UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA DE SISTEMAS, INDUSTRIAL E INFORMÁTICA

TESIS

AUDITORIA EN SEGURIDAD INFORMÁTICA Y GESTION DE RIESGO EN EL HOSPITAL REGIONAL DE HUACHO, 2018

PRESENTADO POR:

ALAN RAUL GAVINO LLAGAS

PARA OPTAR EL GRADO ACADÉMICO DE INGENIERO INFORMÁTICO

ASESOR:

Ing. ANGEL HUAMÁN TENA

HUACHO - 2018

AUDITORIA EN SEGURIDAD INFORMÁTICA Y GESTION DE RIESGO EN EL HOSPITAL REGIONAL DE HUACHO, 2018

ALAN RAUL GAVINO LLAGAS

ASESOR: Ing. ANGEL HUAMÁN TENA

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN
FACULTAD DE INGENIERIA DE SISTEMAS, INDUSTRIAL E INFORMÁTICA

ESCUELA DE INGENIERIA INFORMÁTICA
HUACHO

2018

DEDICATORIA

A mis padres por todo el apoyo que me brindan tanto moral como espiritual, por todo el amor y dedicación que me dan para poder seguir adelante siempre con el objetivo de poder lograr una prosperidad para nuestra familia, por acompañarme en los momentos más difíciles y no permitirme flaquear o declinar ante ninguna dificultad.

ALAN RAUL GAVINO LLAGAS

AGRADECIMIENTO

Mi agradecimiento muy especial al Ing. Ángel Huamán Tena por haberme guiado en la elaboración de la presente tesis.

ALAN RAUL GAVINO LLAGAS

ÍNDICE

RESUMEN

Objetivo: Analizar la auditoria en seguridad informática para determinar su relación con la gestión de riesgo en el Hospital Regional de Huacho, 2018. Métodos: Se ha empleado el método científico en sus niveles de análisis y síntesis y corresponde al diseño no experimental, transversal correlacional puesto que el trabajo metodológico ha consistido en analizar la relación de las variables: Auditoria en seguridad informática y Gestión de Riesgo, asimismo es un estudio cuantitativo de investigación. Resultado: La investigación nos ha permitido comprobar que la Auditoria en seguridad informática tiene una relación directa con la Gestión de Riesgo en el Hospital Regional Huacho, 2018. Conclusiones: Que la Auditoria en seguridad informática tiene una relación directa en un grado de correlación muy alta (0,936) con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

Palabras clave**:** Auditoria, Gestión, informática.

ABSTRACT

Objective: to analyze the safety in the environment to determine its relationship with risk management in the Huacho Regional Hospital, 2018. Methods: The scientific method has been used in its levels of analysis and synthesis and corresponds to a non-experimental, correlational design transversal methodological work has consisted in analyzing the relationship of the variables: computer security audit and risk management, as well as a quantitative research study. Result: The investigation has allowed us that the Computer Security Audit has a direct relationship with the Risk Management in the Huacho Regional Hospital, 2018. Conclusions: That the Computer Security Audit has a direct relationship in a very high degree of correlation (0.936) with Risk Management at the Huacho Regional Hospital, 2018.

Keywords: audit, management, informatics

INTRODUCCIÓN

Las variables de estudio se han examinado y analizado con la finalidad de conocer si existe o no relación entre ellas. Estas variables son Auditoria en seguridad informática y Gestión de Riesgo. El resultado de esta investigación ha permitido conocer que existe relación entre ellas cuyos detalles se presentan y analizan en todo el contenido de la tesis.

Este trabajo de investigación lo he desarrollado con el propósito de obtener mi grado de ingeniero informático. En su elaboración se ha seguido los pasos del método científico, en tal sentido, espero haber cumplido con todos los requisitos metodológicos y procedimentales para desarrollar la presente Tesis y para su estudio se ha dividido en cinco capítulos.

En el Capítulo I, se trata del planteamiento del problema de investigación, de su identificación, su formulación, su importancia, su justificación y las limitaciones del trabajo de investigación.

