tesista - Asesor.
3	Redacción y confección del proyecto de tesis.																					Tesista - Asesor.
4	Presentación y aprobación del proyecto de tesis.																					Tesista - Dictaminantes
5	Análisis, diseño y construcción de instrumentos de recolección de datos.																					Tesista - Asesor y Expertos.
6	Ejecución y administración de los instrumentos de recolección de datos.																					Tesista - Colaboradores.
7	Procesamiento, análisis e interpretación de resultados.																					Tesista - Asesor.
8	Redacción y transcripción de la tesis.																					Tesista - Asesor.
9	Anillado y empastado de la tesis.																					Tesista - Imprenta.
10	Emisión, presentación y aprobación de la tesis.																					Tesista - Asesor.
11	Dictaminación de la tesis.																					Jurado dictaminador.
12	Sustentación y Aprobación del Grado.																					Tesista - Jurado de Grado Académico.

Presupuesto y financiamiento

Presupuesto

Para el desarrollo de la presente investigación se contempló recursos económicos acordes a las necesidades y requerimientos para la concreción del estudio, basados en los costos operativos siguientes:

N°	DETALLES	RECURSOS	COSTO (S/.)
1	Planteamiento, diseño y construcción del problema.	Servicio de biblioteca e internet.	150.00
2	Analisis y confección del marco teórico.	Bibliografías: libros, revistas, textos y servicio de internet	200.00
3	Redacción y confección del proyecto de Tesis.	Desarrollo, procesamiento e impresión.	1,500.00
4	Análisis, diseño y construcción de instrumentos de recolección de datos.	Computadora personal, servicio de internet e impresiones.	200.00
5	Ejecución y administración de los instrumentos de recolección de datos.	Fotocopiado de las encuestas y otros.	250.00
6	Procesamiento, análisis e interpretación de resultados.	Computadora personal, digitación y almacenamiento.	1,200.00
7	Redacción y transcripción de la tesis.	Computadora personal, digitación, almacenamiento e impresiones.	1,800.00
8	Anillado y empastado de la tesis.	Impresión de la tesis.	150.00
9	Emisión, presentación y aprobación de la Tesis.	Empastados finales de la Tesis.	200.00
10	Sustentación de la Tesis.	Inversión en la Carpeta de Grado (Derechos Académicos).	2,500.00
11	Transporte y movilidad interna y externa.	Servicio de taxí urbano y rural.	200.00
12	Imprevistos 4 %.	Para cubrir eventualidades.	417.50
TOTAL			**S/. 8,767.50**

Financiamiento

Es estudio estuvo financiado por las responsables de la ejecución de la tesis.

BIBLIOGRAFÍA

Aguilera, P. (2011). *"Redes seguras (Seguridad informática)".* Madrid, España. Editex.

Ancajima M., María A. (2019). *"Propuesta de implementación de seguridad informática en las tic de la I.E. San Miguel Arcángel, Catacaos-Piura; 2016"*. Consultado el 05/01/2021 y disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/9381/CONTROL_SEGURIDAD_ANCAJIMA_MENDOZA_MARIA_ALEJANDRA.pdf?sequence=1&isAllowed=y

Camargo R., Juan D. (2017). *"Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil CNSC basado en la norma ISO27000 e ISO27001"*. Consultado el 14/07/2021 y disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11992/75104100.pdf?sequence=1&isAllowed=y

Ca' Zorzi, Antonio (2011). *"Las TIC en el desarrollo de la PyME: Algunas experiencias de América Latina"*. Centro internacional de investigaciones para el desarrollo en colaboración con fondo multilateral de inversiones/banco interamericano de desarrollo, p. 91. Consultado el 20/12/2020 y disponible en: https://pymespracticas.typepad.com/files/tic-y-pymes-en-al-final-2011.pdf

