UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

PROGRAMA DE MESTRÍA EN INGENIERÍA DE SISTEMAS

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

MAESTRO (A) EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

AUTOR

Ing. JOSEPH ADRIÁN GUAYLUPO OCAÑA

ASESOR

Mgtr. NOÉ GREGORIO SILVA ZELADA

PIURA – PERÚ

2017

JURADO EVALUADOR DE TESIS Y ASESOR

Dr. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN
PRESIDENTE

Mgtr. MARLENY SERNAQUÉ BARRANTES
SECRETARIO

Mgtr. OSWALDO GABIEL CORONADO ZULOETA
MIEMBRO

Mgtr. NOÉ GREGORIO SILVA ZELADA
ASESOR

AGRADECIMIENTO

A todas aquellas personas que me brindaron su colaboración, sus conocimientos, experiencias, enseñanzas y que me ayudaron de manera incondicional en esta investigación.

A los representantes y funcionarios de la Dirección Regional de Educación de Piura, por las facilidades y apoyo en la realización de la investigación.

DEDICATORIA

A Dios por darme fortaleza, y a la virgen María Auxiliadora por sus bendiciones y darme la oportunidad de cumplir con este sueño trazado.

A mis hijos Sara y Sebastian, a mis Padres y a toda mi Familia por brindarme su apoyo en todos los momentos de mi vida.

RESUMEN

La presente investigación corresponde a la línea de investigación: Implementación de las Tecnologías de la Información y Comunicación (TIC), para la mejora continua de la calidad en las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica Los Ángeles de Chimbote (ULADECH Católica). El objetivo general fue implementar una solución holística de seguridad informática para mejorar la gestión de las tecnologías de información y comunicación en la Dirección Regional de Educación de Piura - DREP, en el departamento de Piura en el año 2016; las variables seleccionadas para la investigación fueron la solución holística de seguridad informática y gestión de las tecnologías de información y comunicación; la metodología de la investigación que presento es de nivel descriptivo, con un diseño no experimental, transversal. La población objetivo está conformada por 14 funcionarios de nivel estratégico de la DREP, la técnica de recolección de datos es la encuesta, y el instrumento es el cuestionario. Luego del análisis de los resultados obtenidos, se plantea como propuesta diseñar una Solución holística de seguridad informática, para mejorar la gestión de las tecnologías de la información y comunicación en la DREP. Asimismo, dentro de las principales conclusiones se determinó que la DREP presenta diversos inconvenientes dentro del manejo de la información, consecuencia de la falta de conciencia de la importancia de asegurar la información existente; ausencia de políticas que regulen las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información. La investigación concluye, con los siguientes resultados: el 64.29 % de los funcionarios indicaron que estaban en desacuerdo, mientras que el 35.71 % estaban ni de acuerdo ni en desacuerdo con la seguridad informática. Finalmente, se debe implementar una versión informática que permita obtener el valor óptimo de las tecnologías de la información, siendo la versión de COBIT 5.0, la idónea, ya que se enfoca en el gobierno empresarial de las TIC; manteniendo un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

Palabras clave: Seguridad informática, TIC, Transacciones, Beneficios.

ABSTRACT

This research corresponds to the line of research: Implementation of Information and Communication Technologies (ICT), for the continuous improvement of quality in organizations in Peru of the professional school of Systems Engineering of the Universidad Catolica Los Angeles de Chimbote (ULADECH Catolica). The general objective was to implement a holistic computer security solution to improve the management of information and communication technologies in the Regional Direction of Education – DREP, in the department of Piura in 2016; the variables selected for the research were the holistic solution of computer security and management of information and communication technologies; the methodology of the research that I present is descriptive, with a non-experimental, transversal design. The target population consists of 14 officials at the strategic level of the DREP, the technique of data collection is the survey, and the instrument is the questionnaire. After the analysis of the results, it is proposed to design a holistic IT security solution to improve the management of information and communication technologies in the DREP. In the same way, within the main conclusions it was determined that DREP has several drawbacks handling the information, as a consequence of the lack of awareness of the importance of saving the existing information; absence of policies that regulate good practices in each of the transactions, processes and resources related to information. As a general summary of the results it was obtained that 64.29% of officials indicated that they disagreed, while 35.71% were neither in agreement nor in disagreement with computer security. Finally, a computer version should be implemented to obtain the optimal value of information technologies, being the version of COBIT 5.0, the ideal one, since it focuses on the corporate governance of ICT; maintaining a balance between the realization of benefits and the optimization of risk levels and use of resources.

Key words: IT Security, ICT, Processes, Transactions, Benefits.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

I. INTRODUCCIÓN

La palabra holismo proviene de un vocablo griego (yólos) que significa todo, totalidad, por entero. Según este método de estudio se debe tomar a los sistemas físicos, biológicos, económicos, mentales, lingüísticos, sociales, etcétera, como totalidades y analizar el todo junto a las características del sistema y no sólo remitirse a las partes.

La holística considera cada sistema como un todo en que sus partes se encuentran integradas. El estudio de cada una de las partes de un todo no puede explicar cómo funciona el sistema de manera global. Un sistema es mucho más que la simple suma de las partes, por eso es que este método de estudio considera el sinergismo de las partes como importante y no la individualidad de las mismas [(1)].

A lo largo de la historia, la necesidad de almacenar y propagar la información ha cobrado cada vez más importancia, y en la actualidad son cuestiones básicas para el desarrollo de la vida humana. Muchas de las limitaciones de las primeras épocas de la informática han sido superadas, como ser las dimensiones de los dispositivos, la velocidad de procesamiento y la volatilidad de la memoria (los primeros medios de almacenamiento eran incapaces de retener los datos una vez que se interrumpía el suministro de energía eléctrica, así como ocurre con la memoria RAM), pero aún quedan muchos desafíos pendientes, siendo la estabilidad de Internet una de las principales, sin dejar de lado las diferencias abismales entre los proveedores de países desarrollados frente a los subdesarrollados [(2)].

Según AEC [(3)]; la Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Conviene aclarar que la seguridad absoluta no es posible, no existe un sistema 100 % seguro, de forma que el elemento de riesgo está siempre presente, independiente de las medidas que tomemos, por lo que se debe hablar de niveles de seguridad.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización, datos de sus clientes o proveedores, o de sus colaboradores, se guardaba en papel y se almacenaba en grandes cantidades de

abultados archivadores, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesamiento. Los sistemas informáticos permiten la digitalización de todo este volumen de información, reduciendo el espacio ocupado, pero sobre todo facilitando su acceso, análisis y rapidez en el procesamiento y mejoras en la presentación de dicha información.

La Dirección Regional de Educación de Piura – DREP, es una entidad en crecimiento que debe involucrar dentro de sus procesos buenas prácticas encaminadas a la protección de la información; razón por la cual es necesario el desarrollo del análisis de riesgo de la seguridad de la información aplicado a cada uno de los activos de información. El análisis de riesgo permite realizar un diagnóstico para conocer las debilidades y fortalezas internas, encaminadas en la generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática, que hacen parte de un Sistema de Gestión de Seguridad de la Información (SGSI), además de facilitar su continuo monitoreo a través de procesos de auditorías y mejoras continuas.

La DREP, no tiene un sistema de seguridad de la información que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la información presente en cada uno de los procesos internos; además no tiene estandarizados controles que lleven a mitigar delitos informáticos o amenazas a los que están expuestos los datos, comprometiendo la integridad, confidencialidad y disponibilidad de la información.

Existen procedimientos creados subjetivamente por iniciativa y experiencia de los miembros del equipo de TI; no obstante, no existe una política de uso de claves de usuario, dado que es en los servidores donde se realiza el cambio de claves de acceso a criterio del personal de TI sin una periodicidad y bitácora definida.

La DREP, tiene muchos inconvenientes dentro del manejo de la información debido principalmente a que viene funcionando en ambientes no diseñados para oficinas, sino para aulas de clase, además que no se ha tomado conciencia de la importancia de asegurar la información existente; a medida que avanza es necesario adoptar y crear políticas que regulen las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información y para esto, es indispensable realizar un

análisis de riesgos de la seguridad de la información, incluyendo los activos que directa e indirectamente están ligados a este proceso.

De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de riesgos; seguramente en un futuro cercano podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros.

Por lo antes caracterizado, el enunciado del problema es: ¿En qué medida la implementación de una solución holística de seguridad informática, mejorará la gestión de tecnología de información y comunicación en la Dirección Regional de Educación de Piura, en el departamento de Piura en el año 2016?

Siendo el objetivo general implementar una solución holística de seguridad informática para mejorar la gestión de tecnología de información y comunicación en la Dirección Regional de Educación de Piura, en el departamento de Piura en el año 2016. Y como objetivos específicos: (a) Revisar información bibliográfica relacionada a seguridad informática; (b) Evaluar la seguridad informática en la Dirección Regional de Educación de Piura; (c) Analizar y diseñar una solución informática holística adecuada para la Dirección Regional de Educación de Piura; (d) Implementar una solución informática holística para la Dirección Regional de Educación de Piura y e) Evaluar la seguridad informática posterior a la aplicación de la solución informática holística en la Dirección Regional de Educación de Piura.

Esta investigación se justifica por la necesidad de una solución holística de seguridad informática, para mejorar la gestión de Tecnología de información y comunicación, que permita integrar y sintetizar de manera eficiente y eficaz los proyectos tecnológicos para la Dirección Regional de Educación de Piura, en el departamento de Piura. Así mismo sirva de modelo para otras direcciones regionales de educación del país.

La Investigación está orientada a revisar las metodologías existentes en la implementación de soluciones holísticas de seguridad informática, disponibles el

mercado para encontrar coincidencias que puedan plasmarse en un nuevo modelo, que permita garantizar un elevado índice de éxito de proyectos de este tipo bajo un mismo patrón de trabajo, tomando en cuenta los siguientes aspectos: Desde el aspecto operacional: Desarrollar una solución holística de seguridad informática, que permita dar lineamientos eficientes y eficaces a la gestión de TIC con que cuenta la Dirección Regional de Educación de Piura.

En relación al aspecto económico: Una solución holística de seguridad informática para mejorar la gestión de TIC, reduce los costos de gestión de TIC de cualquier organización.

Desde el aspecto humano: Permitirá apoyar a todos los involucrados en dar lineamientos a los procesos de gestión de TIC de la organización, permitiendo un lenguaje común en la gestión del proyecto.

Finalmente, en cuanto al aspecto técnico: La metodología ágil será desarrollada de acorde a los estándares existentes de gestión de proyectos de sistemas de información y tecnologías de la información.

II. MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1. Antecedentes a nivel internacional

Estudio de sistemas de seguridad basado en la detección de intrusión física y tecnológica [4]. El objetivo de este proyecto es el análisis y estudio de todos los sistemas de seguridad cuya finalidad es la misma: Prevenir y actuar ante cualquier intrusión física y lógica. Teniendo en cuenta que con el avance de las tecnologías de la información y, con ello, la integridad, confidencialidad y disponibilidad de las mismas en redes internas y externas, es necesaria la implantación de medidas cada vez más complejas, que garanticen la seguridad tanto física como lógica de toda información de vital importancia. Como objeto de este proyecto se analizará y estudiará la propuesta de un Sistema de Seguridad Integral como un único sistema, fruto de la unificación de los sistemas de seguridad física y los sistemas de seguridad informática. Este sistema puede tenerse en cuenta frente al desarrollo del Plan de Seguridad a implantar en una instalación cualesquiera.

La correlación con la presente investigación está, en que el objetivo de un Plan de Seguridad, es la protección de todo riesgo al que nos enfrentemos con el fin de garantizar la seguridad en su mayor grado respecto del sujeto a proteger, bien sea este personas o elementos materiales o inmateriales, teniendo en cuenta que actualmente, en el mundo empresarial es imprescindible la comunicación con clientes y proveedores a través de la red: enviar y recibir correo, buscar información, realizar gestiones, etc.

La creciente evolución de Internet y las nuevas tecnologías desarrolladas en el ámbito de la seguridad, implica que paralelamente se esté produciendo un aumento de las necesidades y exigencias de los clientes con el fin de disponer de la máxima protección.

Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual[5]. En este estudio se ha auditado, recomendado e implementado políticas generales de seguridad informática y seguridad de la información de la empresa GNN7 TV, el objetivo ha sido poder manejar su sistema de gestión de la seguridad de la información siguiendo procedimientos estandarizados que permiten identificar y reducir a corto y mediano plazo los diferentes riesgos informáticos , así como incidentes que involucran a la información que pueden ser accidentales o provocados como alteraciones, accesos no autorizados, o en su defecto, fuga o pérdida de información de vital importancia para la continuidad del negocio. Mediante conversaciones con los miembros del departamento de TI y una entrevista final al responsable del área, se pudo concluir que la mayoría de los riesgos identificados de seguridad informática y seguridad de la información en la empresa eran de nivel intermedio y críticos, esto representaba un alto riesgo para la empresa por estar comprometida su información y su infraestructura tecnológica debido a que carecían de varios controles de seguridad necesarios y también porque sus políticas generales de seguridad tenían múltiples falencias. Aplicando mejoras y recomendaciones basadas en varios dominios, objetivos de control y controles de la norma ISO 27002:2005 se logró reducir gradualmente los riesgos de nivel bajo, intermedios y críticos de seguridad informática y seguridad de la información identificados al inicio de este estudio.

La correlación con la presente investigación está, en que el proyecto brinda la oportunidad de crear un esquema de procesos y buenas prácticas de seguridad informática y de información basada en la norma ISO 27002:2005, profundizando con esto el aprendizaje de procesos seguros en el tratamiento de la información.

En su parte estructural consta no solo de recomendaciones en base a una auditoría sobre cada objetivo de la norma ISO 27002:2005, sino también en el estudio y soluciones de las mismas, facilitando así la toma de

decisiones, documentación y registro de eventos sobre cualquier incidente informático y de información suscitado en la organización.

Del mismo modo se diseñaron formatos de control, actas y políticas a seguir para cada punto tratado en el proyecto, brindando así facilidad de registro eventual, pasos a seguir para mejorar la calidad de soporte brindado por el área de TI y sobre todo seguir un esquema de seguridad de procesos relacionados a la organización.

Aseguramiento de los sistemas computacionales de la empresa SITIOSDIMA.NET (6). La seguridad de un sistema informático, empieza en la elección del sistema operativo y las características implementadas en su instalación. El Hardening, es un método que permite implementar tantas estrategias como herramientas en busca de un sistema operativo más seguro. En el presente trabajo, se da a conocer en detalle, qué es Hardening, las actividades técnicas que se deberían tener en cuenta en su implementación, las configuraciones seguras y otras medidas aplicables. Seguidamente, se analizan algunas herramientas relacionadas en el uso de una estrategia se seguridad Hardening. Tras la instalación de un sistema operativo quedan puertos abiertos por defecto, se verá de qué manera considerar cuáles deben mantenerse abiertos y cuáles deben cerrarse. De igual modo, se estudian aplicaciones que permiten monitorear el flujo de información entrante y saliente del sistema operativo y, de qué forma hacer que el Firewall sea más eficaz.

La correlación con la presente investigación está, en que actualmente las empresas se encuentran inmersas en el manejo de las nuevas tecnologías de la información, lo que conlleva nuevos desafíos frente a procesos enmarcados en la seguridad de la información, lo que las convierte en objetivos de ataques informáticos, tanto externos como internos.

Tomando en cuenta que la manipulación no apropiada de parte de los usuarios de los sistemas operativos, redes de datos y sistemas de información, han hecho que se presenten más opciones para los

delincuentes informáticos, por lo que el aseguramiento en profundidad de las TIC, toma una importancia vital para ser proactivos frente a posibles intrusiones, esto con el fin de limitar en lo posible vulnerabilidades y evitar pérdida de información o manipulación de los equipos comprometidos. Es por eso que al aplicar técnicas de aseguramiento Hardening en los sistemas operativos de las empresas, se minimizan los riesgos y se evitan pérdidas económicas, afectación de la imagen de la empresa, entre otras consecuencias.

No obstante, se tiene que tener en cuenta que para que cualquier proceso de aseguramiento sea exitoso, debe ser complementado con políticas de seguridad de alta exigencia, y que a su vez requiere de una adecuada capacitación tanto a administradores de sistemas de información, como a los usuarios de los mismos. Aun así, se entiende que no hay sistema totalmente inmune a cualquier vulnerabilidad, hay conocimiento que implementar un proceso de aseguramiento Hardening, es un paso muy importante en pro de la seguridad informática de cualquier organización.

2.1.2. Antecedentes a nivel nacional

Sistema de monitoreo de seguridad física en plataforma libre de componentes electrónicos para asegurar la gestión de los niveles de continuidad de los servicios informáticos en la central de datos USAT[7]. La hipótesis indica que “La implementación de un sistema de monitoreo de seguridad física mejora la gestión de los niveles de continuidad de los servicios informáticos de la central de datos USAT.” en lo esencial, describe todos los procesos, ventajas y desventajas de la implementación de la propuesta, teniendo como objetivo principal asegurar la continuidad de los servicios informáticos que brinda la central de datos protegiendo desde una perspectiva holística de seguridad física el hardware instalado. El entorno donde se aplica esta investigación es un diseño cuasi experimental y nuestra población fue dividida en zonas específicas de la central de datos compuestas por equipos informáticos de acuerdo a los indicadores establecidos. Se utilizó una metodología de desarrollo de

proyectos de hardware libre la cual ha garantizado en todos los hitos el correcto desarrollo de la solución propuesta.

La correlación con la presente investigación está, en que los costos operativos que conlleva la adquisición de equipos informáticos nuevos por reposición se afectan positivamente debido a que se reducen significativamente las averías en los equipos informáticos instalados en la organización, provocadas por problemas diversos. Así mismo, con un sistema de seguridad física implantado se logrará reducir el riesgo de posibles robos de equipos informáticos, salvaguardando de esta manera el patrimonio tecnológico de la organización, asegurando los niveles de continuidad de los sistemas de información del negocio y reduciendo los costos operativos.

Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo (8). El presente trabajo de investigación se enfoca en elaboración de una Guía de implementación de la seguridad basada en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas de información en la institución Policial Comisaria del Norte – Chiclayo.

Para la obtención de dicha información y recolección de datos se consideró conveniente el uso de las técnicas de recolección de datos tales como encuestas, entrevistas, así como fichas de observación, como medio para poder extraer la información y su posterior interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO/IEC 27001, lográndose determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de dicha institución.

Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación. Se logró incrementar los procedimientos utilizados en favor de la Institución permitiéndole la detección de anomalías en la

seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. Con el Plan de tratamiento de Riesgos, se permitió la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la institución, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos. Finalmente, con el Plan de Capacitación y Concienciación puesto en marcha en la Institución, se pudo incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución.

Una correcta implementación de la Guía desarrollada en el presente trabajo de investigación permite incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, lo cual se manifiesta en el incremento de políticas de seguridad puestas en marcha que benefician a la institución y ayudan a incrementar el nivel de seguridad en la misma.

La correlación con la presente investigación es, debido a que hoy en día, en las organizaciones es de suma importancia determinar si los controles implementados son eficientes y suficientes, identificar las causas de los problemas existentes en los sistemas de información y a su vez las áreas de oportunidad que puedan encontrarse, identificando causas y soluciones a problemas específicos de los sistemas de información, que pueden estar afectando la operación y las estrategias del negocio; así como las acciones preventivas y correctivas necesarias para mantener los sistemas de información confiables y disponibles.

Así pues, las empresas en la actualidad se están sistematizando y utilizando herramientas, equipos informáticos y personal capacitado para facilitar los procesos de trabajo y obtener así un mayor rendimiento laboral. No obstante, la mayoría de estas empresas no le dan la suficiente

importancia a la auditoría de sistemas, creyendo que este tipo de herramienta no les corresponde y lo ven como un gasto y no como una inversión; es por eso que una guía de implementación de seguridad de sistemas de información es básico y necesario. En esa guía se puede gestionar la tecnología de la información en las entidades, a través de auditorías internas y externas.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. (9). La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma.

Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo.

En consecuencia, se realizaron varias reuniones con la alta dirección que permitieran definir el alcance y las políticas del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, posteriormente se realizó una serie de entrevistas que permitieran identificar y valorar los activos críticos de la organización, así como identificar y evaluar los riesgos a los cuales estos estaban sometidos.

Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

La correlación con la presente investigación es, que la necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las empresas deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos más importantes dentro de las organizaciones llegando a tener una importancia estratégica para muchas de ellas ya que les permite mantener una ventaja competitiva frente a otras empresas.

La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información, es decir, busca protegerla tanto de ataques físicos, tales como robos o incendios, como de ataques cibernéticos, tales como el aprovechar vulnerabilidades de los sistemas de información.

En nuestro país, desde hace más de diez años, las políticas del gobierno han ido recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la norma técnica peruana (NTP) ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la seguridad de la información.

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la

Información (SGSI), basándose en la NTP – ISO/IEC 27001:2008 mediante la resolución ministerial N° 129-2012-PCM emitida en mayo del 2012.

2.1.3. Antecedentes a nivel local

Propuesta de un plan de auditoría informática para el "Sistema de información en salud" y el "Aplicativo para el registro de formatos SIS" en los establecimientos de salud de la unidad ejecutora 400 en la Región Piura en el año 2015 (10). El presente trabajo de tesis tiene como objetivo principal proponer un plan de auditoría informática para los dos sistemas más importantes de cada establecimiento de salud, los cuales son el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.

Para alcanzar dicho objetivo, se ha planteado los siguientes objetivos específicos:

- Conocer la organización, normas y procedimientos de la Unidad Ejecutora 400 de la Región Piura donde para el cual se realizará la propuesta del Plan de Auditoría.
- Establecer los objetivos de control y los procedimientos de auditoría a aplicar sobre el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.
- Determinar el programa de auditoría que se utilizará de guía para ejecutar el Plan de Auditoría.

Al respecto, la propuesta del plan de auditoría informática se ha realizado en base a la Guía de Control Interno de las entidades del Estado Peruano para realizar un análisis de riesgos de ambos sistemas de información basadas en encuestas aplicadas a l0 establecimientos de salud, además se aplicó la Norma Técnica Peruana ISO 27001: 2008 con la finalidad de establecer los objetivos y procedimientos de control adaptados a los establecimientos de salud para posteriormente plasmarlo en el programa

detallado de auditoría informática y aplicarlo en un futuro mediante el papel de trabajo por cada procedimiento de control.

Todo esto con la finalidad de brindar una guía para las futuras auditorías a los sistemas informáticos del estado peruano, tomando como base la propuesta del plan de auditoría informática y a la vez facilitando la identificación de los riesgos existentes asociados a los controles de los procesos informáticos que acarrea cada sistema, los cuales pueden afectar el logro de los objetivos y metas de cada institución.

La correlación con la presente investigación es, que las exigencias de un mercado cada vez más competitivo plantean nuevos desafíos, que son imposibles de alcanzar sin la incorporación de la tecnología adecuada para el manejo de la información que cada empresa desarrolla día a día, la cual está sujeta a amenazas tanto de índole externa como interna.

La información en la empresa es uno de los activos más importantes que posee y por ende se debería desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información.

En los sin número de establecimientos de salud a nivel nacional, que utilizan diversos sistemas de información, se genera información muy relevante en los cuales la información es uno de los pilares más importantes, teniendo que brindársele la seguridad pertinente, mes a mes que se genera.

Es por eso que la propuesta de auditoria informática es de vital importancia para que cuando se presente algún tipo de inconveniente o supervisión se tenga una ayuda para saber cómo actuar frente a alguna amenaza que puede poner en riesgo la información, o en general para que se evalúen los sistemas de información desde sus entradas, procedimientos, controles, archivos, seguridad, etc.

Estudio y diseño de red de datos y cámaras de seguridad en la empresa REGENDA H Y D Inversiones y Servicios EIRL. Castilla – Piura;

2016[11]. La presente investigación corresponde a la línea de investigación: Implementación de las Tecnologías de la Información y Comunicación para la mejora continua en las empresas del Perú de la escuela profesional de Ingeniería de Sistemas, cuyo objetivo general fue: Estudio y Diseño de Red de Datos y Cámaras de Seguridad en la Empresa REGENDA H Y D INVERSIONES Y SERVICIOS EIRL Castilla – Piura; 2016, para mejorar la conectividad en las oficinas administrativas de la empresa. La investigación tuvo un diseño no experimental, siendo el tipo de la investigación descriptivo y de corte transversal. Se delimitó una población muestral de 23 trabajadores que hacen uso de las tecnologías de información y comunicación en las oficinas y que están relacionados con el tema de la investigación, obteniéndose los siguientes resultados: el 95.65 % de los trabajadores administrativos encuestados expresaron que No están satisfechos con la red actual en la empresa, el 91.30 % de los trabajadores administrativos encuestados expresaron que NO perciben ningún tipo de seguridad interna de la empresa y finalmente el 95.65% de los trabajadores administrativos encuestados expresaron que si es necesario realizar el diseño de una red de datos y cámaras de seguridad en nuestra empresa; motivo por el cual queda demostrada la necesidad de realizar el diseño para la Red de Datos y Cámaras de Seguridad en la empresa REGENDA H Y D INVERSIONES Y SERVICIOS EIRL Castilla –. Piura. Asimismo, se puede concluir que la hipótesis general propuesta queda aceptada.