El Capítulo II, está destinado para el Marco Teórico en el mismo que tratamos los Antecedentes Teóricos, las Bases Teóricas dentro del cual se ha considerado los temas relacionadas con las variables en estudio tales como: vocación profesional, psicología educativa, factores de evaluación en la orientación vocacional, intereses, herramientas, sistemas de orientación vocacional, etc. En este mismo capítulo también se ha realizado un tratamiento teórico del rendimiento académico: Concepto y significado, coeficiente y eficiencia, rendimiento académico y el aprendizaje, etc.

En el Capítulo III: De la Metodología, tratamos sobre la propuesta de los objetivos, las hipótesis, tanto general, como específicas, las variables de estudio y su operacionalización, el tipo, el método y el diseño de investigación al que corresponde el estudio.

El Capítulo IV asignado con el nombre de Técnicas, Instrumentos y Resultados de la Investigación está destinado a explicar las técnicas que se han empleado en el estudio de investigación, así como los instrumentos aplicados para la recolección de datos, el tratamiento estadístico y la discusión de los resultados.

Finalmente en el Capítulo V se consigna las conclusiones a las que se ha arribado como resultado de todo el proceso de investigación, así como las recomendaciones pertinentes para el tratamiento de la problemática explicada y detallada en la presente tesis.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

A lo largo de los años, la tecnología avanzó mucho y alcanzó una gran evolución, junto con eso, los riesgos asociados a la tecnología están avanzando, y hoy, para muchas empresas en Perú, ya sean públicas o privadas, la seguridad de las computadoras es un problema que ellos tienen en común, porque muy pocas de esas empresas proponen medidas de seguridad para salvaguardar la información.

La mayoría de las veces, esta información se almacena en diversos medios físicos y electrónicos, lo cual es motivo de preocupación y trata de mejorar la seguridad de la información, ya que uno de los mayores problemas en la unidad de información y estadísticas del hospital en la región de Huacho es que el acceso no autorizado a la información se vuelve más fácil. Debido a la cantidad de métodos nuevos y existentes para obtener información, ha hecho más difícil proteger la información y sus métodos de transmisión si estas comunicaciones son verbales, archivos, documentos, bases de datos, etc.

Por todo lo expuesto, creo que existe la necesidad de conocer y explicar de manera objetiva y real si existe relación entre las variables auditoria en seguridad informática y gestión de riesgos.

1.2 Formulación del problema

1.2.1 Problema general

¿En qué medida la auditoria en seguridad informática se relaciona con la Gestión de Riesgo en el Hospital Regional Huacho, 2018?

1.2.2 Problemas específicos

a) ¿Qué relación existe entre la auditoria en seguridad lógica y la gestión de riesgo en el Hospital Regional de Huacho?

b) ¿Cómo la auditoria en Seguridad de aplicaciones se relaciona con la gestión de riesgo en el Hospital Regional de Huacho?

c) ¿Qué relación existe entre la auditoria en administración del centro de procesamiento y la gestión de riesgo en el Hospital Regional de Huacho?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Analizar la auditoria en seguridad informática para determinar su relación con la gestión de riesgo en el Hospital Regional de Huacho, 2018.

1.3.2 Objetivos específicos

a) Determinar la relación que existe entre la auditoria en seguridad lógica y la gestión de riesgo en el Hospital Regional de Huacho.

b) Conocer la relación que existe entre la auditoria en Seguridad de aplicaciones se relaciona con la gestión de riesgo en el Hospital Regional de Huacho.

c) Determinar la relación que existe en la auditoria en administración del centro de procesamiento y la gestión de riesgo en el Hospital regional de Huacho.

1.4 Justificación de la investigación

En la actualidad el ingreso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más complicado proteger la información y sus métodos de transmisión, la presente investigación se justifica en la necesidad que tienen las organizaciones sean grandes o pequeñas de asegurar su información frente al uso masivo de tecnología, paralelamente aumentan los ataques informáticos (hacker, troyanos, spyware, etc.), empleados que pueden perder valiosa información, todo esto conllevaría en el peor de los casos la interrupción de la continuidad del negocio provocando pérdidas económicas considerables.