Cortés, Gregorio (2018).*"TIC definición y componentes"*. Consultado el 02/01/2021 y disponible en: https://sites.google.com/site/tecnologiaeducativachepo/tic-antecedentes-y-definicion

Daccach, J. C. (s. f.). *"Tecnologías de la Información y Comunicaciones (TIC)*". Consultado el 12/01/2021 y disponible en: http://www.gestiopolis.com/delta/term/TER434.html

Gobierno Regional de Apurímac (2019), *"Portal Web: Allin Kawsanapaq"*. Consultado el 12/01/2021 y disponible en: http://www.regionapurimac.gob.pe/

Gómez V. Álvaro (2017). *"Enciclopedia de la Seguridad Informática".* 2da. Ed. actualizada. Edit. RA-MA. Consultado el 02/01/2021 y disponible en: https://books.google.com.pe/books?id=Bq8-DwAAQBAJ&pg=PT221&hl=es&source=gbs_selected_pages&cad=2#v=onepage&q&f=false

Guevara T., Ramiro A. (2017). *"Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnologías de la información y comunicación del distrito 18D01 de educación"*. Consultado el 19/07/2021 y disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Tesis_t1339 si.pdf

Guaylupo O., Joseph A. (2017). *"Solución holística de seguridad informática para mejorar la gestión de las tecnologías de la información y comunicación, en la dirección regional de educación de Piura, departamento de Piura en el año 2016"*. Consultado el 18/07/2021 y disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/15755/TIC_TRANSACCIONES_GUAYLUPO_OCANA_JOSEPH_ADRIAN.pdf?sequence=1&isAllowed=y

Hernández, R. Fernández, C. y Baptista, P. (2014). *"Metodología de la investigación"*, sexta edición. Editorial McGraw-Hill Interamericana. México.

Huamán A., Yuver (2018). *"Modelo de gestión de seguridad de la información con ISO/IEC 27001 para minimizar la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2018"*. Consultado el 10/07/2021 y disponible en: https://repositorio.unajma.edu.pe/handle/123456789/487

Huidobro, J. (2007). *"Informe de investigación académica sobre Tecnologías de in-formación y comunicación para Facultad de Ciencias contables: Universidad Politécnica de Madrid"*, consultado el 26/12/2020 y disponible en: http://cmap-spublic3.ihmc.us/rid=1H3108YC5-BY-QQP-R83/Tecnologias%20de%20Infor-maci%C3%B3nyComunicacion.pdf

Kendall, Kenneth E. y Kendall, Julie E. (2011). *"Análisis y diseño de sistemas"*. Pearson Educación. 8va. Edición. México. Pp. 600.

Lino S., Luis A. y Quimi R., Loraine E. (2019). *"Las tecnologías de información y comunicación (tic) y su influencia en la administración de las pequeñas empresas del ecuador 2017-2018"*. [Consultado 06 de enero de 2021] y disponible en: http://repositorio.ug.edu.ec/bitstream/redug/42756/1/%E2%80%9CLAS%20TECNOLOG%C3%8DAS%20DE%20INFORMACI%C3%93N%20Y%20COMUNICACI%C3%93N%20%28TIC%29%20Y%20SU%20INFLUENCIA%20EN%20LA%20ADMIN

ISTRACI%C3%93N%20DE%20LAS%20PEQUE%C3%91AS%20EMPRESAS%20DEL%20EC~1.pdf

Madé S., Nicolás (2006). *"Metodología de la investigación*". México. Editorial Mac Graw Hill.

Machicao M., Saulo G. (2019). *"Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) –UNA Puno 2018".* Consultado el 10/01/2021 y disponible: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/13958/Machicao_Mollocondo_Saulo_Gustavo.pdf?sequence=1&isAllowed=y

Marqués, P. (2000). "*Calidad de la formación virtual y de los materiales multimedia"*. XII Congreso Nacional I Iberoamericano de Pedagogía. Madrid.