La correlación con la presente investigación es, que en la actualidad las TIC se han convertido en el eje vertebral de diversas entidades, como empresas, instituciones y organizaciones ya sean públicas o privadas, ya que rompen fronteras y acortan distancias, lo que redunda en beneficios para la entidad en sí, como para sus usuarios internos y/o externos. Es así que durante las últimas décadas ha habido un enorme crecimiento en lo que respecta las redes de datos, cableadas o inalámbricas. Muchas de ellas sin embargo se desarrollan utilizando implementaciones de

hardware y software diferentes y hasta poco acorde con la necesidad propia de la entidad.

La necesidad de contar con una adecuada red de datos, recae en obtener una mejor administración y desarrollo de los recursos financieros, humanos, logísticos, etc., lo cual es fundamental para que la entidad obtenga información exacta y en el momento indicado, de modo que la dirección tenga un apoyo y se le facilite el desarrollo de sus actividades de manera eficaz y confiable.

2.2. BASES TEÓRICAS

2.2.1. Dirección Regional de Educación de Piura.

Resumen

En las décadas del 60 y 70 la administración de la educación de Piura dependía de la Primera Región de Educación con sede en la ciudad de Chiclayo, del departamento de Lambayeque. En estos años las gestiones administrativas se realizaban, primero desde la capital del Perú y luego desde Lambayeque. La sede educacional de Piura fue conocida como la Zona de Educación N° 13 y en Tumbes funcionó la Zona de Educación N° 12.

Esta estructura se mantuvo hasta el año 1978 en que mediante el DS. N° 007-78/ED, se desvincula de la Primera Región de Educación de Chiclayo y se convierte en la Novena Región de Educación de Piura, la misma que administraba además la Zona de Educación N° 92 con su área de ejecución en el departamento fronterizo de Tumbes.

Ubicación

La Dirección Regional de Educación de Piura se encuentra ubicada en la Prolongación Grau cuadra. 22, en el distrito 26 de octubre, en la provincia y departamento de Piura.

Giro del Negocio

La Dirección Regional de Educación de Piura – DREP, es una institución pública que tiene como función principal Regular la buena marcha Pedagógica y Administrativa correspondiente a la Educación Básica Regular – EBR, Educación Básica Especial – EBE, Educación Básica Alternativa – EBA y la Educación Superior no Universitaria de la región Piura, agrupadas en sus 12 Unidades de Gestión Educativa Local – UGEL. Así mismo tiene el reto de diseñar estrategias que permitan garantizar el aprendizaje de nuestros escolares, y desarrollar una gestión administrativa eficaz.

Misión

La dirección Regional de Educación Piura, promueve la participación activa, concertada y sostenida del estado con la sociedad civil, para la consecución de una educación democrática y de calidad, prioritariamente de la Escuela Pública en la Zona Rural y Urbano Marginal, orientada a la formación de los actores sociales, con capacidad de generar mayores condiciones de vida a favor del Desarrollo Humano sostenible.

Visión

Al 2021, las personas que viven en la región Piura acceden con equidad a una educación de calidad, que les forme como ciudadanas y ciudadanos que asumen su identidad, consolidan su proyecto de vida, aportan al desarrollo humano y construyen una sociedad democrática y ética, en el marco del proceso de descentralización del país y en corresponsabilidad con la comunidad Educativa.

Objetivo General

Mejorar la calidad y ampliar la cobertura de los servicios de saneamiento básico, educación, salud y nutrición, priorizando la atención a la población menos favorecida como soporte del desarrollo regional.

Objetivos Específicos

1. Apoyar y ejecuta las acciones de carácter multidisciplinario vinculada a la gestión educativa.
2. Mejorar la calidad y ampliar la cobertura de la Educación Básica, priorizando las zonas de menor desarrollo relativo, áreas rurales y de frontera, garantizando una formación integral y dotando de material educativo a los docente y alumnos.
3. Posibilidad que los adolescentes y jóvenes alcancen una formación integral que permita la consecución de logros de aprendizaje y una salida formación en valores.
4. Garantizar la calidad de servicio educativo en los centros de educación técnico productiva, ocupacional y centros educativos especiales.

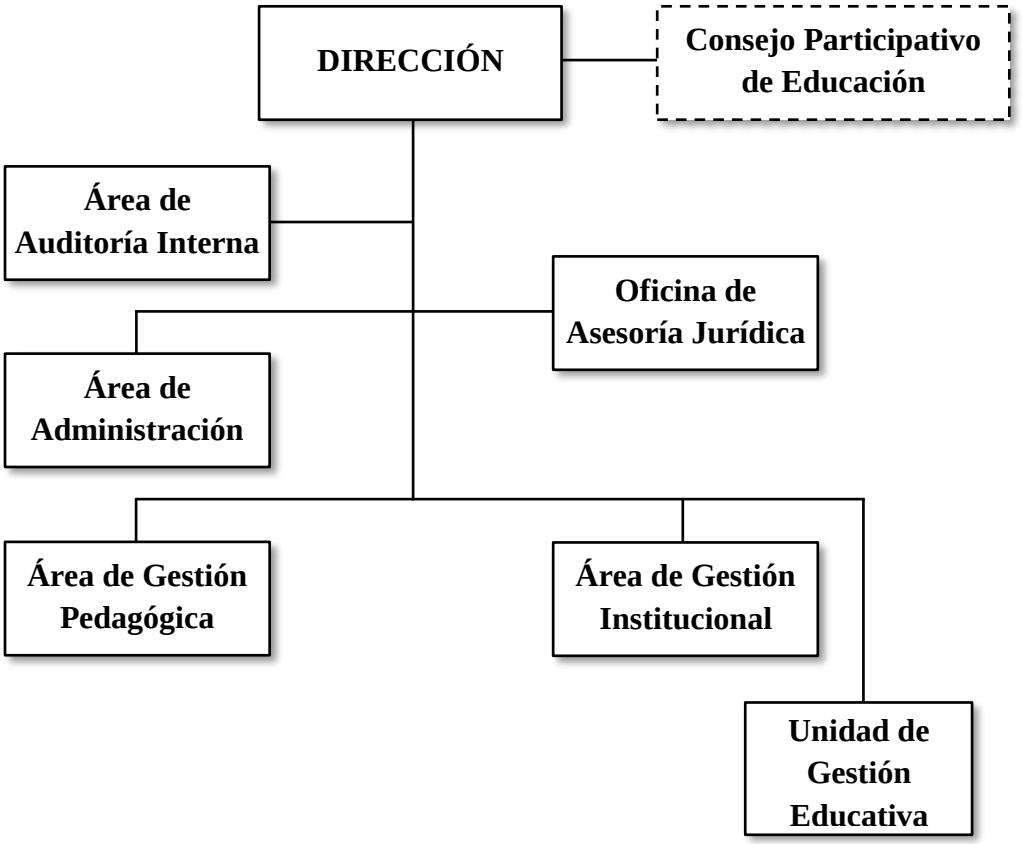
Funciones

La Dirección Regional de Educación de Piura tiene las siguientes funciones:

a. Aplicar y ejecutar la política educativa nacional emitida por el MINEDU y evaluar su implementación en la jurisdicción del departamento de Piura.
b. Diseñar y proponer al MINEDU, planes de intervención en el departamento de Piura, en concordancia con la política educativa nacional.
c. Emitir disposiciones para la diversificación curricular en el departamento de Piura, en concordancia con la política educativa nacional.
d. Supervisar los servicios brindados por las UGEL del departamento de Piura, referidos a la educación básica y técnico-productiva, en concordancia con la política educativa nacional emitida por el MINEDU.

e. Dirigir la gestión de los servicios de educación superior técnica, artística y pedagógica del departamento de Piura, en el ámbito de su competencia y en concordancia con la política educativa nacional.
f. Autorizar, crear, coordinar y supervisar el funcionamiento de las instituciones educativas de educación básica y técnico-productiva, públicas y privadas, en coordinación con las UGEL del departamento de Piura y conforme a la normativa aplicable.
g. Celebrar convenios de colaboración que contribuyan al mejoramiento de la calidad del servicio educativo en el departamento de Piura, en el ámbito de su competencia.
h. Promover la implementación de mecanismos de participación para garantizar una gestión transparente y equitativa.
i. Coordinar con la Dirección General de Gestión Descentralizada del MINEDU, en las materias de su competencia.
j. Actuar como instancia administrativa en los asuntos de su competencia.
k. Otras que, en el marco de sus competencias, le sean asignadas.

Organigrama



Fuente: Portal web institucional de la Dirección Regional de Educación Piura.

2.2.2. Las Tecnologías de Información y Comunicación (TIC)

2.2.2.1. Definición

Teniendo en cuenta el rol que desempeña la "Tecnología de Información y Comunicación" (TIC) en la era actual, resulta estratégico hacer operativo este concepto. Y no para buscar una definición uniforme, sino con el objetivo de analizarlo desde una perspectiva académica. Dado que no existe una única definición sobre TIC, se elaboró un benchmarking (enfoque comparativo y lógico orientado a comprender y evaluar de manera objetiva las fortalezas y debilidades de un determinado objeto de estudio) que recopiló, analizó y clasificó qué entienden por este concepto distintos organismos internacionales, así como entidades educativas. Este trabajo propone una definición sobre estas tecnologías, una metodología de análisis y una propuesta conceptual sobre las competencias digitales en entornos de aprendizaje [12].

Los resultados del benchmarking con el propósito de recolectar y analizar aquellas definiciones existentes, sobre el término tecnologías de información y comunicación y utilizando una muestra de más de 20 organismos públicos o privados, nacionales o internacionales destacados por su papel en el impulso de las TIC, dieron como mejores conceptos los siguientes:

"Las TIC se definen colectivamente como innovaciones en microelectrónica, computación (hardware y software), telecomunicaciones y optoelectrónica – microprocesadores, semiconductores, fibra óptica – que permiten el procesamiento y acumulación de enormes cantidades de información, además de una rápida distribución de la información a través de redes de comunicación. La vinculación de estos dispositivos electrónicos, permitiendo que se comuniquen entre sí, crea sistemas de información en red basados en un protocolo en común. Esto va cambiando radicalmente el acceso a la información y la estructura de la comunicación, extendiendo el alcance de la red a casi todo el mundo [...] Herramientas que las personas usan para

compartir, distribuir y reunir información, y comunicarse entre sí, o en grupos, por medio de las computadoras o las redes de computadoras interconectadas. Se trata de medios que utilizan tanto las telecomunicaciones como las tecnologías de la computación para transmitir información [...] Es esencial tener en cuenta los nuevos usos que se da a las viejas tecnologías. Por ejemplo, el mejoramiento o el reemplazo de la transmisión televisiva puede incorporar la interactividad" a lo que de otra manera sería un medio de una sola vía de comunicación. Como resultado, este medio tradicional puede tener características de una nueva TIC" (13).

"Nos referimos a ellas como una serie de nuevos medios que van desde los hipertextos, los multimedios, Internet, la realidad virtual, o la televisión por satélite. Una característica común que las definen es que estas nuevas tecnologías giran de manera interactiva en torno a las telecomunicaciones, la informática y los audiovisuales y su combinación, como son los multimedios [...] En la actualidad, cuando hablamos de nuevas tecnologías, lo primero que se nos viene a la mente son las redes informáticas, que permiten que al interactuar los ordenadores unos con otros amplíen la potencia y funcionalidad que tienen de forma individual, permitiendo no sólo procesar información almacenada en soportes físicos, sino también acceder a recursos y servicios prestados por ordenadores situados en lugares remotos [...] Las nuevas tecnologías vendrían a diferenciarse de las tradicionales, en las posibilidades de creación de nuevos entornos comunicativos y expresivos que facilitan a los receptores la posibilidad de desarrollar nuevas experiencias formativas, expresivas y educativas" (14).

Luego de leer y analizar estas definiciones se propone una definición:

Las Tecnologías de Información y Comunicación (TIC) son: Dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información que cuentan con protocolos comunes. Estas aplicaciones, que integran medios de informática, telecomunicaciones y redes, posibilitan tanto la comunicación y

colaboración interpersonal como la multidireccional. Estas herramientas desempeñan un papel sustantivo en la generación, intercambio, difusión, gestión y acceso al conocimiento. La acelerada innovación e hibridación de estos dispositivos ha incidido en diversos escenarios. Entre ellos destacan: Las relaciones sociales, las estructuras organizacionales, los métodos de enseñanza – aprendizaje, las formas de expresión cultural, los modelos negocios, las políticas públicas, nacionales e internacionales, la producción científica, entre otros. En el contexto de las sociedades del conocimiento, estos medios pueden contribuir al desarrollo educativo, laboral, político, económico, al bienestar social, entre otros ámbitos de la vida diaria.

2.2.2.2. Áreas de aplicación de las TIC

De acuerdo a Costa [15] las TIC son herramientas para mejorar y optimizar procesos, para agilizar operaciones y las actividades empresariales, ya sea para poder capturar los datos de una manera rápida y segura (aplicación operativa) o para poder procesar estos datos, y convertirlos en información de análisis (aplicación táctica) y, por tanto, ayudar a la toma de decisiones (aplicación estratégica).

Sólo hay que ver cómo todos los procesos de las compañías están soportados actualmente por estas tecnologías:

- El proceso de planificación, ejecución y control de las operaciones dentro de la cadena de suministro con el propósito de satisfacer las necesidades del cliente con tanta eficacia como sea posible, con las herramientas SCM (Supply chain management –Administración de redes de suministro).
- El proceso productivo con los conocidos y famosos ERP (Entreprise Resource Planning o Sistemas de Gestión Integral).
- Las actividades comerciales y de marketing con las herramientas enmarcadas dentro del ámbito de la gestión de la relación con los clientes conocidos como CRM (Custormer Relationship Management).

- Los procesos de desarrollo de nuevos productos, con herramientas de CAD (Computer Aided Design).
- Y por supuesto, la mejora de las comunicaciones en el trabajo en equipo y la colaboración entre los profesionales, dentro y fuera de la propia organización, con las intranets, los correos electrónicos o las redes sociales, entre otros.

2.2.2.3. Ventajas de las TIC para las empresas

A la hora de poner en valor las ventajas de las TIC para las empresas, hay que tener muy claro que el proceso de transformación digital es imparable y que, para muchas pymes las nuevas tecnologías son la oportunidad que estaban esperando no solo para mantenerse, sino para crecer y llevar más allá sus negocios (16).

Las ventajas de las TIC, para las empresas son:

a) Apertura de mercados a nivel global gracias a la implantación y ventajas del e-commerce**.**
b) Nuevos modelos de negocio y en la relación con el cliente.
c) Automatización de servicios y procesos internos y externos.
d) Importante ahorro de costes.
e) Flexibilidad en su relación con sus empleados gracias a la implantación de soluciones de teletrabajo.
f) Fomento del trabajo colaborativo.
g) Agilidad en la toma de decisiones y respuesta rápida tanto a nivel interno como en la relación con sus clientes.
h) Mejora en la comunicación interna y externa.
i) Información precisa de nuestro mercado y clientes gracias a la implantación de soluciones Big Data.

j) Nuevas estrategias apoyadas en herramientas y estrategias de marketing digital y gestión de redes sociales.

2.2.2.4. Principales TIC utilizadas en las empresas.

Las empresas que se organizan en red son más competitivas que el resto, según un informe coordinado por la Universitat Oberta de Catalunya (UOC) que lleva el título TIC y trabajo: hacia nuevos sistemas organizativos, nuevas estructuras ocupacionales y salariales, y nuevos mecanismos de intermediación. Además, el estudio demuestra que los trabajadores de las empresas del conocimiento ganan un 35 % más que la media. Estos datos son fruto de una muestra recogida en más de 2,000 empresas catalanas representativas del tejido económico del país (17).

Con la finalidad de comprender mejor la aplicación de Internet y Comercio Electrónico en modelos de información de apoyo, presentamos un breve repaso de algunas tecnologías de vanguardia, todas ellas asociadas a la red mundial Internet.

Páginas Web Dinámicas. Con estas tecnologías existe la posibilidad de desarrollar Páginas Web que actúen de forma dinámica, comportándose de manera diferente bajo diferentes condiciones o usuarios (17).

Máquinas de Búsqueda. Se tiene ya la posibilidad de incorporar Máquinas de Búsqueda (Buscadores) que apoyen en la búsqueda de información dentro de un sitio Web (17).

Bases de Datos Relacionales y Documentales integradas al Web. Cada vez más las páginas Web son la puerta de entrada a bases de datos de muy diversos tipos (17).

Correo electrónico con interfaz Web. Hoy en día acceder al correo electrónico se hace desde cualquier parte del mundo mediante una página Web (17).

Inteligencia de Negocio. El término inteligencias empresariales se refiere al uso de datos en una empresa para facilitar la toma de decisiones. Abarca la comprensión del funcionamiento actual de la empresa, bien como la anticipación de acontecimientos futuros, con el objetivo de ofrecer conocimientos para respaldar las decisiones empresariales [17].

Big Data. Disciplina dedicada a los datos masivos que se enmarca en el sector de las tecnologías de la información y la comunicación. Esta disciplina se ocupa de todas las actividades relacionadas con los sistemas que manipulan grandes conjuntos de datos. Las dificultades más habituales vinculadas a la gestión de estas cantidades de datos se centran en la captura, el almacenamiento, búsqueda, compartición, análisis, y visualización. La tendencia a manipular grandes cantidades de datos se debe a la necesidad en muchos casos de incluir los datos relacionados del análisis en un gran conjunto de datos, como los análisis de negocio, los datos de enfermedades infecciosas o la lucha contra el crimen organizado [17].

Existen muchísimas herramientas para tratar con Big Data, como Hadoop, NoSQL, Cassandra, Business Intelligence, Machine Learning, MapReduce, entre los más conocidos, que tratan con algunos de los tres tipos de Big Data:

- Datos estructurados (Structured Data): Datos que tienen bien definidos su longitud y su formato, como las fechas, los números o las cadenas de caracteres. Se almacenan en tablas. Un ejemplo son las bases de datos relacionales y las hojas de cálculo.
- Datos no estructurados (Unstructured Data): Datos en el formato tal y como fueron recolectados, carecen de un formato específico. No se pueden almacenar dentro de una tabla ya que no se puede desgranar su información a tipos básicos de datos. Algunos ejemplos son los PDF, documentos multimedia, correos electrónicos o documentos de texto.
- Datos semi-estructurados (Semistructured Data): Datos que no se limitan a campos determinados, pero que contiene marcadores para separar los diferentes elementos. Es una información poco regular como para ser

gestionada de una forma estándar. Estos datos poseen sus propios metadatos que describen los objetos y las relaciones entre ellos, y pueden acabar siendo aceptados por convención. Un ejemplo es el HTML, el XML o el JSON.

2.2.2.5. Nivel de uso de las TIC para el planeamiento y gestión de empresas.

Consiste en el desarrollo de herramientas de gestión basadas en TIC que permitirán mayor eficiencia en el proceso de acompañamiento y gestión de las empresas. Estas herramientas acompañan el desempeño de cada empresa, a través de la utilización de indicadores y metas preestablecidas conjuntamente.

Las herramientas desarrolladas basadas en TIC pueden proporcionar información (cantidad y calidad) superior a la que se obtiene con procesos tradicionales.

El uso de TIC en la gestión de empresas tiene los siguientes objetivos:

- Profesionalizar la gestión de las empresas.
- Dar mayor transparencia a las informaciones proporcionadas por la empresa.
- Optimizar los recursos disponibles para una gestión más eficiente.
- Mejorar las oportunidades de éxito del nuevo emprendimiento.
- Implementar prácticas gerenciales más modernas y eficientes.

Factores Críticos.

- Definición de la arquitectura del sistema de gestión basado en TIC: Esta definición debe iniciarse por el elevamiento de todo el tipo de información que se desea obtener a través del sistema de gestión. Una vez definida y ordenada la información se define la arquitectura básica del sistema a ser desarrollado.

- Definición de las funciones y módulos del sistema: Definida la arquitectura básica del sistema, se debe definir las funciones y los módulos que tendrá el sistema. La arquitectura define un modelo general del sistema, en esta etapa, se deben definir los módulos específicos del sistema, así como las funciones específicas que serán atribuidas a cada módulo.
- Definición de la infraestructura de TIC para dar soporte a la herramienta de gestión: Con el sistema de gestión definido, diseñado, con sus módulos y funciones estructurados, se debe definir la infraestructura que tendrá que ser utilizada para dar soporte a la herramienta de gestión. Esta infraestructura involucra las máquinas, conectividad, Internet, red lógica y biblioteca de software.

2.2.2.6. Papel de las TIC en la empresa del siglo XXI.

La constante evolución de la tecnología, junto a la aparición de nuevas y más complejas formas de utilización de la misma y a la completa interconexión y globalización de la economía, y los sistemas, implican que, más que nunca, las Tecnologías de la Información (TIC) ofrecen extraordinarias oportunidades.

Los costos, riesgos y oportunidades hacen de las TIC; un elemento estratégico para el crecimiento, maduración y transformación de las organizaciones, pero, además, las convierte en factor crítico de éxito y de supervivencia de la empresa.

Toda organización debe considerar un plan de Gestión de TIC, que abarque actuaciones en cada uno de los siguientes aspectos:

- Dirigir: Alineamiento con los objetivos del negocio para poder construir los mecanismos necesarios para entregar valor.
- Crear: Retorno de valor de la inversión realizada en TIC. Proteger: Gestión de riesgos para preservar el valor de los activos.

- Actuar: Gestión de recursos y desarrollo del plan TIC
- Monitorizar: Evaluación de la ejecución y desempeño del plan establecido para realinear el gobierno de las TIC con el del negocio si es necesario.

2.2.3. SEGURIDAD DE LA INFORMACIÓN

2.2.3.1. Definición

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma (18).

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

2.2.3.2. Principios básicos en la Seguridad de la Información

Cuando se habla de seguridad de la información, es importante conocer el término CIA (Confidencialidad, Integridad, Disponibilidad), que presenta los principios básicos de la seguridad de la información [19].

Realizar una correcta gestión de la seguridad de la información establece como principio básico que sin los tres elementos mencionados no existe nada seguro, con que solo falle uno de los componentes nos encontramos ante un peligro para nuestra seguridad de la información.

Tenemos que recordar que ningún sistema de seguridad es completamente seguro, siempre debemos tener claro que un sistema es mucho más vulnerable de lo que pensamos. Es necesario que tengamos en cuenta las causas de los riesgos y la posibilidad de que ocurran fallos. Una vez que tenemos esto claro podemos tomar las medidas necesarias para conseguir un sistema menos vulnerable. A continuación, aclaramos cada uno de los puntos que forman la CIA:

- Confidencialidad: La confidencialidad se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.
- Integridad: Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros, cuando una violación modifica algo en la base de datos, sea por accidente o intencionado se pierde la integridad y falla el proceso.

  Por este motivo se debe proteger la información para que solo sea modificada por la misma persona, evitando así que se pierda la integridad. Una manera de proteger los datos es cifrando la información mediante un método de autenticidad como una contraseña o mediante huella digital.

- Disponibilidad: Es un pilar fundamental de la seguridad de la información, nada hacemos teniendo segura e íntegra nuestra información, si no va a estar disponible cuando el usuario o sistema necesite realizar una consulta.

  Para cumplir con la última condición tenemos que tener claro cuál será el flujo de datos que debemos manejar, para conocer donde se debe almacenar dicha información, que tipo de servicio debemos contratar, etc.

2.2.3.3. Gestión de riesgo en la Seguridad de la Información

En la seguridad informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos.

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la seguridad informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo, hay que destacar que, aunque se diferencia entre la seguridad de la información y la protección de datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su pérdida y modificación no autorizada. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la seguridad de la información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial).

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información [20].

2.2.3.4. Sistema de Gestión de Seguridad de Información (SGSI)

El Sistema de Gestión de Seguridad de la Información es el principal concepto sobre el que se conforma la norma ISO 27001.

Podemos entender por información todo el conjunto de datos que se organizan en una empresa y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

El SGSI, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

Fundamentos:

Para garantizar que el SGSI sea gestionado de forma correcta se tiene que identificar el ciclo de vida y los aspectos relevantes adoptados para garantizar su: Confidencialidad, integridad y disponibilidad.

Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un SGSI [21].