1.5 Delimitaciones del estudio

1.5.1 Delimitación espacial

El presente trabajo de investigación se llevó a cabo en el área de Estadística e Informática del Hospital Regional, ubicada en el distrito de Huacho, provincia de Huaura, región Lima.

1.5.2 Delimitación Temporal

El análisis de la investigación se efectuó en el año 2018.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Investigaciones internacionales

a. Viteri, M (2014), en su trabajo de investigación titulado "*Políticas de seguridad informática en el Departamento de tecnologías de la Información y Comunicación en beneficio de la Universidad Técnica Estatal de Quevedo Manual de Procedimientos*" realizada en la ciudad de Chiclayo Perú. Presentado a la Universidad Técnica Estatal de Quevedo Ecuador, para obtener el título de ingeniería de sistemas, obtuvo la siguiente conclusión:

   1. Con la conclusión preliminar, se realizó un análisis de los riesgos informáticos a través de una encuesta a todo el personal de la Unidad de TIC para evaluar los activos, adaptando así la política a la realidad de la institución. Se pudo concluir que las conexiones a Internet deben tener elementos de prevención, gestión de intrusos, filtrado de virus, gestión de filtros que afectan la integridad del sistema e información institucional.

b. Álvarez, B. (2005). En su trabajo de investigación titulado: "*Seguridad en Informática (Auditoria de Sistemas)*" Para obtener el grado de Maestro en Ingeniería de Sistemas Empresariales, Universidad Iberoamericana, llego a las siguientes conclusiones:

   1. La sociedad de la información y las nuevas tecnologías de la comunicación constituyen la necesidad de mantener la usabilidad y confidencialidad de los sistemas de información en las organizaciones; Por lo tanto, es especialmente importante elegir e implementar sistemas y métodos con la seguridad más adecuada para proteger las redes y los sistemas contra cualquier amenaza, ya sea presente o futura.

2. Los servicios de auditoría incluyen estudios de sistemas de gestión de vulnerabilidades que pueden estar presentes en los sistemas. Cuando se documentan las desviaciones locales, se informan los resultados de estas medidas responsables y proactivas para hacer cumplir el cumplimiento siempre después de un proceso secuencial que mejora sus sistemas de seguridad de errores pasados.

3. Las auditorías de sistemas brindan información al momento de su implementación, que es la situación exacta de los activos de información, sobre protección, control y medidas de seguridad.

4 Realizar el trabajo de auditoría con cierta periodicidad es necesario para garantizar que la seguridad de la red corporativa sea óptima. El cambio continuo de configuraciones, la apariencia de los parches y las mejoras de software, y la adquisición de nuevo hardware, hacen necesario que los sistemas sean revisados regularmente por una auditoría.

5. Una auditoría de sistemas es una radiografía completa de su situación. Compruebe que está preparado para interconectar. Auditoría de sus sistemas.

c. Reyes, M. (2011). En su trabajo de investigación titulado: "*Propuestas para impulsar la seguridad informática en materia de educación*" Para optar por el título de Ingeniero en Computación, Universidad Nacional Autónoma de México, llego a la siguiente conclusión:

1.- Actualmente, la información está desempeñando un papel importante en los negocios, por lo que es necesario tener un sistema de seguridad de acuerdo con las necesidades tanto de las empresas como de los usuarios privados, ya que el primero es el punto débil para los piratas informáticos. solo manejando información sensible.

d. Tola, D. (2012). En su trabajo de investigación titulado: "*Implementación De Un Sistema De Gestión De Seguridad De La Información Para Una Empresa De Consultoría Y Auditoría, Aplicando La Norma ISO/IEC 27001*" Para optar el título de Licenciado En Sistemas De Información,

Escuela Superior Politécnica Del Litoral, llego a las siguientes conclusiones

1. Como las organizaciones en la optimización de recursos son cruciales, el alcance del sistema de administración de seguridad de la información se convierte en una actividad muy importante, ya que limita el alcance de la acción y el uso de los recursos

2. Es importante determinar los objetivos y principios del sistema de gestión de seguridad de la información, ya que definen la forma en que la organización desea ir para preservar la privacidad, accesibilidad y accesibilidad de la información y, por lo tanto, la participación de la administración.