Martín, Jessica (s.f.). *"Importancia de las TIC en las empresas". Universidad de Salamanca: Campus de excelencia internacional*. Consultado el 22/12/2020 y disponible en: https://diarium.usal.es/i_jmartin/importancia-de-las-tic-en-las-empresas/

Muñoz Ñ., Juan D. (2016). *"Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la Universidad de Cuenca"*. Consultado el 02/01/2021 y disponible en: http://dspace.ucuenca.edu.ec/bitstream/123456789/25646/1/Tesis.pdf

Molinetti, Sebastián (2019). *"Principales tipos de seguridad informática en las empresas".* Consultado el 28//12/2020 y disponible en: https://empresas.blogthinkbig.com/tipos-seguridad-informatica-empresas/

Morris A, Eddy (2009). *"Las tecnologías de la información en las empresas".* Consultado el 27 de diciembre de 2020 y disponible en: https://www.esan.edu.pe/conexion/actualidad/2009/10/10/las-tecnologias-de-la-informacion-en-las-empresas/

Ochoa S., Claudia M. (2015). *"Implementación de las tecnologías de la información y la comunicación TIC para la mejora de la gestión contable y financiera en la empresa Fundimetales"*. Consultado el 18/07/2021 y disponible en: https://repositorio.uptc.edu.co/bitstream/001/1551/1/TGT-287.pdf

Ortiz M., Einstein A. (2018). *"Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de seguridad de la información en la universidad nacional Agraria de la Selva"*. Consultado el 15/07/2021 y disponible en:

http://repositorio.unas.edu.pe/bitstream/handle/UNAS/1710/EAOM_2018.pdf?sequence=1&isAllowed=y

Rodríguez V., María T. y Peña R., José I. (2012). *"Medición de capacidad en tecnología de información en las organizaciones"*. pp. 50-65. Consultado el 10/01/2021 y disponible en: http://www.scielo.org.co/pdf/ean/n72/n72a04.pdf

Romero C., Martha I., Figueroa M., Grace L., Vera N., Denisse S., Álava C., José E., Parrales A., Galo R., Álava M., Christian J., Murillo Q., Ángel L. y Castillo M., Miriam A. (2018). *"Introducción a la seguridad informática y el análisis de vulnerabilidades".* 3 ciencias. Editorial Área de Innovación y Desarrollo,S.L. Consultado el 23/12/2020 y disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Romero O., Miguel A. (2015). *"Tecnologías de la información y la comunicación: conceptos básicos"*. Consultado el 01/01/2021 y disponible en: https://es.slideshare.net/miguelaromero5099/tecnologias-de-la-informacion-y-la-comunicacion-conceptos-basicos

Salazar C., Verónica (2019). *"Gestión de calidad con el uso de tecnología de información y comunicación y propuesta de mejora en las micro y pequeñas empresas, sector comercio, rubro ferretería, ciudad de Juanjui 2019"*. Consultado el 22/12/2020 y disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/11119/CALIDAD_COMUNICACION_SALAZAR_CASTRO_VERONICA.pdf?sequence=1&isAllowed=y

Sancho G., Juana M. (2006). *"Tecnologías para transformar la educación".* Ediciones Akal, S.A. Madrid-España. Consultado el 05 de enero de 2021 y disponible en: https://books.google.com.pe/books?id=6PYaf-sF4-wC&pg=PA9&hl=es&source=gbs_toc_r&cad=2#v=onepage&q&f=false

Santos, J. C. (2014). Seguridad y alta disponibilidad. Bogotá, Colombia: Ra-ma Editorial.