2.2.3.5. Implementar un SGSI

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) debe hacerse de forma rigurosa en la empresa. Aquí presentamos los pasos que no se pueden soslayar en una organización [22]:

Estudiar la norma ISO 27001

Se dan muchos casos de organizaciones que comienzan a introducir un SGSI antes de conocer íntegramente y comprender los alcances de la norma y sus requisitos. Es mejor estudiarla antes de aplicarla en forma sistemática.

Garantizar el compromiso de la alta dirección

Para que la certificación ISO 2100 tenga éxito es imprescindible que la dirección de la organización esté involucrada en el proyecto. No se trata solamente de que dé el visto bueno, sino que participe en la implementación, supervisión, revisión y en la mejora continua del SGSI.

Determinar la política y alcances de la seguridad de la información

Una vez logrado el compromiso de la dirección, será posible trabajar con tranquilidad en la implementación del SGSI. Seguidamente se debe determinar el alcance y definir aspectos claves, como la política de seguridad de la información, los objetivos para la seguridad de la información y las responsabilidades y reglas relacionadas con la seguridad de la información.

Definir el método para evaluar los riesgos

La norma ISO 21007 no define el modelo de evaluación de riesgos que se debe utilizar. En lugar de ello señala ciertas pautas a seguir. El modelo debe: evaluar los riesgos relacionados con confidencialidad, integridad y disponibilidad; establecer metas para mantener los riesgos en un nivel aceptable; y determinar criterios que definan cuándo el riesgo es aceptable.

Definir acciones y objetivos para gestionar los riesgos

La identificación e implementación de acciones y objetivos para la gestión de riesgos permitirán cumplir con el proceso de evaluación de riesgos, que es el siguiente paso. Dicha identificación debe tener en cuenta los criterios para establecer riesgos aceptables e inaceptables, así como obligaciones legales y regulatorias y contractuales.

Identificar, analizar y evaluar los riesgos

Luego de identificar los riesgos de seguridad que serán analizados y evaluados, se debe evaluar cómo la organización podría verse perjudicada si dichos riesgos se convirtieran en una realidad. Establezca las consecuencias en caso que la confidencialidad, integridad o disponibilidad de los recursos de información se vieran comprometidos o dañados.

Implementación de la norma ISO 27001

El plan de implementación de la norma debe incluir, entre otros aspectos, una descripción de la gestión de riesgos en la que se precise la gestión de acciones, recursos, responsabilidades y las prioridades de las acciones con respecto a la seguridad de la información. También se debe incorporar un plan de gestión de riesgos para alcanzar los objetivos, lo cual incluye el financiamiento del plan, así como la asignación de funciones y responsabilidades. Finalmente, se debe determinar las medidas necesarias para alcanzar los objetivos y la capacitación de los colaboradores que participarán directamente.

Auditoría interna, revisión del proceso y mejoras

Para garantizar el funcionamiento eficaz del SGSI, así como su continuidad, la norma ISO 27001 establece la ejecución de la auditoría interna. Igualmente, la dirección de la organización debe ejecutar evaluaciones periódicas del SGSI para asegurar el buen funcionamiento del sistema y facilitar los procedimientos que permitan encontrar mejoras.

Hacer una pre evaluación

Cuando se considere que el SGSI de la organización ya está completamente implementado y funciona como un reloj, o si tiene un avance del 90%, se recomienda realizar una pre evaluación externa del mismo varios meses antes que se realice la auditoría de certificación. La identificación de posibles fallas hará posible determinar correcciones antes de pasar a la auditoría de certificación.

Iniciar la certificación

El proceso de certificación ISO 27001 puede tomar varios meses desde la solicitud para realizarlo hasta completar la auditoría. La empresa certificadora debe cotizar el servicio y los responsables del proceso dentro de la organización deben tomar nota de todos los detalles durante la auditoría.

2.2.4. COBIT 5.0

2.2.4.1. Definición

Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute).

El 10 de abril de 2012 la ISACA publicó COBIT 5.0, que integra Val IT, Risk IT, BMIS (Business Model for Information Security) e ITA (IT Assurance Framework), también desarrollados y publicados por ISACA, además de considerar para sus procesos otros estándares internacionales, mejores prácticas y marcos de referencia como COSO, ISO-9000, ISO-31000, ISO-38500, ITIL, TOGAF y la familia ISO-27000, entre otros [23].

Esta nueva versión de COBIT fue desarrollada para ayudar a organizaciones de todos los tamaños y de cualquier sector a obtener el valor óptimo de las

tecnologías de información, tratando de satisfacer las necesidades de los interesados internos y externos mediante la creación de valor para la empresa a través de TI (Tecnologías de Información), con un enfoque de gestión holística de extremo a extremo, cumpliendo de mejor manera con leyes, regulaciones, políticas, y basándose en buenas prácticas internacionales.

COBIT 5.0 está enfocado en el gobierno empresarial de las tecnologías de información, a diferencia de su antecesor, enfocado principalmente al gobierno de TI.

2.2.4.2. Beneficios de implementar COBIT 5.0

COBIT 5.0 proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de las TI de la organización.

- COBIT 5.0 ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.
- COBIT 5.0 permite que las TIC y relacionadas se gobiernen y administren de una manera holística a nivel de toda la organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.
- Los principios y habilitadores de COBIT 5.0 son genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

2.2.4.3. Principios de COBIT 5.0

Para Osores [24], los principios de COBIT 5.0 son:

1. **Satisfacer las necesidades de los interesados**. Es crítico definir y vincular los objetivos empresariales y los objetivos relacionados con TI.

2. **Cubrir la organización de forma integral**. Las compañías deben cambiar de visión, con el objetivo de considerar el área de TI como un activo y no un costo. Los directivos deben tomar la responsabilidad de gobernar y gestionar los activos relacionados con TI dentro de sus propias funciones.
3. **Aplicar un único modelo de referencia integrado.** Usar un solo marco de gobierno integrado puede ayudar a las organizaciones a brindar valor óptimo de sus activos y recursos de TI.
4. **Posibilitar un enfoque holístico.** El gobierno de TI empresarial (GEIT) requiere de un enfoque holístico que tome en cuenta muchos componentes, también conocidos como habilitadores. Los habilitadores influyen en si algo va a funcionar o no. COBIT 5.0 incluye siete habilitadores para mejorar el GEIT, como los principios, las políticas y marcos; los procesos; la cultura; la información y la gente.
5. **Separar gobierno de la gestión.** Los procesos de gobierno aseguran que los objetivos se alcancen mediante la evaluación de las necesidades de los interesados, el establecimiento de la dirección a través de la priorización y la toma de decisiones; y el monitoreo del desempeño, el cumplimiento y el progreso. De acuerdo con los resultados de las actividades de gobierno, la administración de la empresa y de TI entonces debe planear, crear, realizar y monitorear las actividades para asegurar el alineamiento con la dirección que se estableció.

2.2.4.4. Habilitadores de COBIT 5.0

De acuerdo a lo que señala Auditoria Informática [25], los habilitadores son:

1. **Principios, políticas y marcos**. Son el vehículo para trasladar el comportamiento deseado en guías prácticas para la gestión diaria.
2. **Procesos**. Describen un conjunto de prácticas y actividades organizadas para cumplir con ciertos objetivos y producir un conjunto de salidas para alcanzar los objetivos generales relacionados con TI.

3. **Estructuras organizacionales**. Son las entidades claves en la toma de decisiones de la empresa.
4. **Cultura, ética y comportamiento**. De los individuos y de la empresa muchas veces son sobreestimados como un factor de éxito en las actividades de gobierno y gestión.
5. **Información**. Requerida para mantener la empresa en ejecución y bien gobernada. En el nivel operacional, la información es un producto clave de la empresa.
6. **Servicios, infraestructura y aplicaciones**. Incluye la infraestructura, la tecnología y las aplicaciones para proveer a la empresa los servicios y procesamiento de TI.
7. **Personas, habilidades y competencias**. Requeridas para completar con éxito las actividades y para tomar las decisiones correctas y acciones correctivas.

2.2.4.5. Gobierno y administración de TI – COBIT 5.0

El Gobierno asegura el logro de los objetivos de la Organización, al evaluar las necesidades de las partes interesadas, así como las condiciones y opciones; fijando directivas al establecer prioridades y tomar decisiones; así como monitorear el desempeño, cumplimiento y progreso, comparándolos contra las directivas y objetivos acordados (26).

La Administración planifica, construye, ejecuta y monitorea las actividades conforme a las directivas fijadas por el ente de Gobierno para lograr los objetivos de la Organización.

En otras palabras, COBIT 5.0 une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en TI, así como su uso en beneficio de las partes interesadas.

2.2.4.6. Dominios del modelo COBIT 5.0

De acuerdo a lo que señala QAP [27], los dominios del Modelo COBIT 5 son:

Evaluar, Dirigir y Monitorear.

La Gerencia de TI asegura que los objetivos de la empresa se logren mediante la evaluación de necesidades de los interesados, condiciones y opciones; establecer la dirección a través de la priorización y toma de decisiones; y monitorear el desempeño, el cumplimiento y el progreso contra la dirección y objetivos acordados en el dominio EDM. La siguiente lista muestra el alto nivel de los procesos de TI para este dominio:

- EDM01 Asegurar que se fija el Marco de Gobierno y su Mantenimiento.
- EDM02 Asegurar la Entrega de Valor.
- EDM03 Asegurar la Optimización de los Riesgos.
- EDM04 Asegurar la Optimización de los Recursos.
- EDM05 Asegurar la Transparencia a las partes interesadas.

Alinear, Planear y Organizar.

El dominio Alinear, Planificación y Organización cubre el uso de información y tecnología y la mejor manera que puede ser utilizado en una empresa para ayudar a alcanzar las metas y objetivos de la empresa. También se destaca la forma de organización y de infraestructura de TI, con el fin de lograr los resultados óptimos y para generar los mayores beneficios de la utilización de las TI. La siguiente lista muestra el alto nivel de los procesos de TI para este dominio:

- APO01 Administrar el Marco de la Administración de TI.
- APO02 Administrar la Estrategia.
- APO03 Administrar la Arquitectura Corporativa.
- APO04 Administrar la Innovación.
- APO05 Administrar el Portafolio.
- APO06 Administrar el Presupuesto y los Costos.
- APO07 Administrar el Recurso Humano.

- APO08 Administrar las Relaciones.
- APO09 Administrar los Contratos de Servicios.
- APO10 Administrar los Proveedores.
- APO11 Administrar la Calidad.
- APO12 Administrar los Riesgos.
- APO13 Administrar la Seguridad.

Construir, Adquirir e Implementar.

El dominio Construir, Adquirir e Implementar abarca la identificación de los requisitos de TI, la adquisición de la tecnología y su aplicación dentro de los procesos de negocio actuales de la empresa. En la siguiente lista se enumeran los objetivos de alto nivel de control para el dominio CAI:

- CAI01 Administrar Programas y Proyectos.
- CAI02 Administrar la Definición de Requerimientos.
- CAI03 Administrar la Identificación y Construcción de Soluciones.
- CAI04 Administrar la Disponibilidad y Capacidad.
- CAI05 Administrar la Habilitación del Cambio.
- CAI06 Administrar Cambios.
- CAI07 Administrar la Aceptación de Cambios y Transiciones.
- CAI08 Administrar el Conocimiento.
- CAI09 Administrar los Activos.
- CAI10 Administrar la Configuración.

Entregar, Servir y Dar Soporte.

El dominio Entregar, Servir y Dar Soporte se centra en los aspectos de la prestación de la tecnología de la información. Cubre áreas tales como la ejecución de las aplicaciones dentro del sistema de TI y sus resultados, así como, los procesos de soporte que permiten la ejecución eficaz y eficiente de estos sistemas informáticos. En la siguiente lista se enumeran los objetivos de alto nivel de control para el dominio ESS:

- DSS01 Administrar las Operaciones.
- DSS02 Administrar las Solicitudes de Servicios y los Incidentes.

- DSS03 Administrar Problemas.
- DSS04 Administrar la Continuidad.
- DSS05 Administrar los Servicios de Seguridad.
- DSS06 Administrar los Controles en los Procesos de Negocio.

Monitorear, Evaluar y Valorar.

El dominio Monitorear, Evaluar y Valorar se ocupa de la estrategia de una empresa en la evaluación de las necesidades de la misma y si el sistema de TI actual sigue cumpliendo los objetivos para los que fue diseñado o no, y los controles necesarios para cumplir con los requisitos reglamentarios. La supervisión también abarca la cuestión de una evaluación independiente de la eficacia del sistema de TI en su capacidad para cumplir con los objetivos del negocio y los procesos de control de la empresa por los auditores internos y externos. Los objetivos de alto nivel de control para el dominio MEA son:

- MEV01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento.
- MEV02 Monitorear, Evaluar y Valorar el Sistema de Control Interno.
- MEV03 Monitorear, Evaluar y Valorar el Cumplimiento con Requisitos Externos.

2.2.4.7. Análisis de madurez y capacidad de procesos según COBIT 5.0

Toda organización que pretenda optimizar sus recursos tecnológicos y, por lo tanto, ser más competitiva, requiere comprender el estado de los procesos que gestionan sus Sistemas de TIC, con la finalidad de establecer el Nivel de Administración y Control adecuado que debe proporcionar a sus Sistemas[28].

Para decidir el nivel adecuado, la Gerencia de TI debe realizar un estudio detallado donde se indique la realidad de su gestión actual, y su posición frente a la competencia, con esto como base podrá plantear a la Alta Gerencia las prioridades de atención, para que estos últimos puedan alinear estas necesidades con la estrategia de la empresa, y conjuntamente con la Gerencia de TI, establecer un Plan de Acción que garantice beneficios para la organización.

Ahora bien, es conocido que el desempeño de las actividades diarias de la Gerencia de TI, suele ofuscar una visión objetiva del estado de sus procesos, y por ende medir la eficiencia de su gestión. Por esto, muchas veces, las organizaciones requieren los servicios de una empresa externa, quien pueda tasar de forma imparcial el estado de sus procesos de Gestión de TIC, identificar dónde se requieren mejoras, y proponer hacia donde deben ir.

Está práctica, se traduce, sin lugar a dudas, en beneficio para la organización puesto que en la actualidad es imperativo lograr evolucionar las TIC para adecuarse a la estrategia de la empresa, funcionando entonces como optimizador de recursos y por ende las TIC agregarán valor a las actividades operacionales y de gestión empresarial en general, permitiendo a la organización obtener ventajas competitivas, permanecer en el mercado y centrarse en su negocio.

Para lograrlo, solemos basarnos en el marco de referencia COBIT (actualmente versión 5.0), que sugiere medir la madurez de los procesos a través del "Process Capability Model", el cual está basado en el estándar "ISO/IEC 15504 Software Engineering – Process Assessment Standard". Esta evaluación es muy exigente respecto a lo que debe cumplir cada proceso para ascender de nivel, y permite, entre otras cosas, lo siguiente:

- Establecer un punto de referencia para la evaluación de la capacidad.
- Realizar revisiones sobre "el estado actual" y "el estado objetivo" para asistir al órgano de Gobierno y de Gestión de la empresa en la toma de decisiones de inversiones para la mejora de procesos.
- Realizar un análisis de carencias e información sobre la planificación de mejoras para apoyar la definición de proyectos de mejora justificables.
- Proporcionar al órgano de Gobierno y de Gestión de la empresa los porcentajes de evaluación para medir y monitorizar la capacidad actual.
- Ahora bien, pasamos a explicar que el proceso de evaluación propuesto por COBIT, el Modelo de Evaluación de Procesos (PAM), este modelo ofrece una base para la evaluación de los procesos de una empresa de forma fiable, consistente y repetible, basada en la evidencia para evaluar

la capacidad de los procesos TIC. Este modelo se basa en dos dimensiones, donde se integran las Capacidades que evalúa la ISO 15504 y los Procesos propuestos por COBIT:

- **Dimensión del proceso**: En esta dimensión se definen un conjunto de procesos característicos con declaraciones de propósitos y resultado de cada proceso.
- **Dimensión de la capacidad del proceso**: Consiste en el marco de medición que abarca los seis niveles de capacidad de proceso y sus atributos de proceso.

2.2.4.8. Niveles de capacidad y atributos de procesos según COBIT 5.0

Lo que deseamos con este tipo de evaluación, es conocer la capacidad de los procesos implementados por una organización, lo que se traduce en determinar la información y los datos que los caracterizan, y el grado en el cual estos logran el propósito para el cual fueron desarrollados. Este grado será medido de acuerdo a un conjunto de Atributos de Procesos (PA), donde cada uno de estos mide un aspecto particular de su capacidad [29].

- **Nivel 0 Incompleto**. El proceso no está implementado o no alcanza su propósito. En este nivel hay muy poca o ninguna evidencia de algún logro sistemático del propósito del proceso. No cuenta con PA.

- **Nivel 1 Ejecutado**. El proceso implementado alcanza su propósito. Sus PA son:
  - PA 1.1 Realización del Proceso.

- **Nivel 2 Gestionado**. El proceso ejecutado está implementado de forma gestionada y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente. Sus PA son:
  - PA 2.1 Gestión de desempeño.
  - PA 2.2 Gestión del producto de trabajo.

- **Nivel 3 Establecido**. El proceso gestionado ahora está implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. Sus PA son:
  - PA 3.1 Definición del proceso.
  - PA 3.2 Implementación del proceso.

- **Nivel 4 Predecible**. El proceso establecido ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso. Sus PA son:
  - PA 4.1 Medición del proceso.
  - PA 4.2 Control del proceso.

- **Nivel 5 Optimizado**. El proceso predecible es mejorado de forma continua para cumplir con las metas empresariales presentes y futuras. Sus PA son:
  - PA 5.1 Innovación del proceso.
  - PA 5.2 Optimización del proceso.

Para concluir con el análisis de Madurez, es importante destacar que la decisión de una organización de invertir en la mejora de los procesos TIC debe estar basada en la comprensión de la importancia estratégica para cada uno de sus objetivos. El resultado de esta evaluación permitirá diseñar un plan de acción para la optimización de los procesos y recursos de la gestión TIC.

Para ello se debe desarrollar una lista de prioridades de los objetivos que requieren mayor atención, y a través de las buenas prácticas aplicables en el dominio de interés optimizar su Gestión. Luego se puede alinear esta lista con la estrategia de la Empresa, lo que permitirá comenzar a recorrer el camino a la mejora Organizacional.

2.3. HIPÓTESIS

Para el presente estudio se formula la siguiente hipótesis general: La implementación de una solución holística de seguridad informática, mejorará la gestión de las TIC en la Dirección Regional de Educación de Piura

2.4. VARIABLES

La investigación presenta una variable independiente: Solución holística y otra dependiente: Seguridad de la información.

III. METODOLOGÍA

3.1. TIPO Y NIVEL DE LA INVESTIGACIÓN

El tipo de investigación es Aplicada, dado que se busca la construcción de una solución de Seguridad Informática Holística que mejorará la gestión de las TIC, de manera que se pueda generar información relevante para la toma de decisiones a nivel estratégico en la Dirección Regional de Educación de Piura.

Además, es descriptiva porque busca especificar las características del problema y evalúa los hechos que se dan en un contexto determinado. Según Vara-Horna[30] los diseños descriptivos están hechos para enumerar con mayor precisión y fidelidad posible, una realidad empresarial o un mercado.

3.2. DISEÑO DE LA INVESTIGACIÓN

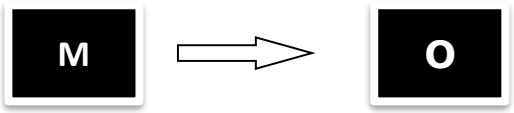
El diseño de la investigación es no experimental, porque no se va a manipular las variables, se limita a observar los datos. Asimismo, transversal porque el recojo de datos se realiza en un mismo periodo de tiempo. No habrá una evaluación posterior para observar cambios en los sujetos de estudio.

Para Hernández, Fernández y Baptista [31] el diseño no experimental se define como la investigación que se realiza sin manipular deliberadamente las variables y en los que sólo se observan los fenómenos en su ambiente natural para luego analizarlos. A su vez el diseño transversal es cuando los datos se recolectan en un solo momento, en un tiempo único, su propósito es describir variables.

Además, posee un enfoque cuantitativo, porque examina los datos de manera científica, en forma numérica, generalmente con ayuda de la estadística. Recoge y analiza datos sobre las variables y estudia las propiedades y fenómenos de la situación problemática de manera objetiva, así los resultados se pueden generalizar.

De acuerdo a Hernández, Fernández y Baptista [31] este enfoque usa recolección de datos con base en la mediación numérica y el análisis estadístico para establecer patrones de comportamiento.

El diseño de la investigación se grafica de la siguiente manera:



Dónde: M = Muestra; O = Observación

3.3. POBLACIÓN Y MUESTRA

3.3.1. Población

En la presente investigación la población se considera a los 137 trabajadores de la DREP, de los cuales se han tomado como población objetivo, 14 funcionarios relacionados con la seguridad de la información y la toma de decisiones.

3.3.2. Muestra

La muestra es la población objetivo: 14 funcionarios de las áreas de dirección, administración, gestión pedagógica, gestión institucional, asesoría jurídica y los jefes de los equipos de trabajo de personal e informática, que dependen del área de administración. Estos funcionarios están relacionados con la seguridad de la información y la toma de decisiones, criterio por el cual fueron seleccionados.

3.4. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES Y LOS INDICADORES

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES	ESCALA DE MEDICIÓN
Solución Holística.	La palabra *holismo* proviene de un vocablo griego (*yólos*) que significa *todo, totalidad, por entero*. Según este método de estudio se debe tomar a los sistemas físicos, biológicos, económicos, mentales, lingüísticos, sociales, etcétera, como totalidades y analizar el todo junto a las características del sistema y no sólo remitirse a las partes[1].	Operacionalmente se midió las falencias de la seguridad de la información a través de un cuestionario aplicado a los funcionarios de la DREP.	- Toma decisiones de adquisición. - Tiene un sistema configurado para realizar prueba/instalación. - Define requerimientos de ambiente físico. - Mantiene actualizados la tecnología en base a estándares. - Define requerimientos de monitoreo del sistema. - Conoce la infraestructura. - Tiene OLAS (Acuerdo de nivel operacional) planeados anticipadamente.	- Nivel 0 Incompleto. - Nivel 1 Ejecutado. - Nivel 2 Gestionado. - Nivel 3 Establecido. - Nivel 4 Predecible. - Nivel 5 Optimizado.
Seguridad de la Información.	La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la	La seguridad de la información se mide a través de las políticas de seguridad, la organización de la seguridad, la gestión de		

	información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Conviene aclarar que la seguridad absoluta no es posible, no existe un sistema 100 % seguro, de forma que el elemento de riesgo está siempre presente, independiente de las medidas que tomemos, por lo que se debe hablar de niveles de seguridad[3].	activos, la seguridad en el recurso humano, la seguridad física, la gestión de comunicaciones y operaciones, el control de acceso, la adquisición, desarrollo y mantenimiento de los sistemas de información, la gestión de incidentes de seguridad, por medio el instrumento cuestionario aplicado a los funcionarios de la DREP.		

3.5. TÉCNICAS E INSTRUMENTOS

3.5.1. Técnica

Encuestas: Serán aplicadas a los 14 funcionarios de nivel estratégico de la Dirección Regional de Educación de Piura.

3.5.2. Instrumentos

Cuestionario: La elaboración de las preguntas se realizó de acuerdo a los indicadores de las variables, con la finalidad de dar respuesta a los objetivos de investigación. La estructura del cuestionario se obtuvo de la estructura del modelo COBIT 5.0

La encuesta es la técnica que se aplica en el desarrollo de la presente investigación, la cual busca recaudar datos a través de un cuestionario prediseñado, de tal manera que no modifica el entorno ni controla el proceso que está en observación. Los datos se obtienen a partir de realizar un conjunto de preguntas normalizadas dirigidas a una muestra representativa, cuya finalidad es conocer estados de opinión, características o hechos específicos.

La escala de medición de los indicadores, son nominales para las preguntas dicotómicas y ordinales para el resto de preguntas.

3.6. PLAN DE ANÁLISIS

Los datos recopilados se codificaron, para mantener el orden y posteriormente elaborar los cuadros estadísticos, mediante el programa SPSS v. 2.1, de los cuales se realizó el análisis e interpretación de la información obtenida, para la discusión de resultados y la elaboración de las conclusiones. Además, para la elaboración de tablas, análisis e interpretación de los datos se usó el programa MS. Excel 2016.