2.1.2 Investigaciones nacionales

a. Huamán, F (2014), en su trabajo de investigación titulado "*Diseño de procedimientos de auditoria de cumplimento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implementación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano*" Tesis previa para obtención del título de ingeniero Informático, Pontifica Universidad Católica del Perú, obtuvo la siguiente conclusión:

   1. Este trabajo de investigación será la base para establecer los procedimientos de auditoria que deben ejecutarse.

b. Villena, M. (2014). En su trabajo de investigación titulado: "*Sistema De Gestión De Seguridad De Información Para Una Institución Financiera*" Para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú, llego a las siguientes conclusiones:

   1. Como se indica en esta tesis, para poder realizar una gestión adecuada de la seguridad de la información en una institución financiera, el primer paso es obtener el apoyo y la asistencia de la alta gerencia, lo que los convierte en participantes activos en lo que significa mantener la información adecuadamente protegida. por la entidad financiera. Al mostrarles la importancia de la protección de la información para los procesos de negocios, se debe esperar su

compromiso continuo por parte de la alta gerencia. Con el apoyo de la línea superior, se ha dado el primer paso importante. Este soporte se debe enviar a los propietarios de los principales procesos comerciales de la institución financiera, que suelen ser la principal responsabilidad.

2. Al informarles sobre la importancia de la seguridad de la información en los procesos que manejan, se espera el apoyo de todo el personal responsable de ellos. Solo en este punto se tratarán todas las pautas para el modelo de gestión expuesto, que se reflejarán en la política de seguridad, normas, estándares y procedimientos, respaldados por la tecnología de la información de la institución. No es necesariamente la tecnología de la información la que garantiza la seguridad de la información. Será importante manejarlo de acuerdo a los objetivos del negocio. No vale la pena obtener los últimos avances técnicos si no es importante proteger la información, que se reflejará en el cumplimiento de todas las políticas de seguridad de la información, siempre actualizada de acuerdo con los cambios constantes en las actividades de una institución financiera.

c. Aroca, J. (2016). En su trabajo de investigación titulado: "*La Auditoria interna y su incidencia en la gestión de empresa De transportes guzmán s.a. de la ciudad de Trujillo*" Para optar por el título de maestro en ciencias económicas, Universidad Nacional de Trujillo, llego a las siguientes conclusiones:

1. La estructura organizativa de la Empresa de Transportes Guzmán S.A. Es uno de los fundadores de la organización de sus actividades operativas, administrativas y de control. La estructura que posee permite la integración y coordinación de todos los miembros de TGSA, lo que la convierte en una compañía más eficiente y eficiente durante los últimos tres (03) períodos.

2. Administración de la Empresa de Transportes Guzmán S.A. Mejoró durante el período 2015 en comparación con el disponible anteriormente debido a que se analizaron sus principales

indicadores: Eficiencia, Eficiencia y Economía, donde los resultados se consideraron adecuados durante el período especificado.

3. La auditoría interna de la empresa de transportes Guzmán S.A. Es óptimo en términos del trabajo de control realizado por el Auditor Interno, que proporciona una garantía razonable a la Junta General Anual con respecto al cumplimiento de las normas, regulaciones y mejores prácticas comerciales en general.

4. El Plan de Operaciones de Auditoría Interna 2015 rige el desempeño de sus funciones y se llevó a cabo de acuerdo con las directrices estratégicas de la Compañía de Transporte de Guzmán SA, lo que dio como resultado observaciones y recomendaciones implementadas a tiempo por la Dirección General con el apoyo de toda la compañía.