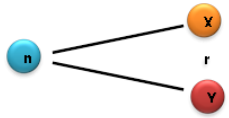
Universidad internacional de Valencia (2018). *"¿Qué es la seguridad informática y cómo puede ayudarme?".* Consultado el 10/12/2020 y disponible en: https://www.

universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

ANEXOS

Matriz de Consistencia

Título: "Gestión de tecnologías de información y comunicación y los procesos de seguridad informática en el gobierno regional de Apurímac, 2021"

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES/ DIMENSIONES	METODOLOGÍA
¿De qué manera la gestión de tecnología de información y comunicación se relacionan con los procesos de seguridad informática en el gobierno regional de Apurímac, 2021?	Determinar la relación existente entre la gestión de tecnología de información y comunicación con los procesos de seguridad informática en el gobierno regional de Apurímac, 2021.	Existe relación significativa entre la gestión de tecnología de información y comunicación con los procesos de seguridad informática en el gobierno regional de Apurímac, 2021.	**Variable de estudio X:** Gestión de tecnología de información y comunicación (TIC) **Variable de estudio Y:** Seguridad informática (SI)	**Enfoque:** Cuantitativo **Tipo:** Básica o fundamental **Nivel o alcance:** Correlacional-descriptivo **Diseño:** No experimental-transeccional
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICAS**	**DIMENSIONES**	
1. ¿Cuál es el nivel de relación de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021? 2. ¿Cuál es el grado de asociación de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021? 3. ¿Cuál es el nivel de relación de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021? 4. ¿Cuál es el grado de asociación de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021?	1. Determinar el nivel de relación de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021. 2. Determinar el grado de asociación de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021. 3. Determinar el nivel de relación de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021. 4.Determinar el grado de asociación de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.	1. Existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con los procesos de la seguridad informática en el gobierno regional de Apurímac, 2021. 2. Existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la confidencialidad de la seguridad informática en el gobierno regional de Apurímac, 2021. 3. Existe un nivel de relación significativa de la gestión de tecnología de información y comunicación con la integridad de la seguridad informática en el gobierno regional de Apurímac, 2021. 4. Existe un grado de asociación significativa de la gestión de tecnología de información y comunicación con la disponibilidad de la seguridad informática en el gobierno regional de Apurímac, 2021.	**VX: Gestión de tecnología de información y comunicación (TIC):** Infraestructura Arquitectura Talento humano Conocimiento Relaciones de la TIC con el negocio **VY: Seguridad informática (SI):** Procesos. Confidencialidad. Integridad. Disponibilidad.	 **Donde:** n = Muestra de estudio X = Gestión de tecnología de información y comunicación (TIC) Y = Seguridad informática (SI) r = Relación entre variables. **Población, muestra y muestreo:** **Población:** El talento humano de las unidades del gobierno regional de Apurímac. Total (82) empleados. **Muestra:** Se obtuvo de manera probabilística por la fórmula de Cochran, tamaño de la muestra: 68 sujetos. **Muestreo:** por el muestreo aleatorio simple **Técnicas e instrumentos de recolección de datos:** VARIABLE DE ESTUDIO / TÉCNICA / INSTRUMENTO Gestión de tecnologías de información y comunicación (TIC) — Encuesta — Cuestionario Seguridad informática (SI) — Encuesta — Cuestionario **Procedimientos, presentación, análisis e interpretación de datos:** A partir de la estadística descriptiva, cuyos datos serán procesados y tabulados de manera numérica en tablas y figuras correspondientes aplicando el software estadístico: SPSS 24, Excel 2016 y Word 2016.

CUESTIONARIO DE MEDICIÓN PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y LOS PROCESOS DE SEGURIDAD INFORMÁTICA EN EL GOBIERNO REGIONAL DE APURIMAC, 2021

INTRODUCCIÓN.

Estimado colaborador el cuestionario es parte de un estudio de investigación que permitirá captar datos e información sobre la "La gestión de tecnologías de información y comunicación y los procesos de seguridad informática en el gobierno regional de Apurímac, 2021"; con la finalidad de efectuar un análisis desde la perspectiva, ambiente y procesos operacionales tecnológicos integrales que se ejecutan en el gobierno local objeto de estudio.

INDICACIONES.