3.7. MATRIZ DE CONSISTENCIA

PROBLEMA GENERAL	OBJETIVO GENERAL	MARCO TÉÓRICO	HIPÓTESIS GENERAL	VARIABLES	METODOLOGÍA
¿En qué medida la implementación de una solución holística de seguridad informática, mejorará la gestión de tecnología de información y comunicación en la Dirección Regional de Educación de Piura, en el	Implementar una solución holística de seguridad informática para mejorar la gestión de la tecnología de información y comunicación en Dirección Regional de Educación de Piura, en el departamento de Piura en el año 2016 **Objetivos Específicos** ▪ Revisar información bibliográfica relacionada a seguridad informática. ▪ Evaluar la seguridad informática en la DREP.	**ANTECEDENTES:** **A nivel internacional** **Aranda L. (2013)** Estudio de sistemas de seguridad basado en la detección de intrusión física y tecnológica. **Arias B., Merizalde A., Noriega G. (2013.)** Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual.	La implementación de una solución de seguridad informática holística, mejorará la gestión de las TIC en la Dirección Regional de Educación de Piura. **Hipótesis Nula** La implementación de una solución de seguridad informática holística, no	**Independiente** Solución Holística. **Dependiente** Seguridad de la Información.	**Tipo de Investigación** Aplicada. **Nivel de Investigación** Descriptiva **Diseño de Investigación** Cuantitativa. **Población y Muestra** ▪ Población: 137 trabajadores de

departamento de Piura en el año 2016?	▪ Analizar y diseñar una solución informática holística adecuada para la DREP. ▪ Implementar una solución informática holística para la DREP. ▪ Evaluar la seguridad informática posterior a la aplicación de la solución informática holística en la DREP.	**Robayo L., Rodríguez R. (2015)** Aseguramiento de los sistemas computacionales de la empresa SITIOSDIMA.NET. **A nivel nacional** **Campos B. (2015)** Sistema de monitoreo de seguridad física en plataforma libre de componentes electrónicos para asegurar la gestión de los niveles de continuidad de los servicios informáticos en la central de datos USAT. **Alcántara F. (2015)** Guía de implementación de la seguridad basado en la	mejorará la gestión de las TIC en la Dirección Regional de Educación de Piura.		la DREP. ▪ Muestra: 14 funcionarios de nivel estratégico de la DREP. **Técnicas e Instrumentos** ▪ Técnica: Encuesta. ▪ Instrumento: Cuestionario.

		norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo. **Aguirre M. (2014)** Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. **<u>A nivel local</u>** **Ramos Arca (2015)** Propuesta de un plan de auditoría informática para el "Sistema de información en salud" y el "Aplicativo para el registro de formatos SIS" en los establecimientos de salud			

		de la unidad ejecutora 400 en la Región Piura en el año 2015. **Arévalo H. (2016)** Estudio y diseño de red de datos y cámaras de seguridad en la empresa REGENDA H Y D Inversiones y Servicios EIRL. Castilla – Piura.			

IV. RESULTADOS (ESTO LE ESTOY SOLICITANDO QUE DEBE DE APARECER REDACTADO EN SU RESUMEN) NO LO VEO.

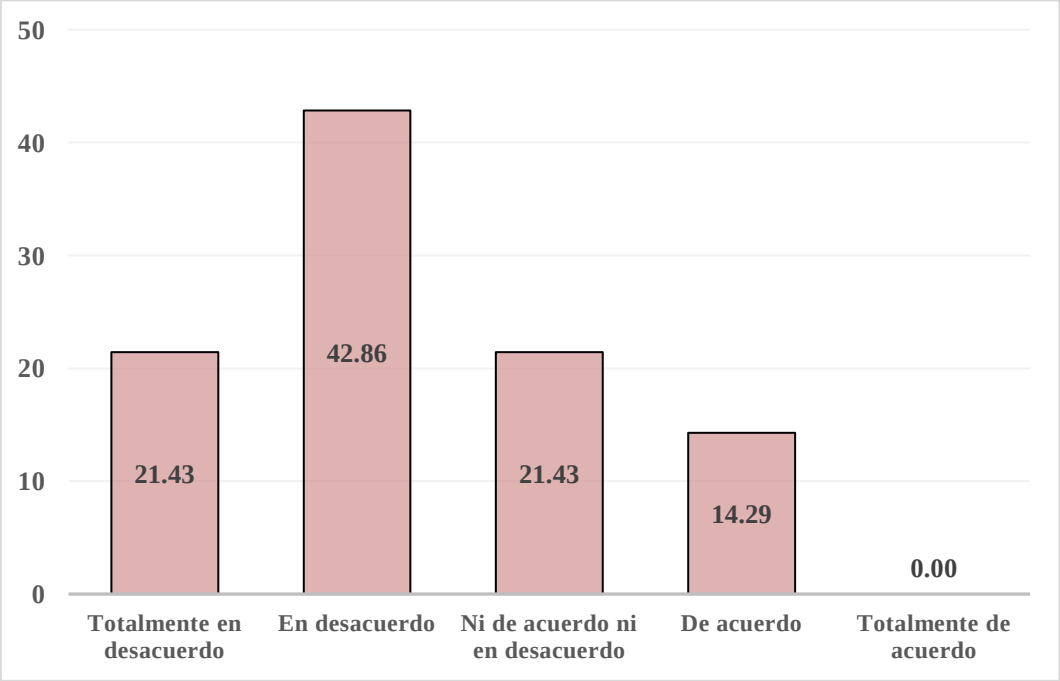
4.1. RESULTADOS

Tabla 1: Distribución de funcionarios según opinión si existen políticas de seguridad de información en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	3	21.43
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	2	14.29
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 1: Distribución de funcionarios según opinión si existen políticas de seguridad de información en la DREP.



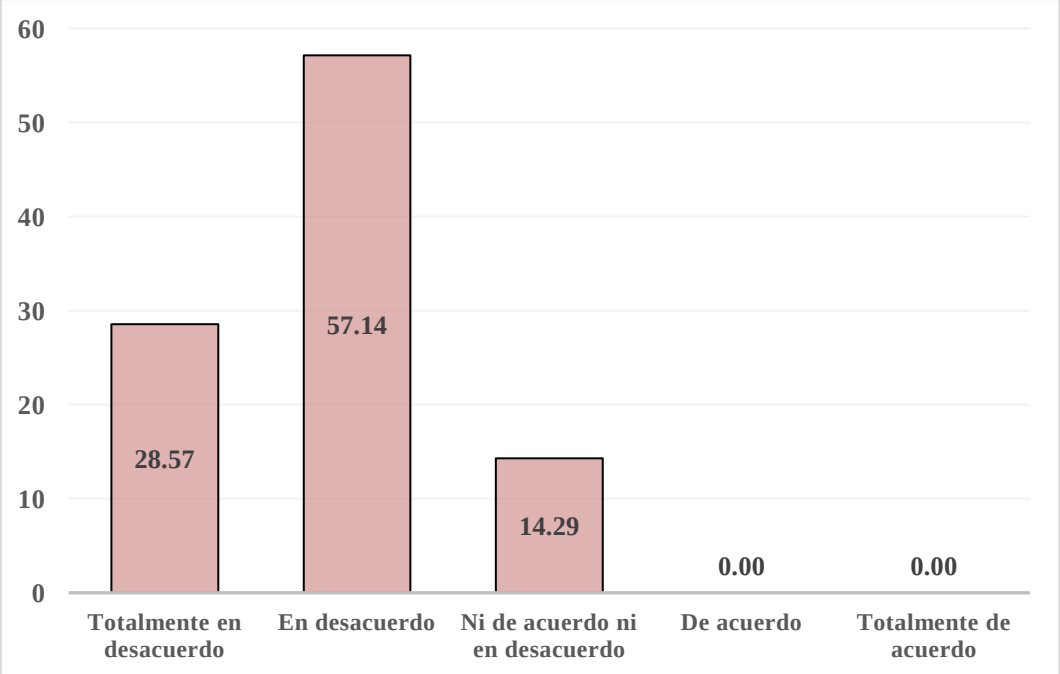
Fuente: Elaboración propia.

Tabla 2: Distribución de funcionarios según opinión si se cumplen políticas de seguridad de información en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	4	28.57
En desacuerdo	8	57.14
Ni de acuerdo ni en desacuerdo	2	14.29
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 2: Distribución de funcionarios según opinión si se cumplen las políticas de seguridad de información en la DREP.



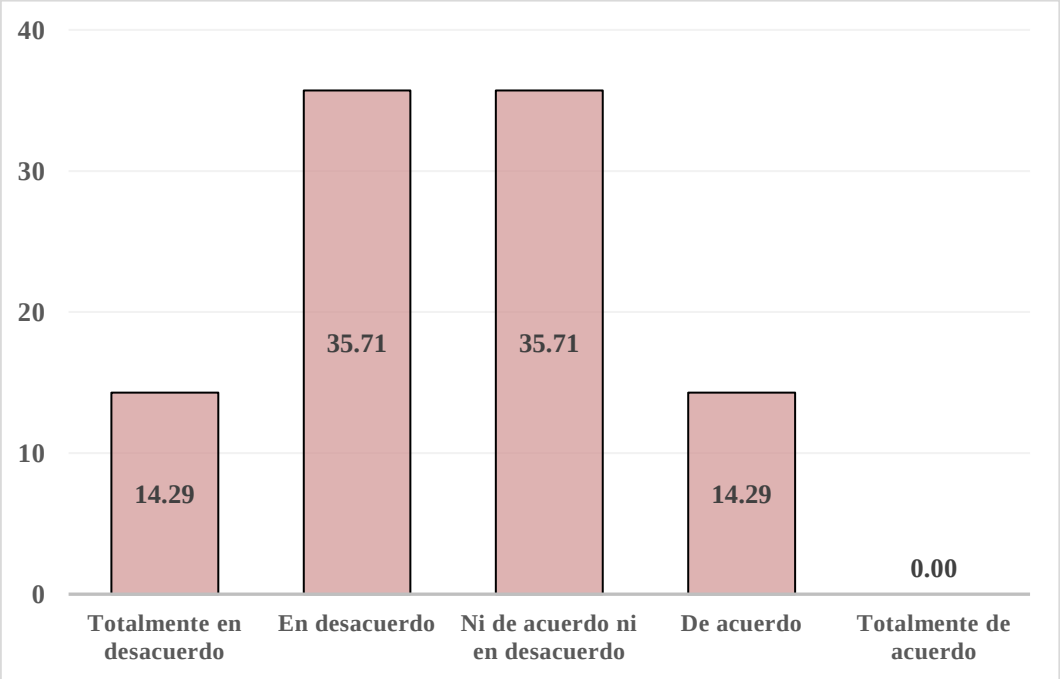
Fuente: Elaboración propia.

Tabla 3: Distribución de funcionarios según opinión si existe una organización interna para la seguridad de la información.

Alternativas	n	%
Totalmente en desacuerdo	2	14.29
En desacuerdo	5	35.71
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	2	14.29
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 3: Distribución de funcionarios según opinión si existe una organización interna para la seguridad de información.



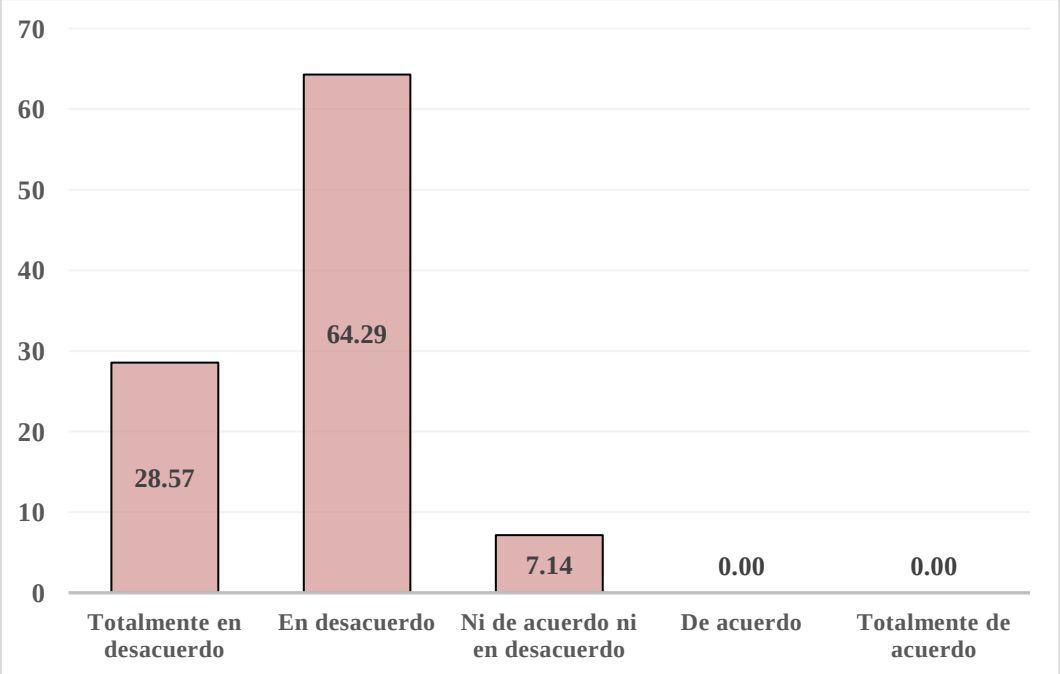
Fuente: Elaboración propia.

Tabla 4: Distribución de funcionarios según opinión si existe una organización externa para la seguridad de información.

Alternativas	n	%
Totalmente en desacuerdo	4	28.57
En desacuerdo	9	64.29
Ni de acuerdo ni en desacuerdo	1	7.14
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 4: Distribución de funcionarios según opinión si existe una organización externa para la seguridad de información.



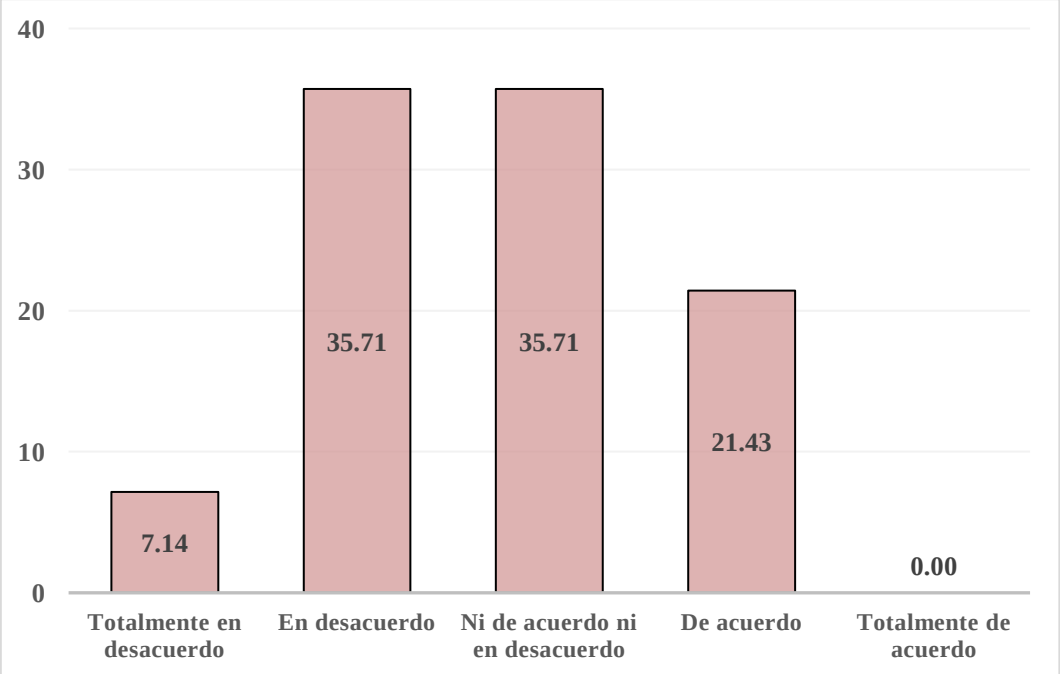
Fuente: Elaboración propia.

Tabla 5: Distribución de funcionarios según opinión si existe una adecuada responsabilidad sobre los activos de la DREP.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	5	35.71
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	3	21.43
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 5: Distribución de funcionarios según opinión si existe una adecuada responsabilidad sobre los activos de la DREP.



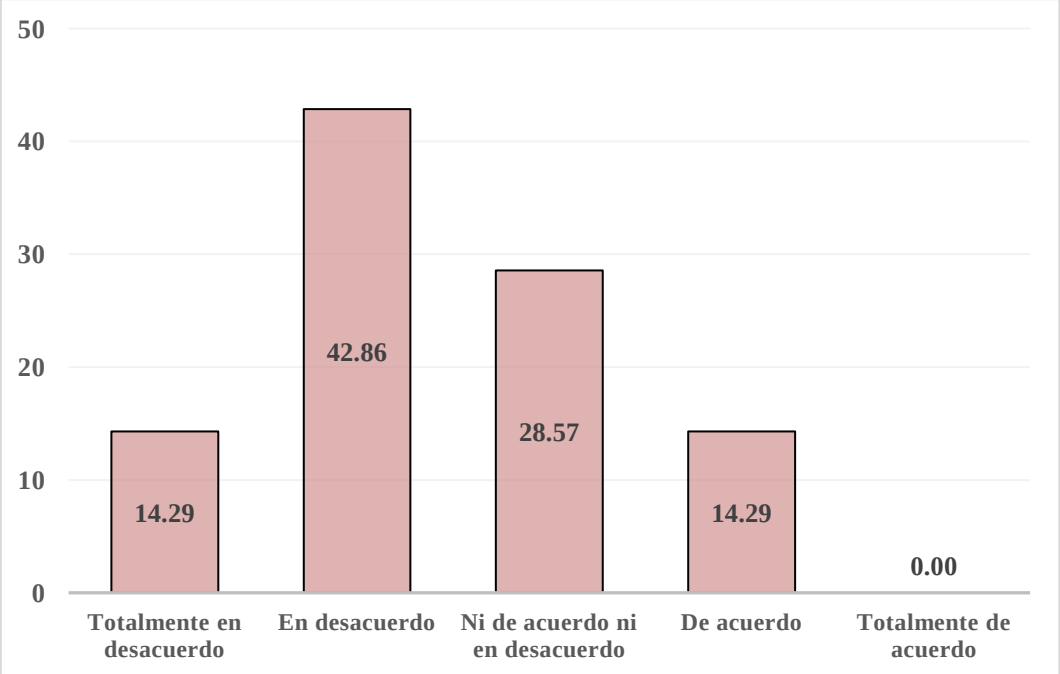
Fuente: Elaboración propia.

Tabla 6: Distribución de funcionarios según opinión si se clasifica la información en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	2	14.29
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	4	28.57
De acuerdo	2	14.29
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 6: Distribución de funcionarios según opinión si se clasifica la información en la DREP.



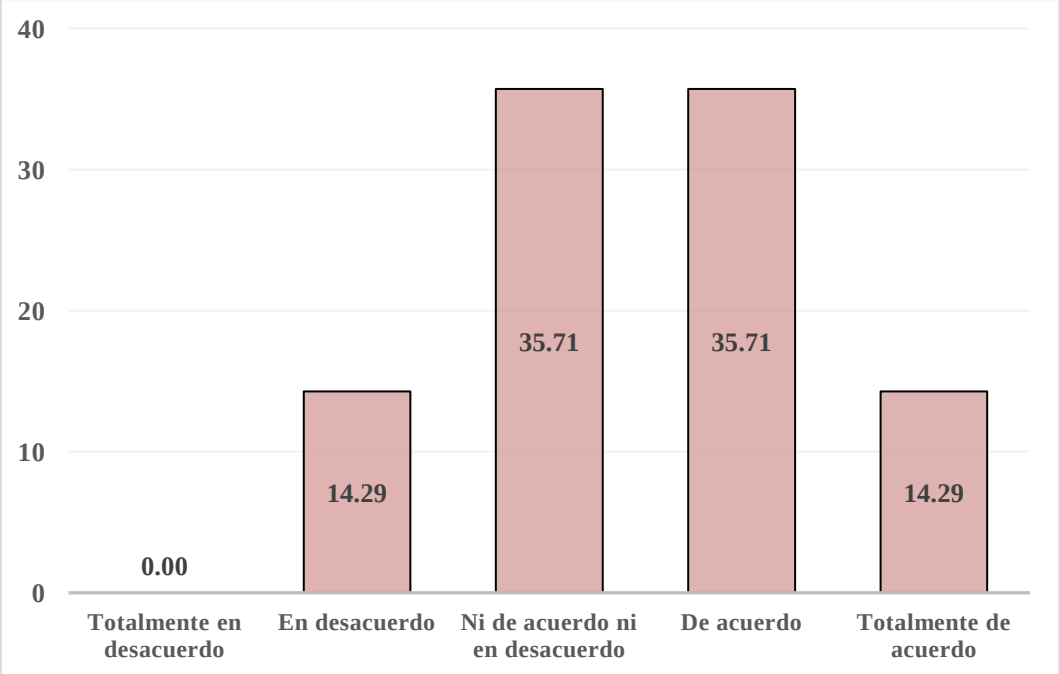
Fuente: Elaboración propia.

Tabla 7: Distribución de funcionarios según opinión si existe seguridad en el recurso humano antes de la contratación.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	2	14.29
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	5	35.71
Totalmente de acuerdo	2	14.29
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 7: Distribución de funcionarios según opinión si existe seguridad en el recurso humano antes de la contratación.



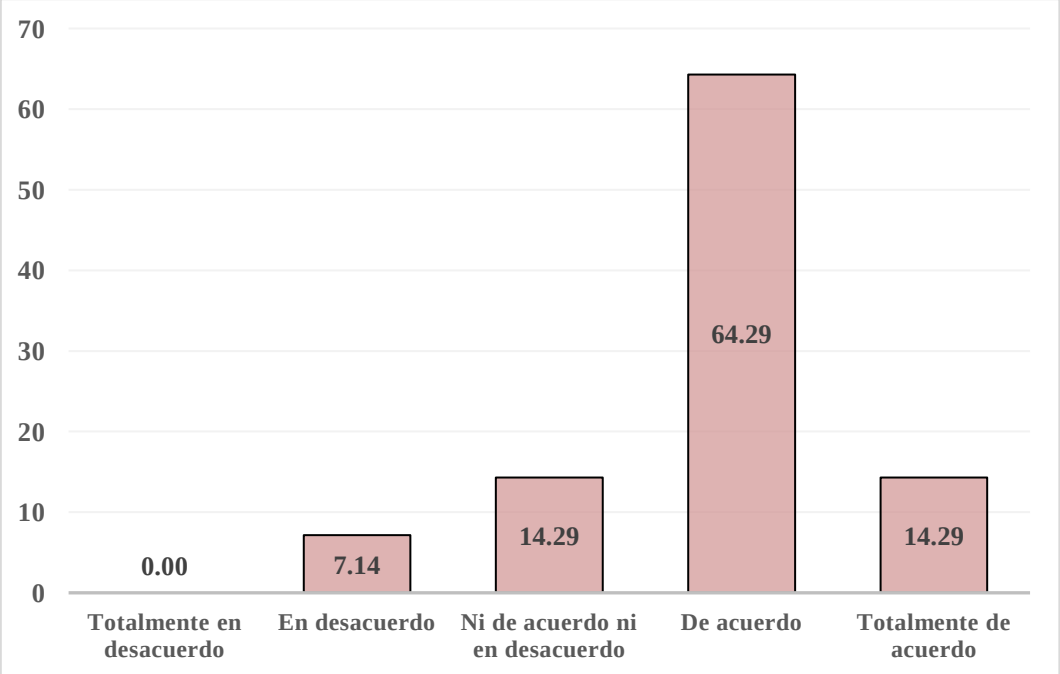
Fuente: Elaboración propia.

Tabla 8: Distribución de funcionarios según opinión si se le brinda seguridad al recurso humano durante la vigencia de la contratación.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	1	7.14
Ni de acuerdo ni en desacuerdo	2	14.29
De acuerdo	9	64.29
Totalmente de acuerdo	2	14.29
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 8: Distribución de funcionarios según opinión si se le brinda seguridad al recurso humano durante la vigencia de la contratación.