5. Empresa de transporte Guzmán S.A. Muestra ganancias positivas en términos de rentabilidad durante el período de 2015, lo que se traduce en una mejora significativa en la administración como resultado de la implementación de las recomendaciones del Departamento de Auditoría Interna durante ese período.

d. Sandoval, V. (2013). En su trabajo de investigación titulado: "*La auditoría financiera y su influencia en la Gestión de las medianas empresas Industriales del distrito de ate – lima"* Para optar el grado académico de maestro en contabilidad y finanzas con mención en gestión tributaria, empresarial y fisca, Universidad San Martin de Porres, llego a las siguientes conclusiones

1. En conclusión, se ha establecido que la auditoría financiera no afecta la administración de empresas industriales de tamaño mediano en el distrito de Ate-Lima, fortalece sus controles internos y proporciona características de mayor calidad y consistencia en su información financiera para que pueda exponer la globalización y competir en el mundo.

2.2 Bases teóricas

I.- AUDITORIA EN SEGURIDAD INFORMÁTICA

1.1 Auditoria

1.1.1 Concepto.

La auditoría es proporcionar una verdadera opinión profesional de una persona especializada, si el asunto de prueba (ya sea un sistema, proceso, producto, estructura organizacional, etc.) cumple las condiciones que se prescriben y presentes realidad que intenta reflejar. (Piattini, 2003)

De la misma forma, ISO 19011: 2002 nos dice que es un proceso sistemático, independiente y documentado para obtener evidencia y evaluarla objetivamente para determinar la extensión en la cual los criterios de auditoría (ISO 2002) son proceso cumplido (Piattini, 2003)

1.1.2 Tareas Principales de la Auditoria.

Según Jiménez nos menciona las siguientes tareas Principales de la Auditoria:

- Estudiar y actualizar permanentemente las áreas susceptibles de revisión.
- Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por organismos generalmente aceptados a nivel nacional e internacional.
- Evaluación y verificación de las áreas requeridas por la alta dirección o responsables directos del negocio.
- Elaboración del informe de auditoría (debilidades y recomendaciones).
- Otras recomendadas para el desempeño eficiente de la auditoría.

1.1.3 Clasificación de Auditoria

La Auditoria se clasifica en dos:

- Auditoria Interna.
- Auditoria Externa.

1.1.3.1 Auditoria Interna

"Al analizar diferentes fuentes bibliográficas, descubrimos que especialistas tienen diferentes puntos de vista sobre el asunto, como es el caso de Arens & Loebbecke (2010), la auditoría interna es un proceso cuya responsabilidad es parte de la gestión y gestión de las cooperativas de servicios múltiples y está diseñada para proporcionar una garantía razonable sobre la realización de los objetivos de las entidades cooperativas. (Gago Rios, 2013)

El Instituto de Internidad del Perú (IAIP) (2012), dijo que "la auditoría interna es una garantía independiente, objetiva y actividad de consultoría destinada a agregar valor y mejorar las operaciones de una organización."

De la misma forma, la ISO Según el Instituto de Auditores Internos (2004, p.23) define la Auditoría Interna, acepta internacionalmente en los siguientes términos.

"La auditoría interna es una función independiente y objetiva en la garantía y consulta, diseñada para agregar valor y mejorar las operaciones de una organización. Ayuda a la organización y al cumplimiento de sus objetivos, proporcionando un enfoque sistemático y disciplinado para mejorar la eficiencia en los procesos de gestión de riesgos, control y gobernanza ".

Además, según Kell & Boynton (2011); "La auditoría interna es sistemática, practicada por los auditores de acuerdo con las normas y procedimientos técnicos establecidos, que consiste en obtener y evaluar objetivamente la evidencia de las reclamaciones en los actos o eventos de múltiples servicios de cooperación técnica, cooperativa y de otro tipo, para determinar el nivel de cumplimiento. entre estas reclamaciones, las normas actuales y los criterios establecidos por dichas entidades cooperativas ".

Mientras tanto, Santillana (2005): "La auditoría interna es una actividad que, como su revisión y evaluación integrales de la implementación correcta y eficiente de los sistemas de control interno, tiene como objetivo garantizar la preservación de la integridad del legado de servicios múltiples cooperativos y la eficiencia de la gestión financiera. y propone acciones correctivas de gestión ".