Se le solicita llegar a responder los ítems de acuerdo a su percepción, conocimiento de manera objetiva, sincera y responsabilidad marcando con una ☑ o una ☒ en el recuadro que más se acerque a su argumento y valoración establecida para cada interrogante.

Antes de empezar:

- No llegue a poner su nombre.
- Las respuestas serán estimadas confidencialmente de forma estricta.
- Elegir y aplicar tan sólo una respuesta.
- Es sumamente importante responder todo el cuestionario y las preguntas respectivas.

Aspectos generales:

Unidad donde labora:_____

Género: Masculino ☐ Femenino ☐ **Edad:**_____ años.

Estado civil: Soltero(a) ☐ Casado(a) ☐ Conviviente ☐ Divorciado (a) ☐

Formación Profesional: Técnico ☐ Bachiller ☐ Profesional ☐ Magister ☐

Tiempo de servicios:

Menos de 01 año……..... ☐
De 01 a 02 años.……..…. ☐
De 03 a 05 años.…….. ☐
Más de 06 años.……... ☐

Puesto que ocupa:

Gerente.……☐
Director……☐
Jefe ……..…….....☐
Analista……☐
Programador:……☐
Otros.……☐

Universidad Tecnológica de los Andes
Transformando vidas

GESTIÓN DE TECNOLÓGIA DE INFORMACIÓN Y COMUNICACIÓN

Escala Valorativa

Nunca	Casi nunca	A veces	Casi siempre	Siempre
1	2	3	4	5

N°	Ítems	Valores				
		1	2	3	4	5
Infraestructura:						
1	¿Considera que los empleados de la organización cuentan con los componentes de hardware (equipamiento) adecuados para el desarrollo de sus actividades y alcanzar los objetivos empresariales?					
2	¿Ud. considera que la institución tiene las aplicaciones de software que forman el sostén de los sistemas, funcionamiento de tareas y comunicaciones necesarias y suficientes?					
3	¿Considera Ud. que las funciones de tecnologías de comunicación se encuentran en el manual de organización y funciones de la oficina de tecnología e informática de la organización?					
4	¿Considera que las responsabilidades de las plataformas de aplicaciones están identificadas adecuadamente?					
5	¿Ud. considera que los proceso de la conectividad de las tecnologías de información y comunicación están debidamente identificadas?					
6	¿Considera que se utiliza una metodología para elaborar los procedimientos de compatibilidad técnica operativa de la tecnología de información y comunicación en la institución?					
7	¿Considera Ud. que la modularidad de los recursos físicos y la competencia del talento humano constituye la plataforma para la construcción de las aplicaciones de negocio y el entrenamiento de los empleados en tecnología de información y comunicación en la organización?					
Arquitectura:		**1**	**2**	**3**	**4**	**5**
8	¿Ud. considera que los objetivos propuestos en la planificación de trabajo de la unidad de tecnologías de información, producen los resultados esperados anualmente?					
9	¿Considera Ud. que se toman en cuenta los modelos, las políticas y las reglas que deben regir para los datos que se van a recopilar, cómo van a ser almacenados, clasificados y explotados por la infraestructura tecnológica disponible en la institución?					
10	¿Según Ud. se consideran las opciones de conectividad para los dispositivos y la cantidad aceptable de latencia del ancho de banda para mejorar la eficiencia operativa y proporcionar un mejor servicio en la organización?					
11	¿Considera que las actividades de la unidad de tecnologías de información sobre seguridad informática apoyan a los objetivos determinados en el plan estratégico organizacional para mantener confianza entre los usuarios?					
12	Considera Ud. que la institución cuenta con una política de tecnología de información y seguridad informática?					
13	¿Según Ud. se efectúan planes y programas para mitigar los riesgos identificados en los sistemas y tecnologías d información de la institución?					
14	Ud. considera que los ambientes y oficinas del personal de tecnología de información para atender y ayudar a los usuarios de manera oportuna son adecuados?					
15	¿Considera que los dispositivos-programas son compatibles con los equipos de cómputo de la institución?					
Talento humano:		**1**	**2**	**3**	**4**	**5**

16	¿Considera que los responsables de la unidad de tecnologías de información cumplen con la atención, el papel y funciones de manera oportuna?					
17	¿Considera Ud. que el talento humano que labora en la unidad de tecnologías de información cuenta con la capacidad, habilidad y conocimientos de procedimientos de seguridad informática?					