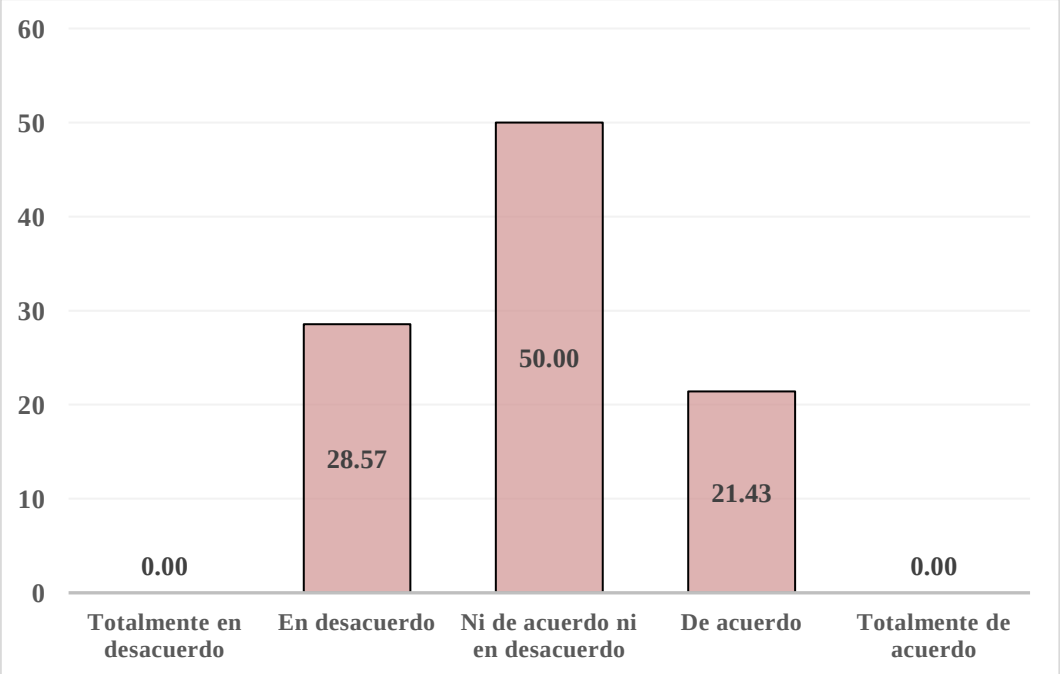
Fuente: Elaboración propia.

Tabla 9: Distribución de funcionarios según opinión si en la terminación o cambio de contratación se continúa con la seguridad del recurso humano.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	4	28.57
Ni de acuerdo ni en desacuerdo	7	50.00
De acuerdo	3	21.43
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 9: Distribución de funcionarios según opinión si en la terminación o cambio de contratación se continúa con la seguridad del recurso humano.



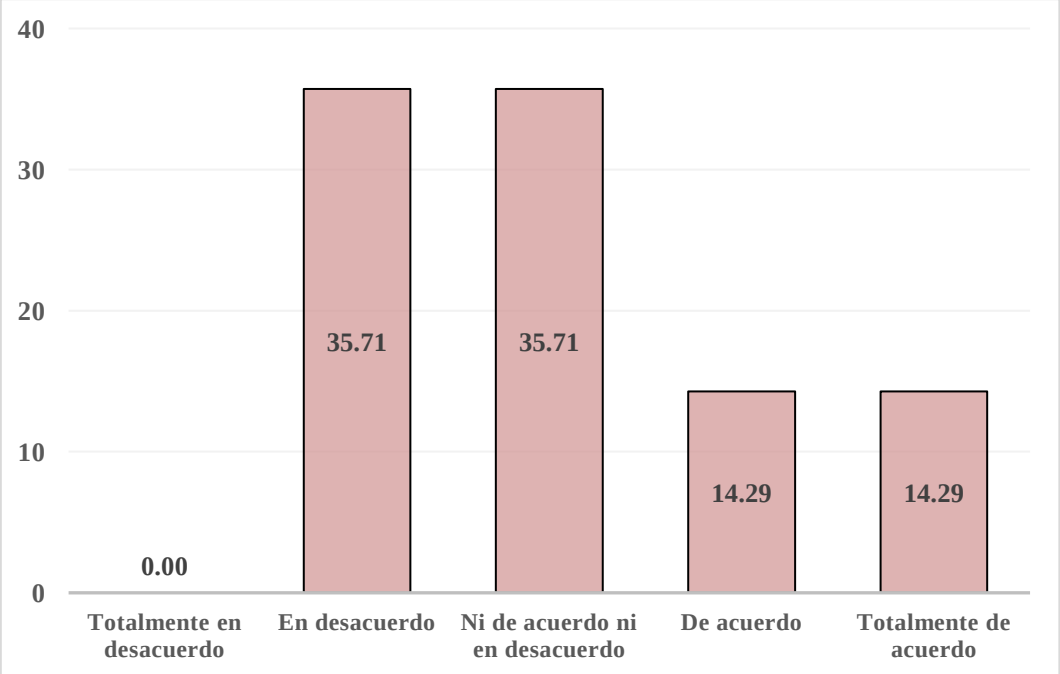
Fuente: Elaboración propia.

Tabla 10: Distribución de funcionarios según opinión si se cuenta con áreas seguras.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	5	35.71
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	2	14.29
Totalmente de acuerdo	2	14.29
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 10: Distribución de funcionarios según opinión si se cuenta con áreas seguras.



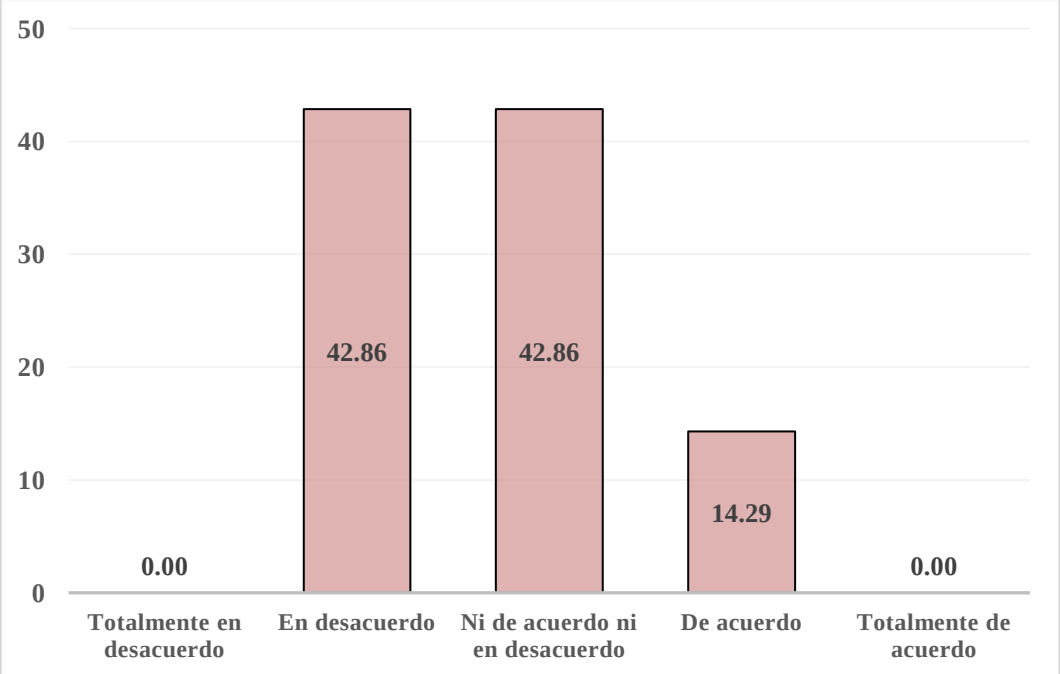
Fuente: Elaboración propia.

Tabla 11: Distribución de funcionarios según opinión si se evidencia un nivel adecuado para la seguridad de los equipos.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	6	42.86
De acuerdo	2	14.29
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 11: Distribución de funcionarios según opinión si se evidencia un nivel adecuado para la seguridad de los equipos.



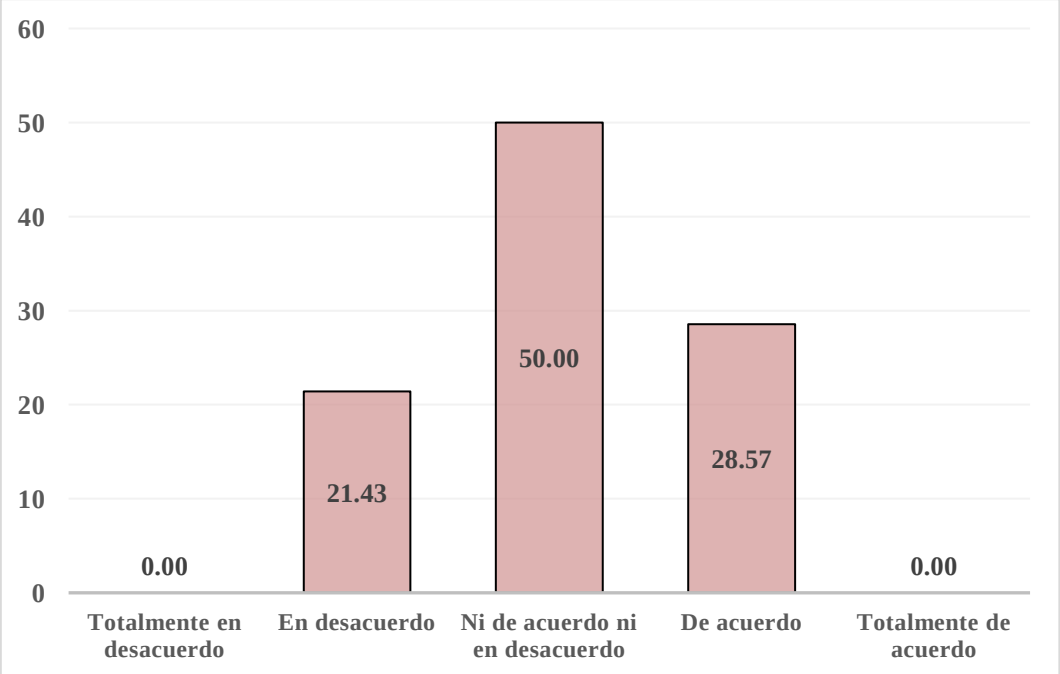
Fuente: Elaboración propia.

Tabla 12: Distribución de funcionarios según opinión si los procedimientos operacionales y de responsabilidades son idóneos.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	3	21.43
Ni de acuerdo ni en desacuerdo	7	50.00
De acuerdo	4	28.57
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 12: Distribución de funcionarios según opinión si los procedimientos operacionales y de responsabilidades son idóneos.



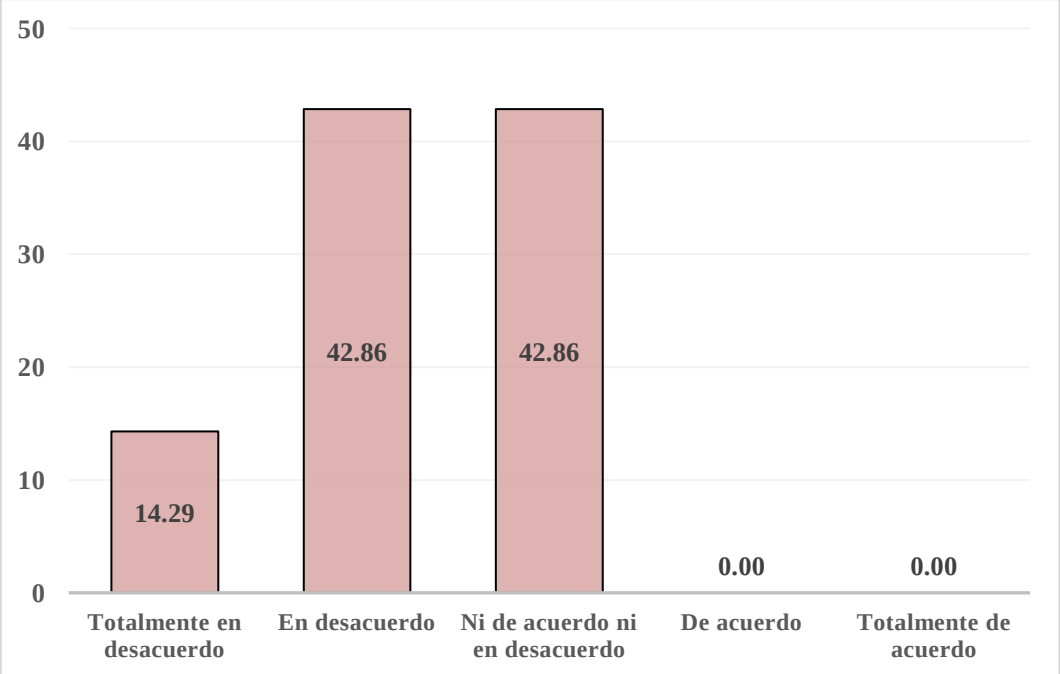
Fuente: Elaboración propia.

Tabla 13: Distribución de funcionarios según opinión si la gestión de la prestación de servicios por terceros es la adecuada.

Alternativas	n	%
Totalmente en desacuerdo	2	14.29
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	6	42.86
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura13: Distribución de funcionarios según opinión si la gestión de la prestación de servicios por terceros es la adecuada.



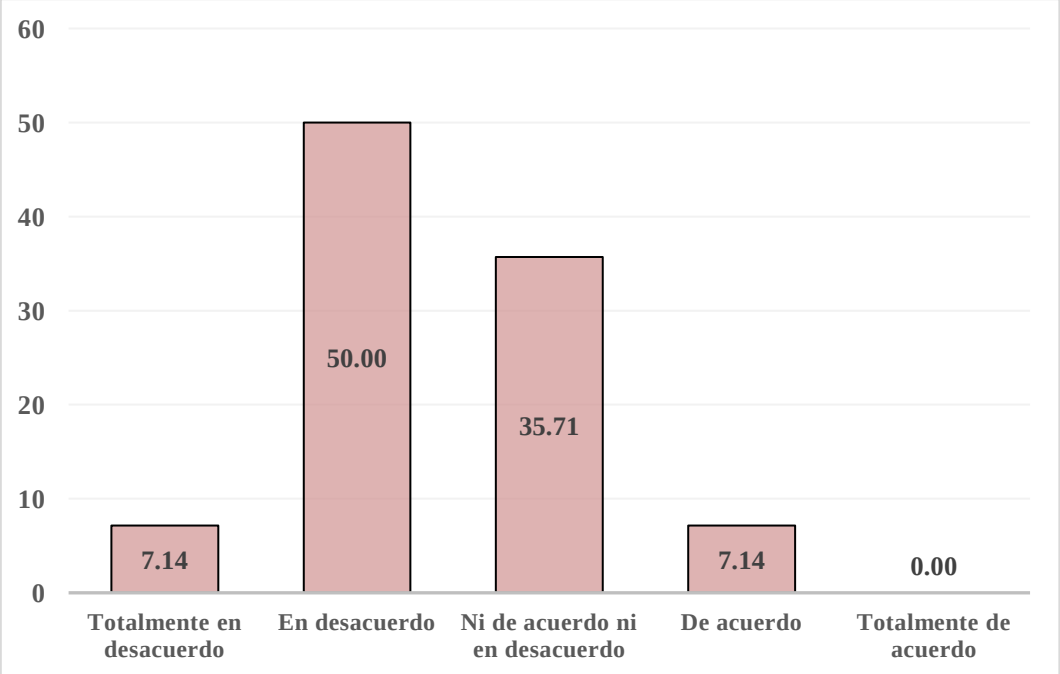
Fuente: Elaboración propia.

Tabla 14: Distribución de funcionarios según opinión si existe una planificación y aceptación de sistemas informáticos en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	7	50.00
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	1	7.14
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 14: Distribución de funcionarios según opinión si existe una planificación y aceptación de sistemas informáticos en la DREP.



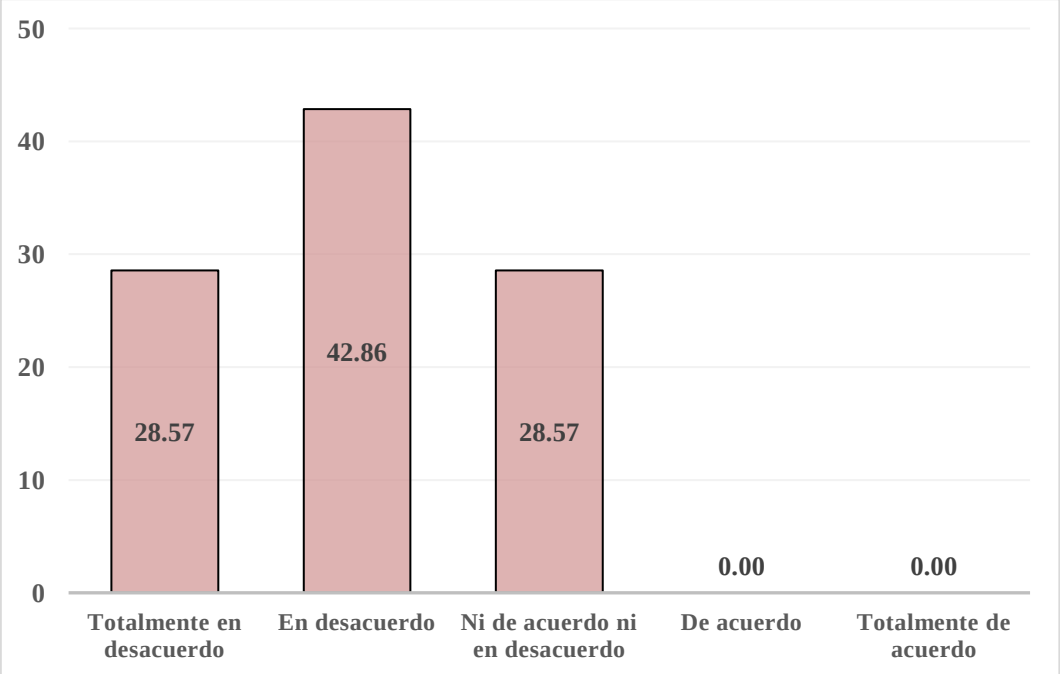
Fuente: Elaboración propia.

Tabla 15: Distribución de funcionarios según opinión si existe protección contra códigos maliciosos y móviles.

Alternativas	n	%
Totalmente en desacuerdo	4	28.57
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	4	28.57
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura15: Distribución de funcionarios según opinión si existe protección contra códigos maliciosos y móviles.



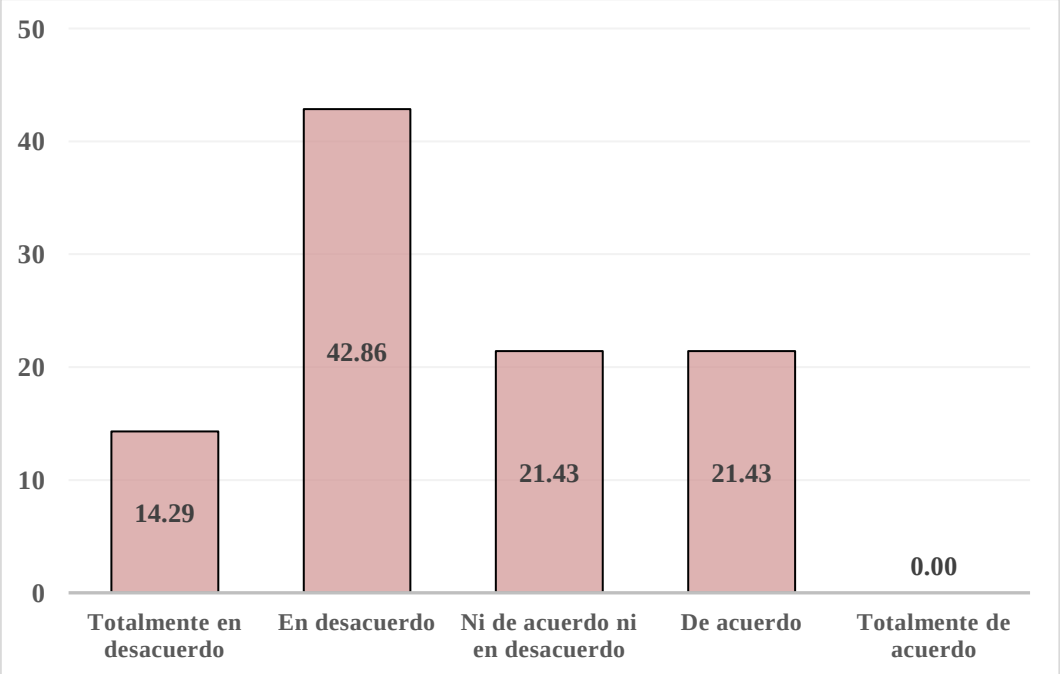
Fuente: Elaboración propia.

Tabla 16: Distribución de funcionarios según opinión si se cuenta con un respaldo informático adecuado en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	2	14.29
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	3	21.43
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura16: Distribución de funcionarios según opinión si se cuenta con un respaldo informático en la DREP.



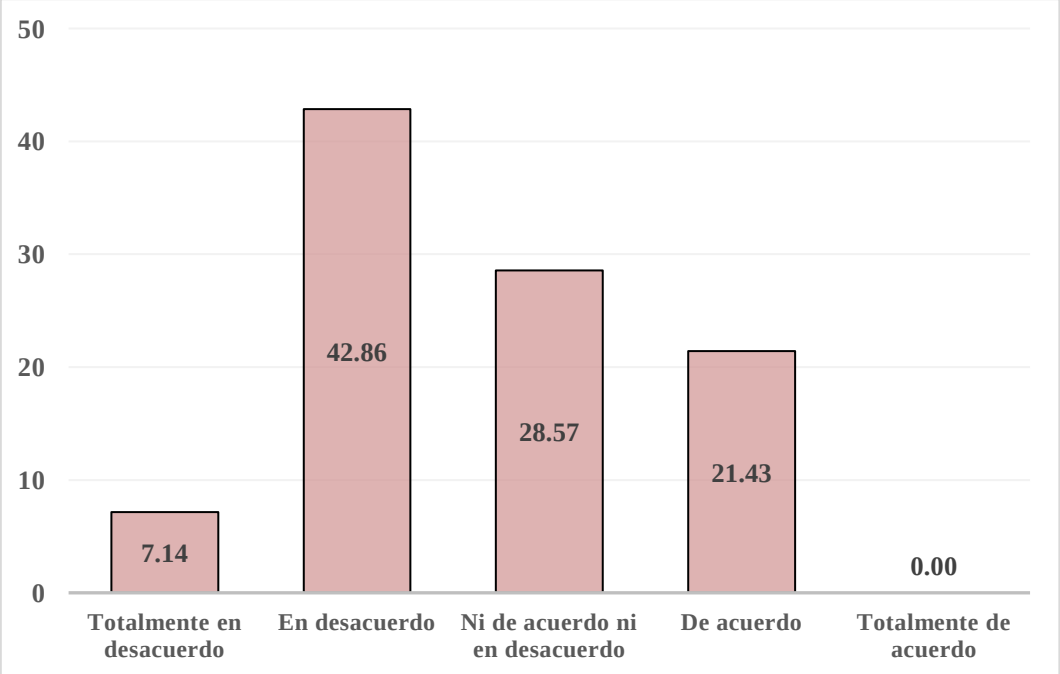
Fuente: Elaboración propia.

Tabla 17: Distribución de funcionarios según opinión si se evidencia un nivel de gestión de seguridad en las redes.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	4	28.57
De acuerdo	3	21.43
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 17: Distribución de funcionarios según opinión si se evidencia un nivel de gestión de seguridad en las redes.



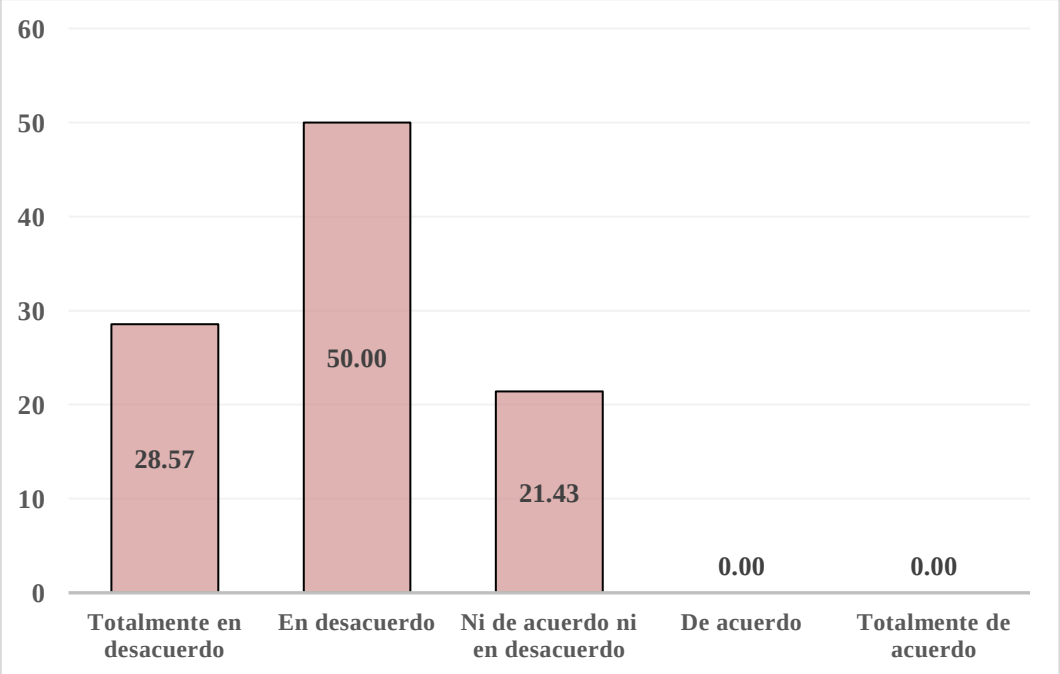
Fuente: Elaboración propia.