Por otro lado, la Universidad de Buenos Aires (UBA) (2008) 1; A lo largo de los años, el concepto de Auditoría Interna se ha desarrollado como un área de actividad para el Auditor Interno, que ya no se limita a la evaluación de registros y detecta errores y fraudes, sino que ha contribuido a la planificación estratégica de la organización a través del asesoramiento de la administración.

Cashin, Neuwirth y Levy (1985) afirma:

> La auditoría interna es una actividad profesional que involucra la práctica de tecnología especial y la aceptación de la responsabilidad pública. Como profesional, el auditor realiza su tarea aplicando una serie de conocimientos especializados que formarán la parte técnica de su negocio. Sin embargo, en el desempeño del trabajo, el auditor no solo adquiere la responsabilidad de la persona que contrata sus servicios, sino también una cantidad de personas relacionadas directa e indirectamente con el negocio. (p46)

Además, la auditoría interna desempeña un papel muy importante en el gobierno corporativo. Este gobierno está relacionado con la manera en que las empresas modernas son controladas y controladas, con los siguientes objetivos: atraer capital; Garantizar la buena gobernanza y la gestión de las empresas. Proteja los derechos de los inversores. Construir confianza en los mercados financieros.

Elorreaga (2009) afirma que:

> La auditoría interna ha desempeñado un papel importante en la empresa moderna, ya que los requisitos actuales, el desarrollo económico y social y la introducción de nuevas prácticas de gestión y gestión han llevado a la gerencia a encontrar un elemento objetivo que les brinda información. Análisis, evaluaciones y recomendaciones. (p90)

Actualmente, se requiere que el alcance de las funciones de la Auditoría Interna para un claro sentido de complementar y apoyar el trabajo de dirección, cada vez que contribuye a la consecución de los objetivos y metas establecidos en la organización.

1.1.3.2 Auditoria Externo

La principal característica de este tipo de auditoría es que la llevan a cabo auditores fuera de la empresa, al menos en el campo de trabajo y trabajo, y le permite al auditor externo utilizar su libre albedrío en la aplicación de los métodos, técnicas y herramientas de Revisión con los que lo hará. Evaluar el negocio y las operaciones de la empresa como auditorías y, por lo tanto, la publicación de los resultados será completamente independiente. (Ogaldez Muñoz, 2011)

En general, estas auditorías externas son realizadas por grandes compañías y firmas de auditoría independientes, que casi siempre tienen una gran popularidad y prestigio en el entorno profesional. Los mercados en los que tienen mayor demanda y aplicación son las auditorías de las áreas contable, fiscal y financiera de las instituciones, así como las actividades específicas que requieren una auditoría externa a la empresa cuando existen condiciones especiales que deben evaluarse. (Ogaldez Muñoz, 2011)

1.1.4 Auditoria de Seguridad Informática

En el marco de la auditoría en tecnología de la información se pretende la verificación y garantía de que las políticas y procedimientos establecidos para la gestión y uso adecuado de la tecnología de la información en la organización son llevados de manera oportuna y eficiente. **(**Piattini, 2003, p.2)

La auditoría por computadora es un proceso necesario que debe ser realizado por personal especializado para garantizar que todos los recursos tecnológicos operen en un ambiente de seguridad y control eficientes para que la entidad esté segura de que opera de manera verdadera, completa, precisa y confiable, Además, la auditoría debe contener observaciones y recomendaciones para la mejora continua de la tecnología de la información en la institución. **(**Piattini, 2003, p.3)

Se desarrolla de acuerdo con las normas, procedimientos y técnicas definidos por institutos establecidos a nivel nacional e internacional; Por lo tanto, nada más indicará algunos aspectos básicos para su comprensión.

Así, la auditoría de la computadora es:

- Proceso para recopilar, agrupar y evaluar evidencia para determinar si un sistema de información protege las operaciones comerciales, mantiene la integridad de los datos, realiza la efectividad de la organización y utiliza los recursos de manera efectiva.
- El conjunto de acciones realizadas por auditores capacitados y personal de TI para garantizar continuamente que los recursos informáticos funcionen en un entorno seguro y efectivo de control para proporcionar a la gerencia o al nivel ejecutivo una garantía de que la información se maneja y circula en el área. con los conceptos básicos de integridad, integridad, precisión, fiabilidad, etc.