18	¿Ud. considera que la institución brinda las oportunidades, motivaciones y estímulos al talento humano de tecnologías de información?					
19	¿Considera que la institución regional proporciona los recursos necesarios y de manera oportuna a la unidad de Tic para el desarrollo de proyectos de tecnologías de información y seguridad informática?					
20	¿Ud. considera que se reporta e informa de manera oportuna y adecuada los resultados de la ejecución y cumplimiento de los procesos y planes de tecnologías de información y seguridad informática?					
21	¿Considera que los responsables de tecnologías de información de la institución ejercen un liderazgo adecuado?					
Conocimiento:		**1**	**2**	**3**	**4**	**5**
22	¿Ud. considera que las tecnologías de información y servicios informáticos con que cuenta la organización apalancan los objetivos definidos en el plan operativo anual?					
23	¿Considera Ud. que la unidad de tecnologías de información, cuenta con el respaldo y apoyo de la alta dirección y demás dependencias de la organización regional?					
24	¿Ud. considera que impactan los procesos de tecnologías de información en la institución?					
25	¿Considera Ud. que la gestión de los procedimientos técnicos operativos de las tecnologías de información y comunicación así como la seguridad informática son adecuados?					
26	¿Ud. considera que se evalúa al talento humano respecto a las capacitaciones actuales y emergentes recibidas?					
27	¿Considera que el talento humano de la unidad de tecnológica de información y demás unidades organizacionales presentan una actitud positiva para identificar los procedimientos tecnológicos y de seguridad informática?					
28	¿Ud. considera que el talento humano que labora en la unidad de tecnología de información y comunicación cuenta con conocimientos de operación y procedimientos de seguridad informática?					
Relaciones de la Tic con el negocio:		**1**	**2**	**3**	**4**	**5**
29	¿Considera Ud. que el talento humano de tecnología de información y comunicación presenta una adecuada comunicación y se expresa favorablemente en cuanto al ambiente de trabajo en la institución?					
30	¿Considera Ud. que la institución cuenta con una normativa para la clasificación de los activos de la información de las diferentes unidades orgánicas?					
31	¿Ud. considera que son conocidos los activos de información y su clasificación en la institución?					
32	¿Considera Ud. que existen herramientas y normativas que apoyan con efectividad a la gestión de las aplicaciones de tecnologías de información y seguridad informática?					
33	¿Ud. considera que los responsables del desarrollado, pruebas y pase a producción de las aplicaciones, tienen conocimiento del ciclo de vida de software?					
34	¿Considera Ud. que la incorporación de talento humano para la unidad de tecnologías de información se ejecuta con responsabilidad y es el adecuado?					
35	¿Ud. considera que se cuenta con una política clara y coherente en los proyectos de tecnologías de información y comunicación y la seguridad informática para el cambio organizacional?					

Gracias por su participación y aporte.