Tabla 18: Distribución de funcionarios según opinión si existe un manejo de medios digitales adecuado en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	4	28.57
En desacuerdo	7	50.00
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 18: Distribución de funcionarios según opinión si existe un manejo de medios digitales adecuado en la DREP.



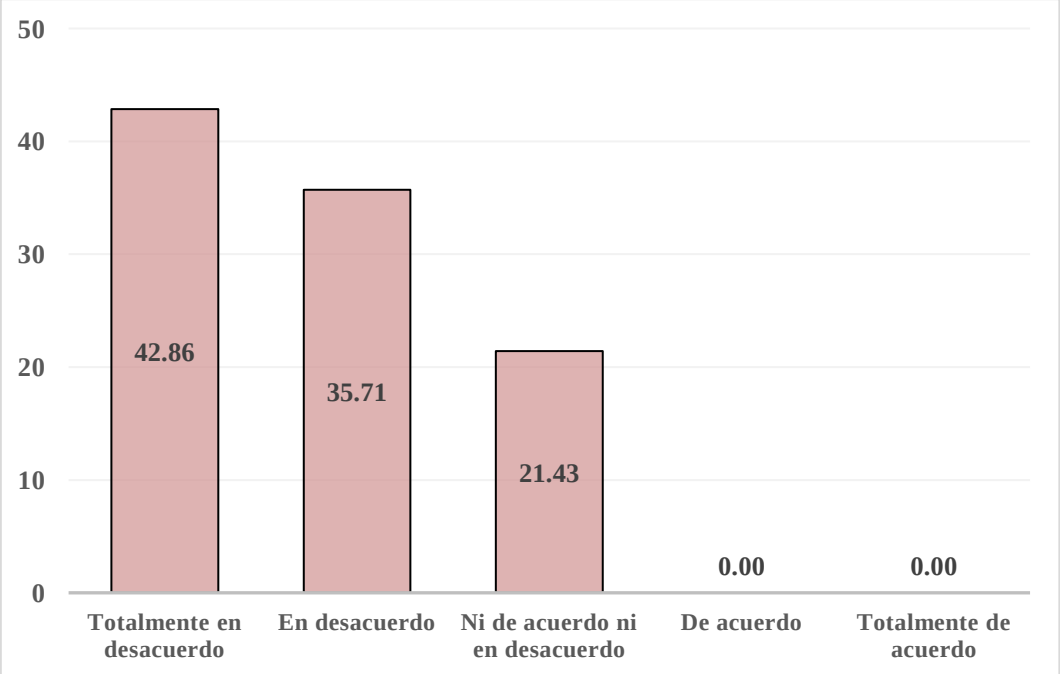
Fuente: Elaboración propia.

Tabla 19: Distribución de funcionarios según opinión si se realiza un intercambio de información idóneo en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	6	42.86
En desacuerdo	5	35.71
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura19: Distribución de funcionarios según opinión si se realiza un intercambio de información idóneo en la DREP.



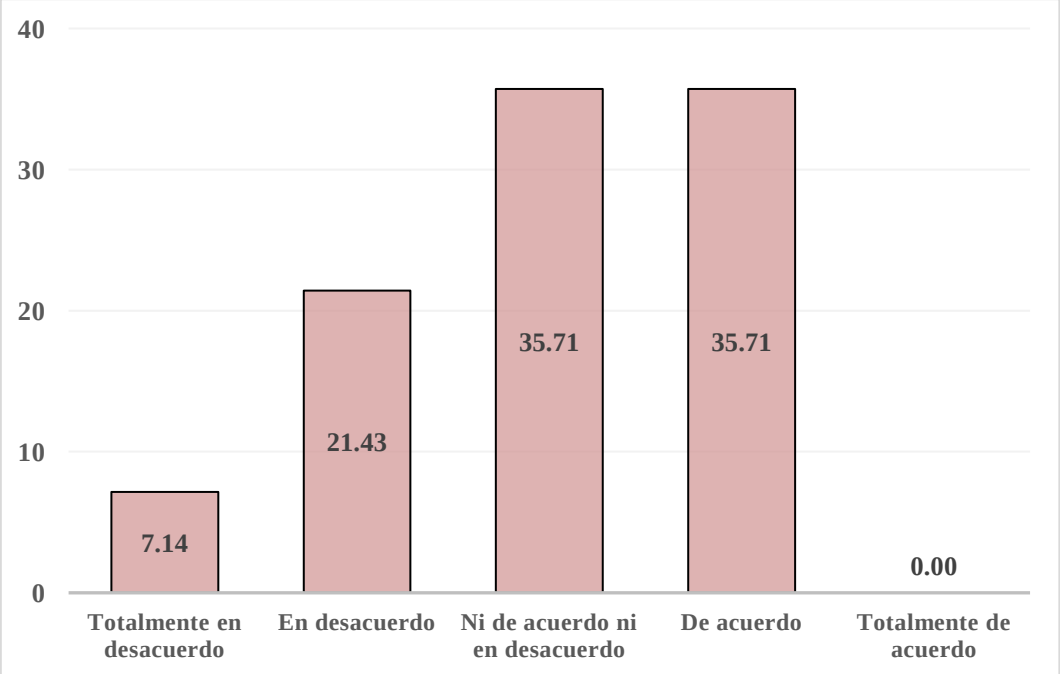
Fuente: Elaboración propia.

Tabla 20: Distribución de funcionarios según opinión si se monitorea constantemente la gestión de comunicaciones y operaciones en la DREP.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	3	21.43
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	5	35.71
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura20: Distribución de funcionarios según opinión si se monitorea constantemente la gestión de comunicación y operaciones en la DREP.



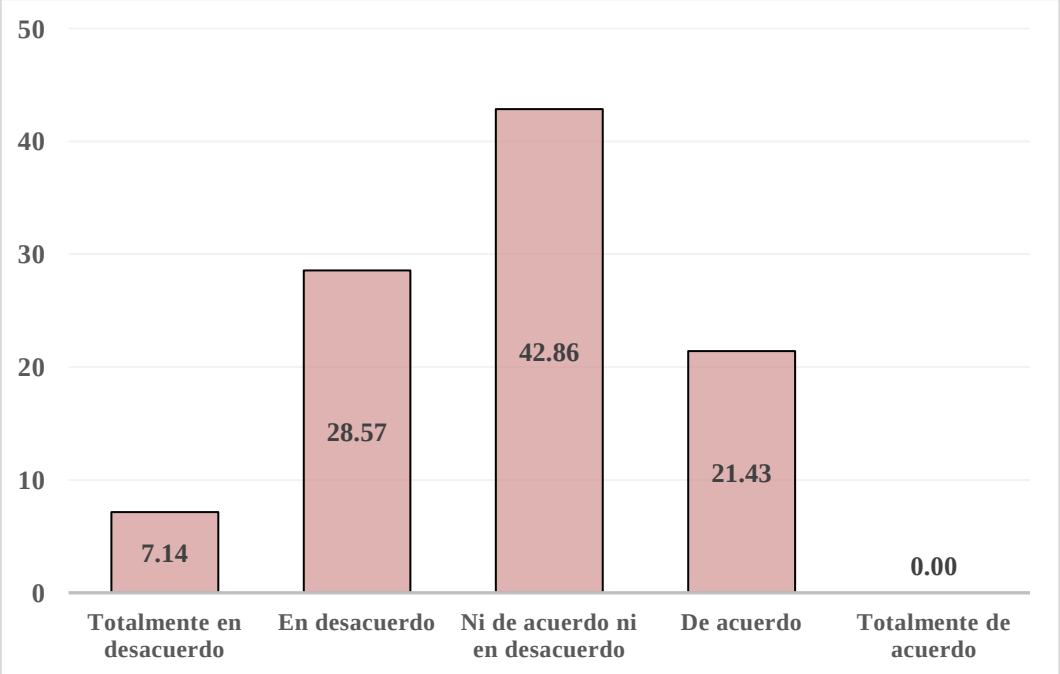
Fuente: Elaboración propia.

Tabla 21: Distribución de funcionarios según opinión si la gestión de acceso de los usuarios se realiza adecuadamente.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	4	28.57
Ni de acuerdo ni en desacuerdo	6	42.86
De acuerdo	3	21.43
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura21: Distribución de funcionarios según opinión si la gestión de acceso de los usuarios se realiza adecuadamente.



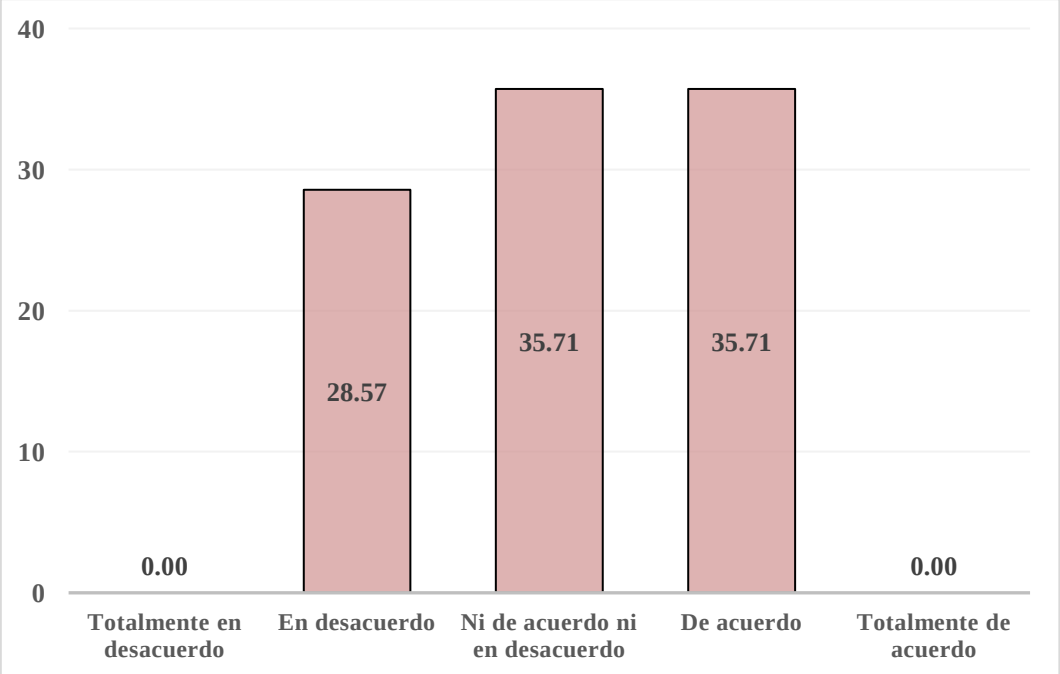
Fuente: Elaboración propia.

Tabla 22: Distribución de funcionarios según opinión si los usuarios evidencian responsabilidad en el acceso a los sistemas de información.

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	4	28.57
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	5	35.71
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 22: Distribución de funcionarios según opinión si los usuarios evidencian responsabilidad en el acceso a los sistemas de información.



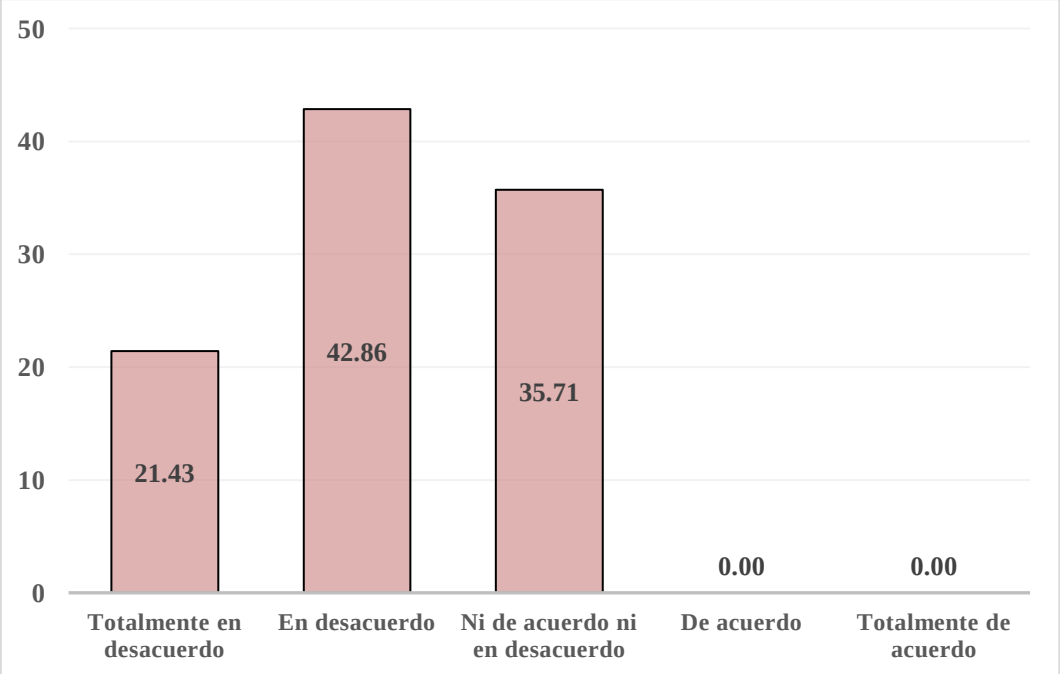
Fuente: Elaboración propia.

Tabla 23: Distribución de funcionarios según opinión si se cuenta con controles de acceso a las redes.

Alternativas	n	%
Totalmente en desacuerdo	3	21.43
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura23: Distribución de funcionarios según opinión si se cuenta con controles de acceso a las redes.



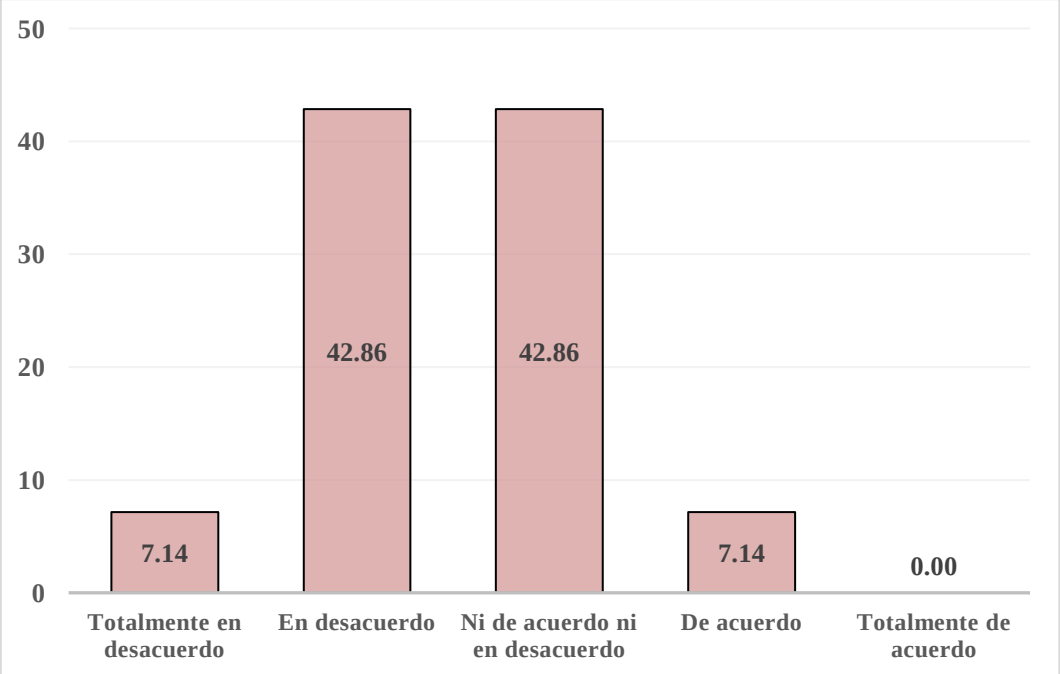
Fuente: Elaboración propia.

Tabla 24: Distribución de funcionarios según opinión si existe un control de acceso al sistema operativo.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	6	42.86
De acuerdo	1	7.14
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 24: Distribución de funcionarios según opinión si existe un control de acceso al sistema operativo.



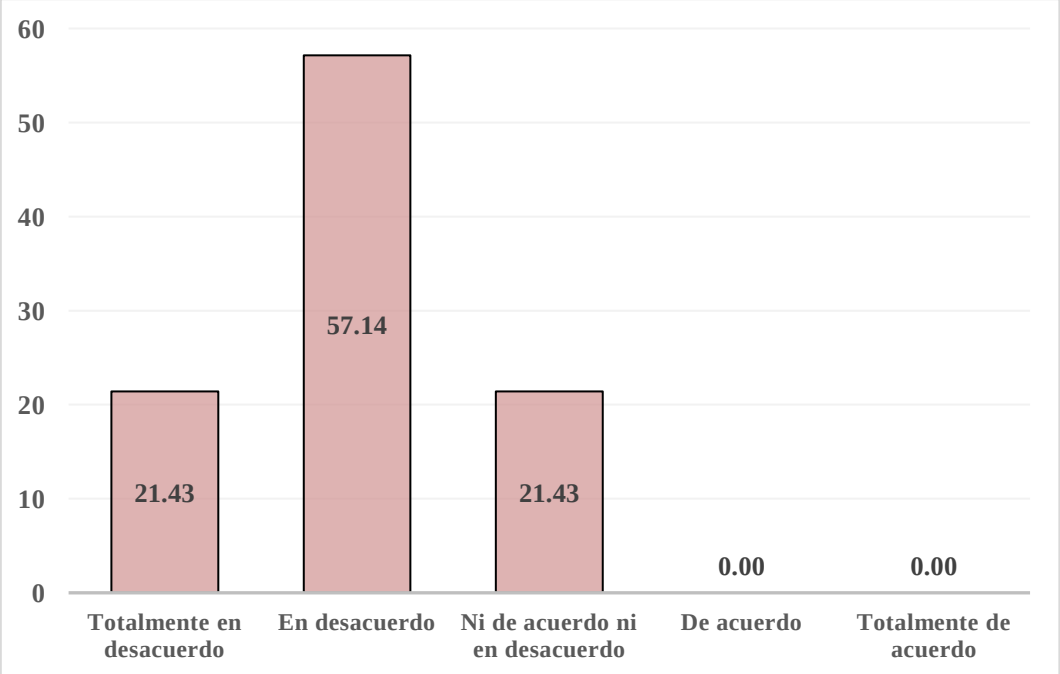
Fuente: Elaboración propia.

Tabla 25: Distribución de funcionarios según opinión si el control de acceso a las aplicaciones y a la información es regulado.

Alternativas	n	%
Totalmente en desacuerdo	3	21.43
En desacuerdo	8	57.14
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 25: Distribución de funcionarios según opinión si el control de acceso a las aplicaciones y a la información es regulado.



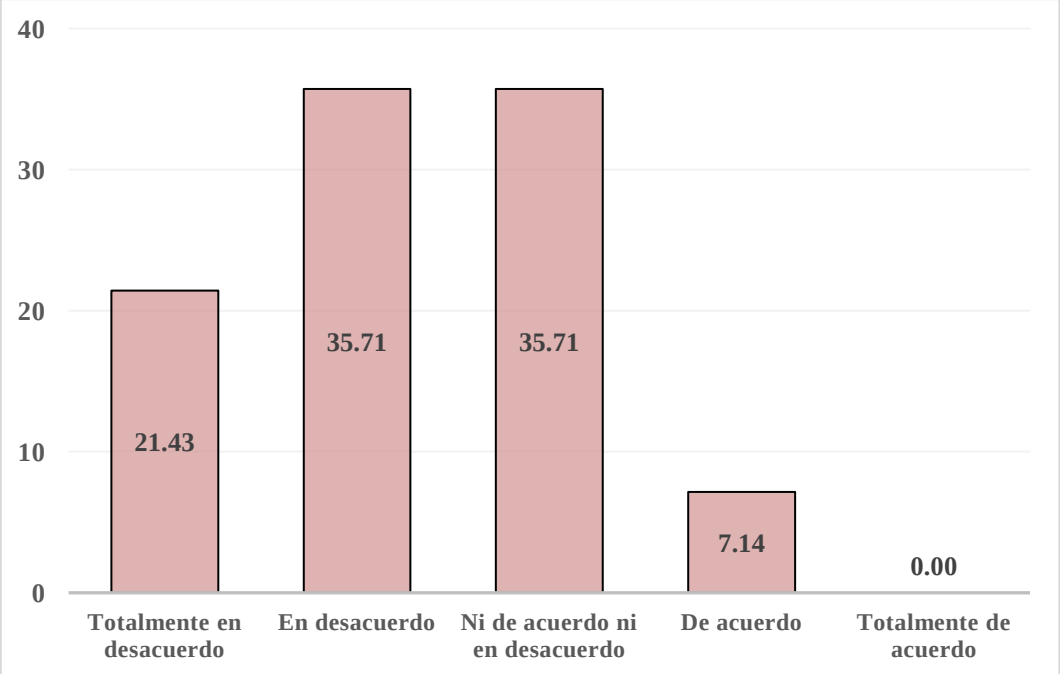
Fuente: Elaboración propia.

Tabla 26: Distribución de funcionarios según opinión si se cumplen con los requisitos de seguridad de los sistemas de información.

Alternativas	n	%
Totalmente en desacuerdo	3	21.43
En desacuerdo	5	35.71
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	1	7.14
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 26: Distribución de funcionarios según opinión si se cumplen con los requisitos de seguridad de los sistemas de información.



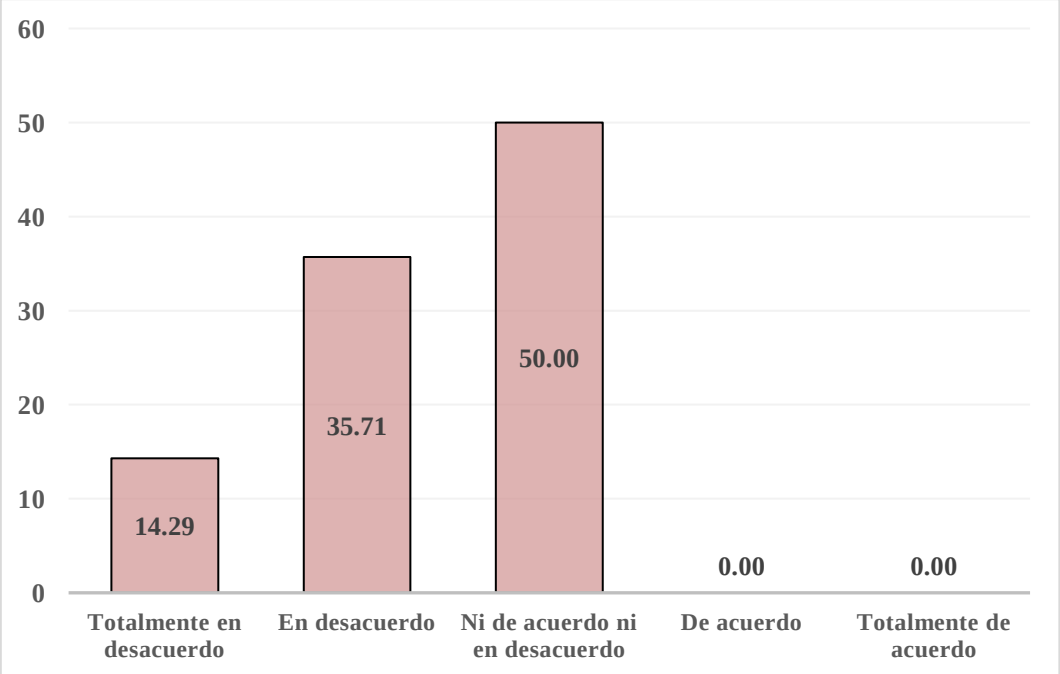
Fuente: Elaboración propia.

Tabla 27: Distribución de funcionarios según opinión si existe un procesamiento correcto en las aplicaciones.

Alternativas	n	%
Totalmente en desacuerdo	2	14.29
En desacuerdo	5	35.71
Ni de acuerdo ni en desacuerdo	7	50.00
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 27: Distribución de funcionarios según opinión si existe un procesamiento correcto en las aplicaciones.