Universidad Tecnológica de los Andes
Transformando vidas

SEGURIDAD INFORMÁTICA

Escala Valorativa

Nunca	Casi nunca	A veces	Casi siempre	Siempre
1	2	3	4	5

N°	Afirmaciones	Valores				
		1	2	3	4	5
Procesos:						
1	¿Considera Ud. que el gobierno regional cuenta con políticas de la seguridad de la información?					
2	¿Considera Ud. que el manejo de las actividades de seguridad informática impactan en los objetivos de la seguridad de la información en la institución?					
3	Ud. considera que lo procedimientos, aseguramiento e identidad de seguridad informática se encuentran actualizados?					
4	Según Ud. la metodología empleada para el intercambio de datos y otros elementos en la institución es la apropiada?					
5	¿Considera Ud. que el gobierno regional cuenta con una unidad de seguridad informática y de la información?					
6	¿Ud. considera que la institución efectúa los controles necesarios para garantizar y proteger la información?					
7	¿Considera Ud. que existen herramientas en la organización para efectuar la identificación, envío y almacenamiento de la información en cumplimiento de la política de la seguridad de informática?					
8	¿Ud. considera que la institución cuenta con una herramienta tecnológica para reportar eventos e incidentes de seguridad informática y de la información?					
Confidencialidad:		**1**	**2**	**3**	**4**	**5**
9	¿Considera Ud. que el acceso que se otorgado está de acuerdo a la función autorizada?					
10	¿Ud. considera que el cambio de rotación de talento humano se refleja en las cuentas asignadas?					
11	¿Considera Ud. que se llegan a actualizar los roles funcionales de las áreas en la organización?					
12	¿Ud. considera que el resguardo y la duplicidad de roles es debido a que no se actualizan la matiz funcional?					
13	¿Considera que la codificación y las medidas correctivas para reducir la duplicidad de roles dan resultado?					
14	¿Ud. considera que la operatividad del servicio se ve afectada por las fugas y filtraciones?					
15	¿Considera Ud. que las custodias y los incidentes que los usuarios reportan son atendidos oportunamente?					
16	¿Ud. considera que existen directivas, reglamentos, procedimientos u otro documento que norme la gestión de accesos en la institución?					
Integridad:		**1**	**2**	**3**	**4**	**5**
17	¿Existen usuarios de las distintas dependencias de la organización que son afectados por ataques de phishing?					
18	¿Considera Ud. que las cualidades de validez, consistencia y exactitud de los datos son apropiadas en la organización?					
19	¿Para Ud. los atributos de consistencia de los datos son adecuados en el gobierno regional?					
20	¿Ud. considera que las condiciones de exactitud de los datos son pertinentes en la institución?					

21	¿Ud. considera que el resguardo y monitoreo de la información que se realiza es el adecuado?					
22	¿Considera Ud. que se efectúa el seguimiento de las vulnerabilidades en los servicios informáticos de la institución?					

23	¿Ud. considera que se desarrollan medidas correctivas a las vulnerabilidades informáticas encontradas en la organización?					
24	¿Considera Ud. que se realizan acciones para la protección de los datos contra el acceso no autorizado e inapropiado?					
25	¿Ud. Considera que se desarrollan operaciones para la protección de los datos contra la modificación no autorizado e inapropiado?					
Disponibilidad:		**1**	**2**	**3**	**4**	**5**
26	Considera Ud. que la información está disponible cuando el usuario o sistema necesite realizar una consulta?					
27	Ud. considera que existe alguna metodología para realizar la gestión de roles de las diferentes unidades del gobierno regional?					
28	¿Considera Ud. que los usuarios tienen roles de acuerdo a su perfil y productividad en la organización?					
29	Ud. considera que el flujo de datos que se maneja o se debe manejar es el adecuado en la institución?					
30	¿Considera Ud. que las tecnologías de información apoyan al sistema comunicativo y a la atención del usuario dentro el plazo establecido?					
31	¿Ud. considera que los requerimientos enviados fuera del plazo tienen inconvenientes para ser atendidos en la organización?					
32	¿Considera Ud. que los usuarios son atendidos fuera del plazo por inconvenientes en las herramientas de las tecnologías de información y seguridad informática?					
33	¿Ud. considera que el almacenamiento de la información se realiza adecuadamente?					
34	¿Considera Ud. que los requerimientos fuera del plazo inciden en la operatividad institucional?					

Gracias por su participación y aporte.

Evidencias