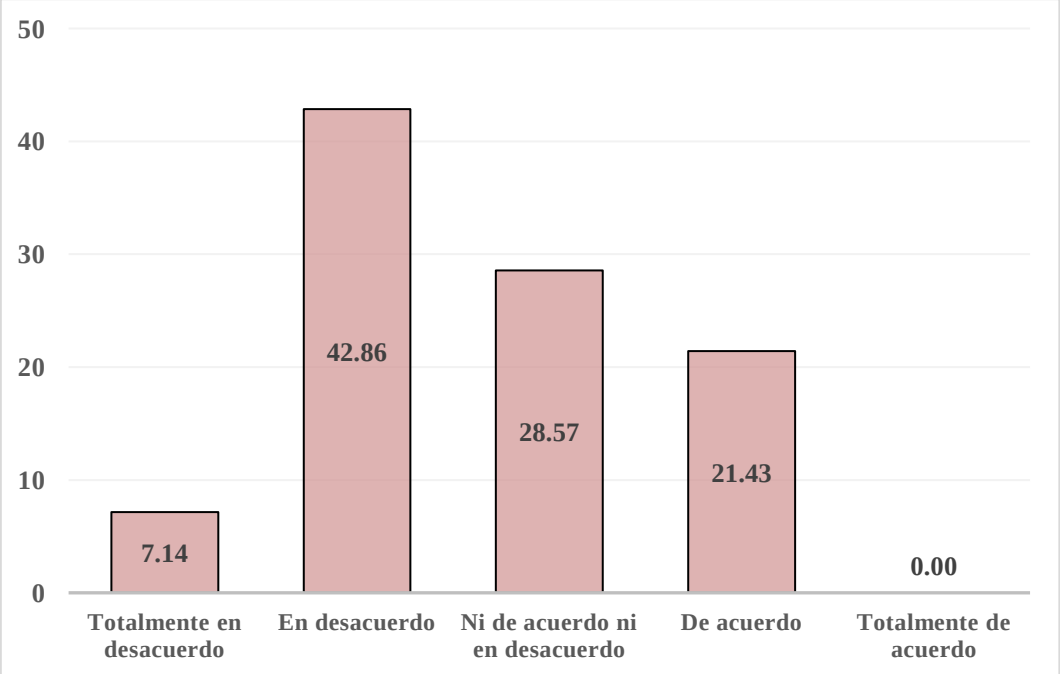
Fuente: Elaboración propia.

Tabla 28: Distribución de funcionarios según opinión si es evidente la seguridad de los archivos de los sistemas de información de la DREP.

Alternativas	n	%
Totalmente en desacuerdo	1	7.14
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	4	28.57
De acuerdo	3	21.43
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 28: Distribución de funcionarios según opinión si es evidente la seguridad de los archivos de los sistemas de información de la DREP.



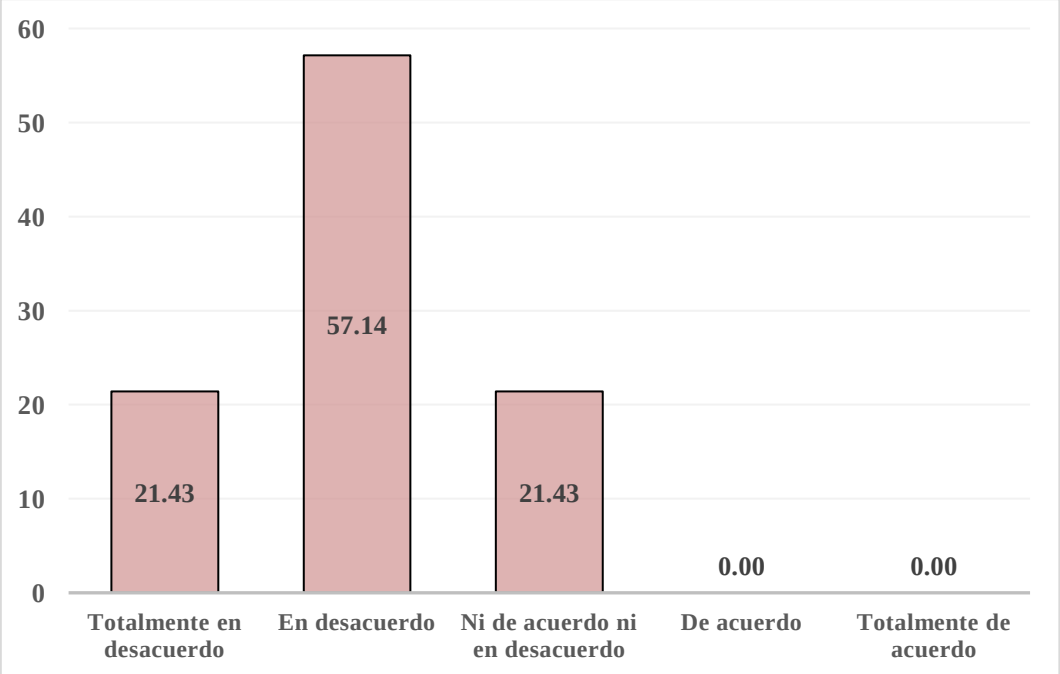
Fuente: Elaboración propia.

Tabla 29: Distribución de funcionarios según opinión si existe seguridad en los procesos de desarrollo y soporte de los sistemas de información.

Alternativas	n	%
Totalmente en desacuerdo	3	21.43
En desacuerdo	8	57.14
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 29: Distribución de funcionarios según opinión si existe seguridad en los procesos de desarrollo y soporte de los sistemas de información.



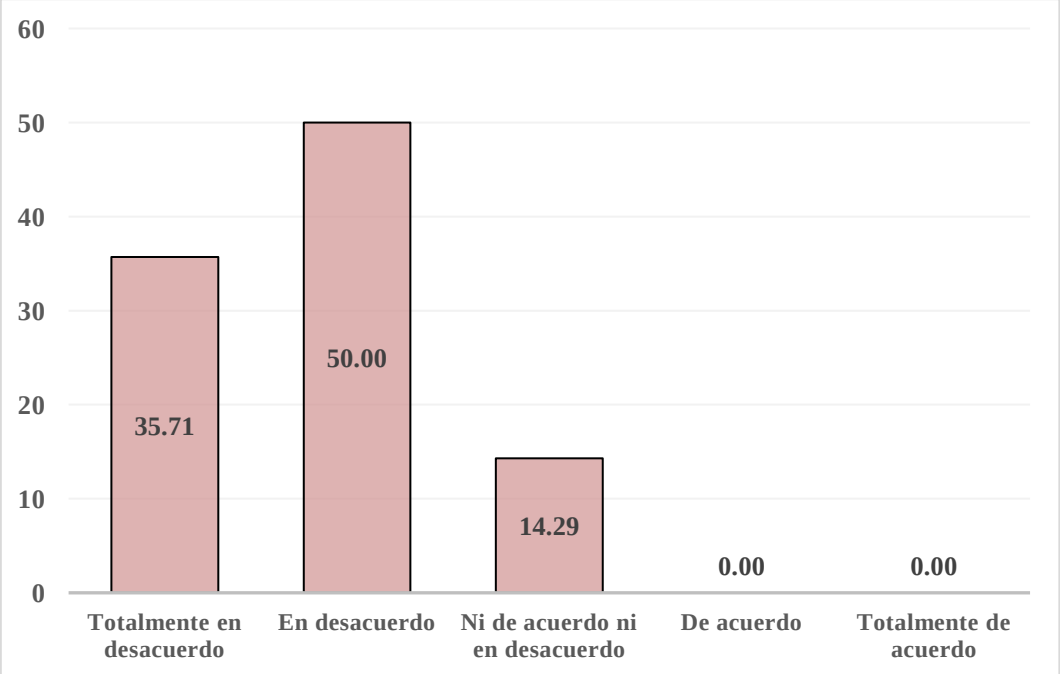
Fuente: Elaboración propia.

Tabla 30: Distribución de funcionarios según opinión si existe una adecuada gestión de vulnerabilidad técnica de los sistemas de información.

Alternativas	n	%
Totalmente en desacuerdo	5	35.71
En desacuerdo	7	50.00
Ni de acuerdo ni en desacuerdo	2	14.29
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 30: Distribución de funcionarios según opinión si existe una adecuada gestión de vulnerabilidad técnica de los sistemas de información.



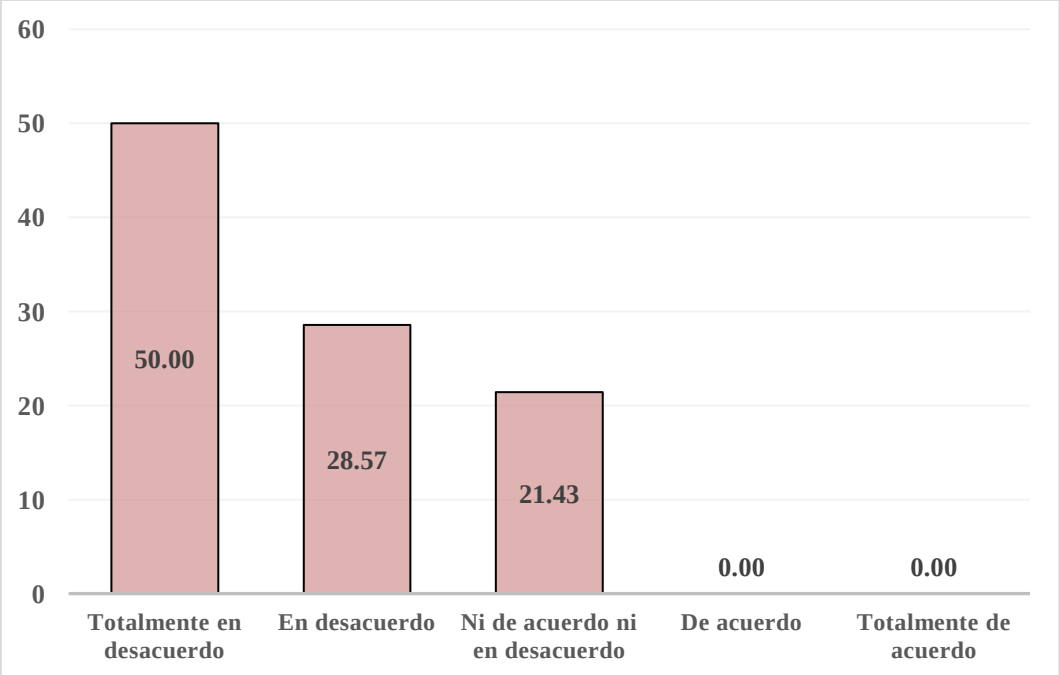
Fuente: Elaboración propia.

Tabla 31: Distribución de funcionarios según opinión si existe un reporte sobre los eventos y las vulnerabilidades de la seguridad de la información.

Alternativas	n	%
Totalmente en desacuerdo	7	50.00
En desacuerdo	4	28.57
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 31: Distribución de funcionarios según opinión si existe un reporte sobre los eventos y la vulnerabilidad de la seguridad de información.



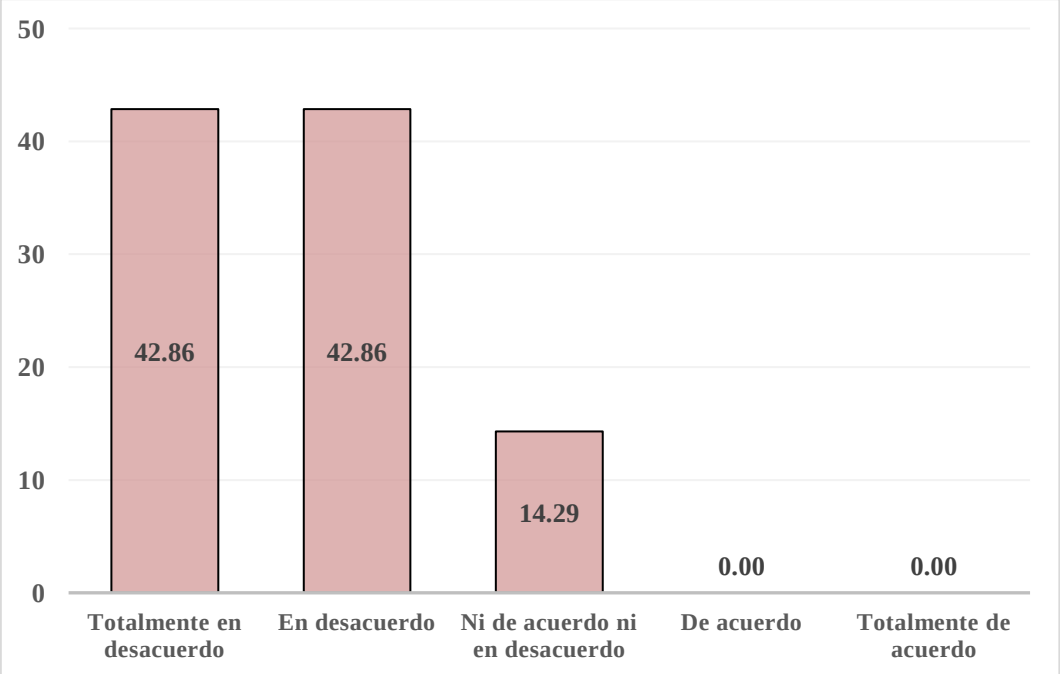
Fuente: Elaboración propia.

Tabla 32: Distribución de funcionarios según opinión si existe una adecuada gestión de incidentes de seguridad de la información.

Alternativas	n	%
Totalmente en desacuerdo	6	42.86
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	2	14.29
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 32: Distribución de funcionarios según opinión si existe una adecuada gestión de incidentes de seguridad de la información.



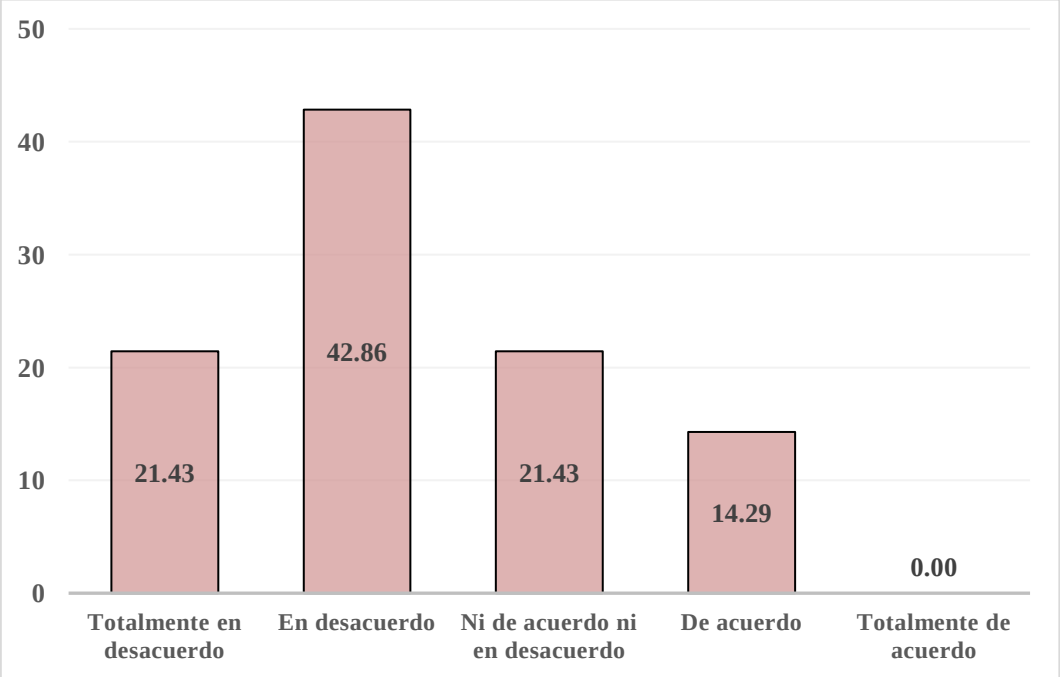
Fuente: Elaboración propia.

Tabla 33: Distribución de funcionarios según opinión si se realizan auditorías a los sistemas de información.

Alternativas	n	%
Totalmente en desacuerdo	3	21.43
En desacuerdo	6	42.86
Ni de acuerdo ni en desacuerdo	3	21.43
De acuerdo	2	14.29
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Aplicación de instrumento Anexo 1 Cuestionario.

Figura 33: Distribución de funcionarios según opinión si se realizan auditorías a los sistemas de información.



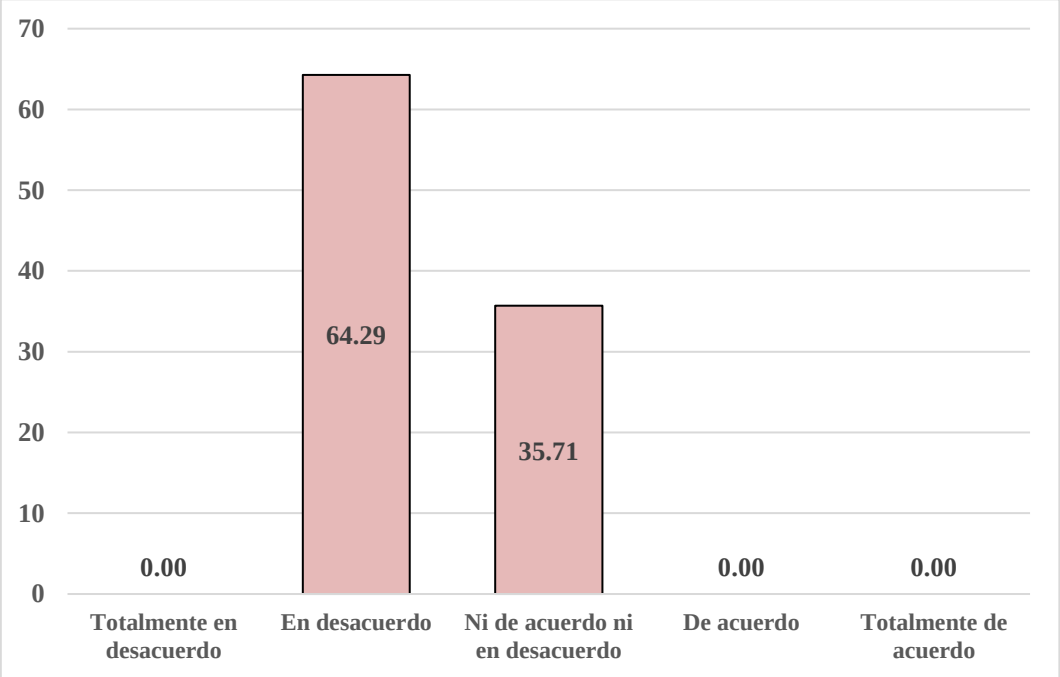
Fuente: Elaboración propia.

Tabla 34: Resumen General

Alternativas	n	%
Totalmente en desacuerdo	0	0.00
En desacuerdo	9	64.29
Ni de acuerdo ni en desacuerdo	5	35.71
De acuerdo	0	0.00
Totalmente de acuerdo	0	0.00
TOTAL	**14**	**100.00**

Fuente: Resumen de aplicación de instrumento Anexo 1 Cuestionario.

Figura 34: Distribución Resumen General



Fuente: Elaboración propia.

4.2. ANÁLISIS DE LOS RESULTADOS

Según los resultados obtenidos de la encuesta aplicada a los funcionarios de la Dirección Regional de Educación de Piura (DREP) respecto a la seguridad informática, se aprecia en la tabla 1 que el 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. A partir de los resultados se infiere que las políticas de seguridad informática no son conocidas por los funcionarios o no existe una declaración formal.

En la tabla 2, se puede apreciar 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. Se deduce que en la DREP no se cumplen las políticas de seguridad, quizá por falta de conocimiento.

Respecto a la existencia de una organización interna para la seguridad de la información, en la tabla 3 se evidencia que los funcionarios están en desacuerdo, y a su vez ni de acuerdo ni en desacuerdo en un 35,7 % respectivamente; evidenciando falta de organización por parte del área y de los directivos encargados de la dirección.

En la tabla 4, respecto a la existencia de una organización externa para la seguridad de la información, los resultados señalan que el 64,3 % de los funcionarios están en desacuerdo, además un 28,6 % se encuentra en total desacuerdo. Evidenciando una falta de eficacia en la gestión, desde la organización interna.

Los resultados de la tabla 5, en relación a la existencia de una adecuada responsabilidad sobre los activos de la DREP; los funcionarios se muestran en desacuerdo en un 35,7 %; también un 35,7 % se manifiesta estar ni de acuerdo ni en desacuerdo. Evidenciando la falta de compromiso con los activos, y por ende un desinterés por los activos con los que cuenta la DREP para realizar la parte operativa de seguridad de información y comunicación.

Respecto a si se clasifica la información en la DREP, en la tabla 6 se aprecia que el 42,9 % de los funcionarios se encuentran en desacuerdo; de la misma manera solamente el 14,3 % se encuentra de acuerdo. Por lo que se deduce que no existe una adecuada clasificación de la información; y debido a ello puede originarse una confusión, que mengue la eficacia de la institución.

En la tabla 7, en cuanto a la existencia de seguridad en el recurso humano antes de la contratación, los funcionarios se muestran de acuerdo en un 35,7 % y un 14,3 % totalmente de acuerdo, evidenciando que se maneja discretamente la información brindada por el postulante antes de la contratación.

Los resultados de la tabla 8, refieren que el 64,3 % de los funcionarios se muestran de acuerdo sobre la seguridad que se le brinda al recurso humano durante la vigencia de su contratación, reafirmando la adecuada gestión del área de recursos humanos, en base a la información de sus trabajadores.

En relación a la seguridad del recurso humano al término o cambio de contratación del servidor en la DREP, el 21,4 % de los funcionarios se muestran de acuerdo; mientras que un 50 % se muestra ni de acuerdo ni en desacuerdo, ya que en algunas oportunidades se filtra información sobre todo cuando un servidor pasa por un cambio de contratación.

En la tabla 10, respecto a si la DREP cuenta con áreas seguras, se evidencia que el 35,7 % de los funcionarios se muestran ni de acuerdo ni en desacuerdo; asimismo se muestran de en desacuerdo en el mismo porcentaje; deduciendo que las áreas tangibles de la institución se encuentran deterioradas o mal organizadas, por lo que no se consideran seguras, ante cualquier fenómeno o evento calamitoso.

En cuanto a la evidencia de un nivel adecuado de seguridad para los equipos de información y comunicación; en la tabla 11 se aprecia que el 42,9 % de los funcionarios se muestran en desacuerdo; y de igual manera ni de acuerdo ni en desacuerdo. Infiriendo que los equipos tecnológicos se encuentran desprotegidos y en un nivel de mantenimiento bajo.

En relación a los procedimientos operacionales y la responsabilidad de los mismos es idónea, los funcionarios evidencian en la tabla 12 que un 50 % se muestra ni de acuerdo ni en desacuerdo; por otro lado, un 28,6 % manifiesta encontrarse de acuerdo. Se puede inferir que ello depende de los mismos servidores y su nivel de involucramiento y compromiso para con la institución.

En la tabla 13, en cuanto a la gestión de prestación de servicios por terceros es la adecuada; un 42,9 % se muestra en desacuerdo; asimismo un 42,9 % de los funcionarios se encuentra ni de acuerdo ni en desacuerdo; por lo que se deduce que la gestión de prestación de servicios por terceros no se realiza adecuadamente, ya sea por la contratación o la calidad de servicios entregados; por lo cual se hace necesario un control.

En relación a la existencia de planificación y aceptación de sistemas informáticos en la DREP, la tabla 14 evidencia que el 50 % de los funcionarios se encuentra en desacuerdo; asimismo un 35,7 % se muestra ni de acuerdo ni en desacuerdo. Se deduce que hace falta planificación y que el sistema que se utiliza no es aceptado de manera unánime, debido a errores o fallas o por la facilidad en el manejo.

En la tabla 15, respecto a la existencia de protección contra códigos maliciosos o móviles, un 42,9 % de los funcionarios se muestra de acuerdo y un 28,6 % en total desacuerdo. Se infiere que ha sucedido experiencias sobre infección de virus en el sistema que ha perjudicado la información que se protege en la DREP.

En cuanto a si se cuenta con un respaldo informático adecuado en la DREP, la tabla 16 evidencia que un 42,9 % de los funcionarios se muestra en desacuerdo; además un 21,4 % se muestra ni de acuerdo ni en desacuerdo; y el mismo porcentaje se muestra de acuerdo. Infiriendo que, si existe un respaldo, pero no es muy eficaz, debido a falta de tecnología o de recurso humano capaz de gestionar eficientemente los recursos con que se cuenta.

En relación al nivel de gestión de seguridad de redes, en la tabla 17 los funcionarios se muestran en desacuerdo con 42,9 %, y un 28,6 % se muestra ni

de acuerdo ni en desacuerdo. Se deduce que el nivel de seguridad no es el idóneo para una institución grande y que almacena grandes volúmenes de información.

En la tabla 18, respecto al manejo de los medios digitales en la DREP, el 50 % de los funcionarios se muestran en desacuerdo y un 28,6 % en total desacuerdo. Se infiere que faltan mayores recursos TIC para contar con una mejor gestión y capacitar a los responsables en los sistemas que se utilizan dentro de la institución.

En la tabla 19, en cuanto a si se realiza un intercambio de información idóneo en la DREP, los resultados demuestran que el 42,9 % de los funcionarios se muestran en total desacuerdo, asimismo un 35,7 % se muestra en desacuerdo. Se infiere que ello sucede por la falta de organización y de relaciones con las diferentes áreas en la institución.

En la tabla 20, en relación al monitoreo constante sobre la gestión de comunicaciones y operaciones, los funcionarios se muestran en un 35,7 % ni de acuerdo ni en desacuerdo; asimismo en igual porcentaje se muestran de acuerdo. Se infiere que debido a la necesidad de mejorar la gestión de la seguridad informática se realizan monitoreo, tratando de optimizar la comunicación y operaciones en la institución.

En relación a la gestión de acceso de los usuarios; la tabla 21 presenta que los funcionarios en un 42,9 % se encuentra ni de acuerdo ni en desacuerdo, además un 28,6 % se muestra en desacuerdo; ya que se evidencian muchos inconvenientes en el acceso por parte de los servidores en el sistema de la institución.

Por otro lado, en la tabla 22, en cuanto a la responsabilidad en el acceso por parte de los servidores a los sistemas de información, un 35,7 % de los funcionarios se muestra de acuerdo y de igual porcentaje ni de acuerdo ni en desacuerdo. Se deduce que existen consecuencias por el uso inadecuado del acceso al sistema por lo que los servidores tratan de acceder de forma consecuente.

En cuanto a los controles de accesos a las redes, en la tabla 23 se evidencia que los funcionarios se muestran en un 42,9 % en desacuerdo; poniendo énfasis en la falta de seguridad informática existente en el sistema de la institución.

De igual forma en la tabla 24, los funcionarios reafirman en un 42,9 % estar en desacuerdo sobre los controles de acceso al sistema operativo; por lo que es necesario contar con alguna estrategia de control que permita mejorar la gestión.

En relación al control de acceso a las aplicaciones y a la información en la tabla 25 se evidencia que un 57,1 % de los funcionarios se muestran en desacuerdo, evidenciando la falta de un control.

En la tabla 26, respecto a si se cumplen con los requisitos de seguridad de los sistemas de información, el 35,7 % de los funcionarios se muestra ni de acuerdo ni en desacuerdo, además en igual porcentaje se encuentra en desacuerdo; se deduce que los requisitos de seguridad no son los adecuados.

Respecto a si existe un procesamiento correcto en las aplicaciones, en la tabla 27 se aprecia que el 50 % de los funcionarios manifiestan estar ni de acuerdo ni en desacuerdo; debido a las fallas constantes del sistema, llevando como consecuencia la ineficacia de los procesos en las aplicaciones que hacen uso los servidores.

En la tabla 28, sobre la evidencia de la seguridad de los archivos de los sistemas de información de la DREP, los funcionarios en un 42,9 % se muestran en desacuerdo, manifestando su descontento y desconfianza sobre la seguridad de los archivos e información en la institución, lo que puede originar pérdida de datos importantes.

Respecto a la seguridad en los procesos de desarrollo y soporte de los sistemas de información, en la tabla 29 se aprecia que los funcionarios en un 57,1 % se muestran en desacuerdo; lo que indica la necesidad de contar con una herramienta que permita mejorar los procesos de soporte informático en la institución.

En cuanto a la existencia de una adecuada gestión de vulnerabilidad técnica de los sistemas de información, la tabla 30 evidencia que el 50 % de los funcionarios está en desacuerdo; permitiendo inferir que existe preocupación por la vulnerabilidad en el sistema, sobre todo en la parte técnica de la institución.

En la tabla 31, respecto a la existencia de reportes sobre los eventos y las vulnerabilidades de la seguridad de la información, los funcionarios en un 50 % se muestran totalmente en desacuerdo, asimismo un 28,6 % se muestra en desacuerdo. Por lo que se deduce que es necesario implementar una herramienta estratégica que permita la mejora de la gestión de TIC.

Al referirse a la existencia de una adecuada gestión de incidentes de seguridad de información en la tabla 32, un 42,9 % de los funcionarios se muestran en total desacuerdo y en desacuerdo respectivamente; evidenciando una vez más la imperiosa necesidad de un contar con un soporte que permita el mejoramiento de la gestión de información y comunicación en la DREP.

Finalmente, en la tabla 33, respecto a si se realizan auditorías a los sistemas de información, un 42,9 % de los funcionarios se muestran en desacuerdo, por lo que se deduce la falta de control sobre los sistemas de información y comunicación existentes en la institución.

4.3. PROPUESTA SOLUCIÓN HOLÍSTICA

Luego del análisis de los resultados obtenidos en la presente investigación, que como resumen general arrojaron el 64.29 % de funcionarios entrevistados están en desacuerdo, y el 35.71 % ni de acuerdo ni en desacuerdo con la seguridad informática, se plantea como propuesta diseñar una 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.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

COBIT 5.0 cuenta con principios y habilitadores genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

En esta investigación se han descrito los principales elementos considerados en la definición de un modelo de seguridad de información de las TIC. Se expone un breve análisis de la relevancia y urgencia del tema. Se debe tener presente que el modelo de implementación es totalmente perfectible, ajustable y que puede ser dimensionado conforme a las particularidades y tamaño de la institución en estudio. Dada la gama de actividades consideradas en el modelo, consideramos que este puede ser la base para establecer un "Gobierno de TI" en la Dirección Regional de Educación de Piura.

Se evidenció que la DRE. Piura presenta diversos inconvenientes dentro del manejo de la información, consecuencia de la falta de conciencia de la importancia de asegurar la información existente; ausencia de políticas que regulen las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información.

5.2. RECOMENDACIONES

La DRE. Piura debe considerar integrar sus sistemas, realizando buenas prácticas para evitar posibles delitos informáticos que obstaculicen su normal funcionamiento; contar con una adecuada gestión de vulnerabilidad técnica y contar con reportes sobre los eventos, por medio de una gestión de incidentes.

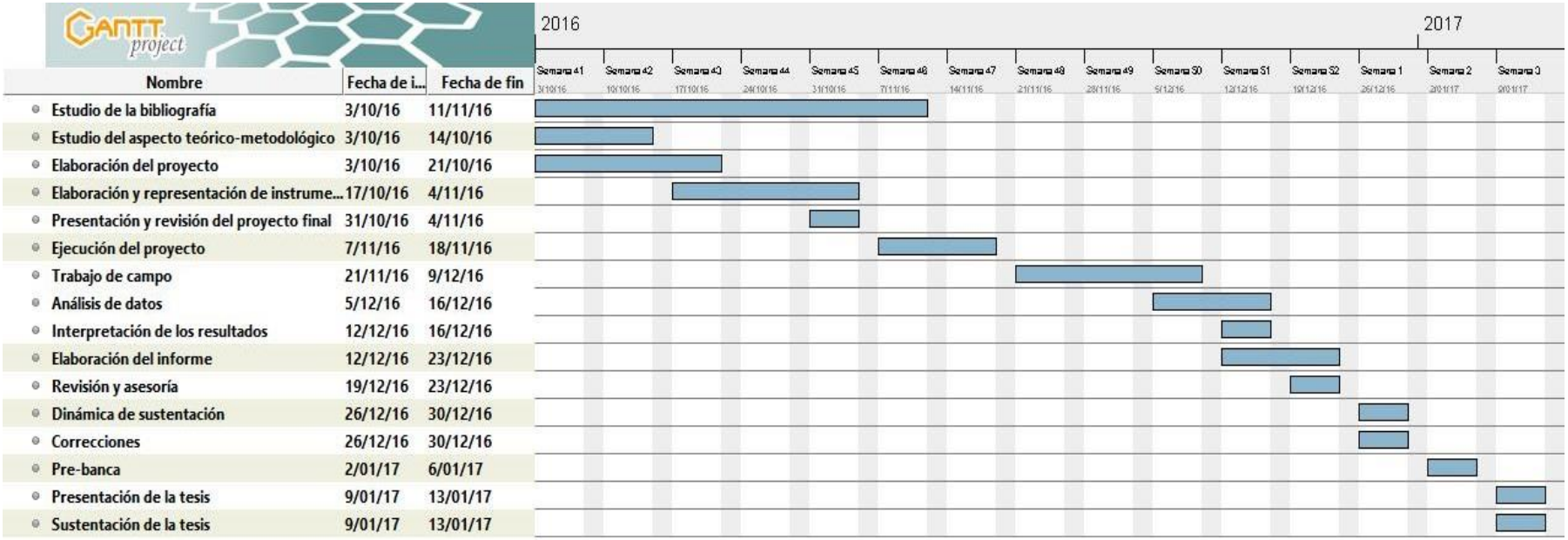
Se debe implementar una versión informática que permita obtener el valor óptimo de las tecnologías de la información. Siendo la versión COBIT 5.0 la idónea ya que se enfoca en el gobierno empresarial de las TIC; manteniendo un

equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

Ya que el análisis de los resultados arrojó que la hipótesis de esta investigación es aceptada, se recomienda que la Dirección Regional de Educación de Piura, en coordinación con el equipo de informática de la misma, diseñe e implemente una solución holística de seguridad informática para mejorar la gestión de las TIC.

ASPECTOS COMPLEMENTARIOS

MATRIZ DE ACTIVIDADES



Nombre	Fecha de i...	Fecha de fin
Estudio de la bibliografía	3/10/16	11/11/16
Estudio del aspecto teórico-metodológico	3/10/16	14/10/16
Elaboración del proyecto	3/10/16	21/10/16
Elaboración y representación de instrume...	17/10/16	4/11/16
Presentación y revisión del proyecto final	31/10/16	4/11/16
Ejecución del proyecto	7/11/16	18/11/16
Trabajo de campo	21/11/16	9/12/16
Análisis de datos	5/12/16	16/12/16
Interpretación de los resultados	12/12/16	16/12/16
Elaboración del informe	12/12/16	23/12/16
Revisión y asesoría	19/12/16	23/12/16
Dinámica de sustentación	26/12/16	30/12/16
Correcciones	26/12/16	30/12/16
Pre-banca	2/01/17	6/01/17
Presentación de la tesis	9/01/17	13/01/17
Sustentación de la tesis	9/01/17	13/01/17

Fuente: Elaborado por el investigador.

PRESUPUESTO Y FINANCIAMIENTO

Título : 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.

Responsable : Ing. Joseph Adrián Guaylupo Ocaña

Presupuesto : S/. 1,178.00

Fuente : Recursos Propios

RUBRO	DESCRIPCION	UNIDAD	CANT.	VALOR	PARCIAL
Transporte	Movilidad x 2 personas.	Días	40	S/. 6.00	S/. 240.00
	Asignaciones Adicionales.	Días	40	S/. 15.00	S/. 600.00
Materiales de Oficina	Lápices Mongol N° 2.	Unidad	2	S/. 1.00	S/. 2.00
	Lapiceros.	Unidad	3	S/. 1.00	S/. 3.00
	Plumones Pinta fina.	Unidad	2	S/. 4.00	S/. 8.00
	Plumones tinta indeleble.	Unidad	1	S/. 5.00	S/. 5.00
	Pegamento.	Unidad	1	S/. 3.50	S/. 3.50
	Folder Manila A-4.	Unidad	10	S/. 1.00	S/. 10.00
	Resaltadores.	Unidad	2	S/. 3.00	S/. 6.00
	Clips.	Unidad	1	S/. 3.00	S/. 3.00
	CD RW.	Unidad	5	S/. 5.00	S/. 25.00
	Grapas.	Caja	1	S/. 7.00	S/. 7.00
Impresos	Encuestas.	Unidad	80	S/. 0.50	S/. 40.00
	Informe.	Unidad	80	S/. 0.50	S/. 40.00
	Proyecto Tesis.	Unidad	146	S/. 0.50	S/. 73.00
	Diapositivas Tesis.	Unidad	25	S/. 0.50	S/. 12.50
	Tesis.	Unidad	200	S/. 0.50	S/. 100.00
TOTAL			**S/.**		**1,178.00**

REFERENCIAS BIBLIOGRÁFICAS

1. Concepto.de. Concepto de Holística [homepage en Internet] concepto.de; c2015 [actualizada 2015; consultado 11 octubre 2016]. Disponible en: http://concepto.de/holistica/

2. Definición.de. Definición de Tecnologías de la Información [homepage en Internet]. Julián Pérez Porto y Ana Gardey; c2014 [actualizada 2016; consultado 11 octubre 2016]. Disponible en: http://definicion.de/tecnologia-de-la-informacion/

3. Asociación Española para la Calidad - AEC [homepage en Internet]. España: Asociación Española para la Calidad; c2016 [actualizada 11 octubre 2016; consultado 11 octubre 2016]. Disponible en: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

4. Aranda L. Estudio de Sistemas de Seguridad basado en la detección de Intrusión Física y Tecnológica [Tesis]. Santander: Universidad de Cantabria. Facultad de Ciencias Económicas y Empresariales; 2013

5. Arias B, Merizalde A, Noriega G. Análisis y Solución de las Vulnerabilidades de la Seguridad Informática y Seguridad de la Información de un Medio de Comunicación Audio-Visual [Tesis]. Guayaquil: Universidad Politécnica Salesiana. Facultad de Ingenierías; 2013

6. Robayo L, Rodríguez R. Aseguramiento de los sistemas computacionales de la empresa SITIOSDIMA.NET [Tesis]. Colombia: Universidad Nacional Abierta y a Distancia – UNAD; 2015.

7. Campos B. Sistema de Monitoreo de Seguridad Física en Plataforma Libre de Componentes Electrónicos para asegurar la Gestión de los Niveles de Continuidad de los Servicios Informáticos en la Central de Datos USAT [Tesis]. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo. Facultad de Ingeniería; 2015.

8. Alcántara F. Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo [Tesis]. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo. Facultad de Ingeniería; 2015.

9. Aguirre M. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. [Tesis] Lima: Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería; 2014.

10. Ramos A. Propuesta de un plan de auditoría informática para el "Sistema de información en salud" y el "Aplicativo para el registro de formatos SIS" en los establecimientos de salud de la unidad ejecutora 400 en la Región Piura en el año 2015 [Tesis] Piura: Universidad Nacional de Piura. Facultad de Ingeniería Industrial. Escuela Profesional de Ingeniería Informática; 2015.

11. Arévalo H. Estudio y diseño de red de datos y cámaras de seguridad en la empresa REGENDA H Y D Inversiones y Servicios EIRL. Castilla – Piura; 2016 [Tesis] Piura: Universidad Católica Los Ángeles de Chimbote. Facultad de Ingeniería. Escuela Profesional de Ingeniería de Sistemas; 2016.

12. Cobo R. El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento [Monografía en Internet]. País Vasco: Universidad del País Vasco; c2008. [aprobado 22 de septiembre 2009; consultado 12 de octubre 2016]. Disponible en: http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf

13. Fernández Muñoz, R. Marco conceptual de las nuevas tecnologías aplicadas a la educación [Internet] Universidad de Castilla – La Mancha, España; c2009 [consultado 12 de octubre 2016] Disponible en: http://www.uclm.es/profesorado/ricardo/ DefinicionesNNTT.html

14. Almenara, C.; Barroso Osuna, J.; Romero Tena, R.; Llorente Cejudo, M. y Román Gravan, P. Definición de Nuevas Tecnologías [Internet] OCW de la Universidad de Sevilla, Facultad de Ciencias de la Educación. España; c2007. [actualizado junio 2009; consultado 12 de octubre 2016] Disponible en: http://ocwus.us.es/didactica-y-organizacionescolar/nuevas-tecnologias-aplicadas-a-la-educacion/NTAE/ asigntae/apartados_NNTT/apartado3-2.asp.html

15. Costa, R. El uso de las TIC en las organizaciones [Internet]. EADA Blog; c2012. [consultado 12 de octubre 2016]. Disponible en: http://blogs.eada.edu/2012/07/05/tecnologias-informacion-en-empresa/

16. Blog Andalucía es digital. Ventajas de las TICs para las empresas [Internet]. España: Blog Andalucía es digital; c2016. [consultado 13 de octubre 2016]. Disponible en: http://www.blog.andaluciaesdigital.es/ventajas-de-las-tics-para-las-empresas/

17. Torrent-Sellens. TIC y trabajo: hacia nuevos sistemas organizativos, nuevas estructuras ocupacionales y salariales, y nuevos mecanismos de intermediación [Monografía en Internet]. Cataluña: Universidad Abierta de Cataluña; c2008. [aprobado febrero 2009; consultado 12 de octubre 2016]. Disponible en: http://www.uoc.edu/uocpapers/6/dt/esp/dossier_tic_y_trabajo.pdf

18. WIKIPEDIA. Seguridad de la información [Internet]. WIKIPEDIA; c2017. [actualizado septiembre 2017, consultado 23 de octubre 2017]. Disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

19. SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? [Internet]. SGSI; c2015. [actualizado julio 2017, consultado 23 de octubre 2017]. Disponible en: http://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

20. Markus Erb. Seguridad de la Información y Protección de Datos [Internet]. España: Gestión de Riesgo en la Seguridad Informática; c2009. [consultado 23 de octubre 2017]. Disponible en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

21. SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Qué es SGSI? [Internet]. SGSI; c2015. [actualizado julio 2015, consultado 23 de octubre 2017]. Disponible en: http://www.pmg-ssi.com/2015/07/que-es-sgsi/

22. ESAN. ¿Cómo implementar un Sistema de Gestión de Seguridad de la Información? [Internet]. Perú: Universidad ESAN; c2014. [publicado mayo 2016, consultado 23 de octubre 2017]. Disponible en: https://www.esan.edu.pe/apuntes-empresariales/2016/05/como-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion/

23. Ramírez, R. Cobit 5 [Monografía en Internet]. México: Magazcitum; c2010. [publicado septiembre 2012; consultado 12 de octubre 2016]. Disponible en: http://www.magazcitum.com.mx/?p=1893

24. Osores, M. Principios de COBIT 5 para el gobierno efectivo de TI [Internet]. TechTarget; c2010-2016. [actualizado julio 2014; consultado 12 de octubre 2016]. Disponible en: http://searchdatacenter.techtarget.com/es/cronica/Principios-de-COBIT-5-para-el-gobierno-efectivo-de-TI

25. Auditoria Informatica. Habilitadores de COBIT 5 [Internet]. Auditoria Informatica; c2015. [consultado 13 de octubre 2016]. Disponible en: https://chaui201511700921278.wordpress.com/2015/04/28/habilitadores-de-cobit-5/

26. ISACA. What is COBIT 5? [Internet]. ISACA; c2016. [consultado 13 de octubre 2016]. Disponible en: www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

27. QAP. Cobit domains and processes (COBIT 5 / 4.1) [Internet]. QAP; c2010. [consultado 13 de octubre 2016]. Disponible en: http://www.qualified-audit-partners.be/index.php?cont=463

28. Orta, O. Análisis de madurez y capacidad de procesos según Cobit 5 [Internet]; c2014. [actualizado septiembre 2014, consultado 14 de octubre 2016]. Disponible en: http://gesegtic.blogspot.pe/2014/09/analisis-de-madurez-y-capacidad-de.html

29. Braga, G. Cómo COBIT 5 mejora la capacidad de procesos de trabajo de auditores, profesionales de aseguramiento y evaluadores [Internet]; c2016. [consultado 14 de octubre 2016]. Disponible en: https://www.isaca.org/Journal/archives/2016/Volume-1/Documents/How-COBIT-5-Improves-the-Work-Process-Capability-of-Auditors-Assurance-Professionals-and-Assessors_joa_Spa_0116.pdf

30. Vara-Horna, A. Desde la idea hasta la sustentación: 7 pasos para una tesis exitosa [Internet]; c2012. [consultado 14 de octubre 2016]. Disponible en: http://www.administracion.usmp.edu.pe/investigacion/files/7-PASOS-PARA-UNA-TESIS-EXITOSA-Desde-la-idea-inicial-hasta-la-sustentaci%C3%B3n.pdf

31. Hernández Sampieri, R.; Fernández Collado, C.; Baptista Lucio, M. Metodología de la Investigación [Internet]; c2010. [consultado 14 de octubre 2016]. Disponible en: http://www.pucesi.edu.ec/web/wp-content/uploads/2016/04/Hern%C3%A1ndez-Sampieri-R.-Fern%C3%A1ndez-Collado-C.-y-Baptista-Lucio-P.-2003.-Metodolog%C3%ADa-de-la-investigaci%C3%B3n.-M%C3%A9xico-McGraw-Hill-PDF.-Descarga-en-l%C3%ADnea.pdf

ANEXOS

ANEXO 1 CUESTIONARIO

UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE
ESCUELA DE POSGRADO
FACULTAD DE INGENIERÍA DE SISTEMAS

Buenos días y/o tardes; las siguientes preguntas son de carácter confidencial y tienen fines académicos, destinadas a recabar información necesaria que servirá de soporte a la investigación que se realiza en cuanto a la 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. Agradeciendo su colaboración, lea cuidadosamente cada pregunta y marque con una X según corresponda.

Sexo: M __ F __	**Edad:** 18 -25 __ 26 -35 __ 36 - 45 __ 45 a más __
Área de trabajo: _____	
Cargo que desempeña: _____	
Tiempo en el cargo: Menos de 01 año __ 01 - 03 años __ 03 - 05 años __ Más de 05 años __	

SEGURIDAD INFORMÁTICA

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Políticas de Seguridad	**1**	**2**	**3**	**4**	**5**
1. Existen políticas de seguridad de la información en la DREP.					
2. Se cumplen políticas de seguridad de información en la DREP.					
Organización de la seguridad de la información	**1**	**2**	**3**	**4**	**5**
3. Existe una organización interna para la seguridad de la información.					

4. Existe una organización externa para la seguridad de la información.					
Gestión de activos	**1**	**2**	**3**	**4**	**5**
5. Existe una adecuada responsabilidad sobre los activos de la DREP.					
6. Se clasifica la información en la DREP.					
Seguridad en el Recurso Humano	**1**	**2**	**3**	**4**	**5**
7. Existe seguridad en los recursos humanos antes de la contratación.					
8. Se le brinda seguridad al recurso humano durante la vigencia de la contratación.					
9. En la terminación o cambio de contratación se continua con la seguridad del recurso humano.					
Seguridad Física y Ambiental	**1**	**2**	**3**	**4**	**5**
10. Se cuenta con áreas seguras					
11. Se evidencia un nivel adecuado para la seguridad de los equipos.					
Gestión de las comunicaciones y operaciones	**1**	**2**	**3**	**4**	**5**
12. Los procedimientos operacionales y de responsabilidades son idóneos.					
13. La gestión de la prestación de servicios por terceros es la adecuada.					

14. Existe una planificación y aceptación de sistemas informáticos en la DREP.					
15. Existe protección contra códigos maliciosos y móviles.					
16. Se cuenta con un respaldo informático adecuado en la DREP.					
17. Se evidencia un nivel de gestión de seguridad en las redes.					
18. Existe un manejo de medios digitales adecuado en la DREP.					
19. Se realiza un intercambio de información idóneo en la DREP.					
20. Se monitorea constantemente la gestión de comunicaciones y operaciones en la DREP.					
Control de acceso	**1**	**2**	**3**	**4**	**5**
21. La gestión de acceso de los usuarios se realiza adecuadamente.					
22. Los usuarios evidencian responsabilidad en el acceso a los sistemas de información.					
23. Se cuenta con controles de acceso a las redes.					
24. Existe un control de acceso al sistema operativo.					
25. El control de acceso a las aplicaciones y a la información es regulado.					

Adquisición, Desarrollo y mantenimiento de Sistema de Información	**1**	**2**	**3**	**4**	**5**
26. Se cumplen con los requisitos de seguridad de los sistemas de información.					
27. Existe un procesamiento correcto en las aplicaciones.					
28. Es evidente la seguridad de los archivos de los sistemas de información de la DREP.					
29. Existe seguridad en los procesos de desarrollo y soporte de los sistemas de información.					
30. Existe una adecuada gestión de vulnerabilidad técnica de los sistemas de información.					
Gestión de incidentes de seguridad	**1**	**2**	**3**	**4**	**5**
31. Existe un reporte sobre los eventos y la vulnerabilidad de la seguridad de la información.					
32. Existe una adecuada gestión de incidentes de seguridad de la información.					
Cumplimiento	**1**	**2**	**3**	**4**	**5**
33. Se realizan auditorías a los sistemas de información.					