1.1.5 Sistemas de control

1.1.5.1 Control interno

El control interno incluye las medidas para la verificación previa, simultánea y posterior realizada por la empresa controlada, con el objetivo de gestionar los recursos, activos y operaciones de manera correcta y eficiente. Su ejercicio es previo, simultáneo y posterior. El control interno previo y simultáneo es responsabilidad exclusiva de las autoridades, funcionarios y funcionarios públicos de las entidades, que son responsables de las funciones inherentes a ellas, basadas en las normas que rigen las operaciones de la organización y en los procedimientos establecidos en sus planes, reglamentos y manuales. y disposiciones institucionales, que contienen políticas y métodos de aprobación, registro, verificación, evaluación, seguridad y protección. El control interno subsiguiente es ejercido por los gerentes o CEOs en base al cumplimiento de las reglas establecidas y por el organismo de control institucional de acuerdo con sus planes y programas anuales, evaluación y verificación de los aspectos administrativos del uso del sistema. Recursos y activos estatales, así como la implementación de la implementación y la implementación en relación con los objetivos establecidos y los resultados obtenidos.

1.1.5.2 Control externo

Control externo Principalmente incluye control financiero, control de eficiencia y control legal. El control externo de las empresas públicas es ejercido por el sector central de la administración pública por la secretaría responsable de la coordinación del sector. la unidad de control externa es realizada por la Institución Suprema de Auditoría de la Federación antes de la contabilidad oficial del Tesoro de la legislatura, su personaje es auditor eminentemente para finalizar responsabilidades según el caso, en los términos de la ley.

1.1.6 Evaluación de riesgos

La evaluación de riesgos en una empresa considera que todos los riesgos relevantes que pueden afectar el rendimiento y la operación. El auditor estará más interesado en la evaluación de riesgos de la Entidad relacionada con la información financiera. Los riesgos relevantes para la información financiera incluyen eventos o circunstancias externas e internas que pueden surgir y afectar la capacidad de la compañía en el registro, procesamiento o informe de información grupal.

1.1.7 Seguridad de la Información

La Organización Internacional de Normalización (ISO) define la seguridad de la información (SI) como: conservación de la privacidad, integridad y accesibilidad de la información; así como los sistemas involucrados en el tratamiento, dentro de una organización. Además, también pueden estar involucradas otras características, tales como: autenticidad, responsabilidad, no repudio y confiabilidad.

Esto significa que estas tres condiciones forman la base de la seguridad de la información, a partir de la cual se resume la explicación a continuación:

Privacidad. La información no está disponible o divulgada a personas, dispositivos o procesos no autorizados.

Integridad. Mantenga la exactitud y la integridad de la información y sus métodos de proceso. Para garantizar la integridad de la

información, el remitente siempre debe estar autenticado. Esto puede verse afectado por hardware, software, virus o personas malintencionadas.

Disponibilidad. Acceso y uso de los sistemas de información y procesamiento por personas autorizadas, entidades o procesos según sea necesario. (López, 2019, p.15)

1.1.8 Amenazas y vulnerabilidades

1.1.8.1 Amenazas

Según la norma ISO 27000, una causa potencial de un incidente no deseado se considera una amenaza, lo que podría provocar daños en un sistema u organización. Alexander y otros (2007) están de acuerdo en que las amenazas pueden clasificarse en grandes grupos para facilitar decisiones genéricas que reduzcan los grupos de riesgo en una sola medida. López (2011) afirma que los grupos propuestos son:

- Naturales. Fuego, inundación, terremotos, etcétera.
- Humanas Accidentales. Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- Humanas Intencionales. Robo de información, ataques.
- Tecnológicas. Virus, hacker, crackers, pérdida de datos, fallas de software, hardware o de red. (p. 16)

1.1.8.2 Vulnerabilidades

Las vulnerabilidades están asociadas con debilidades en los activos de información. La vulnerabilidad asociada con los sistemas de información se considera una ausencia o debilidad en los controles que ayudan a mitigar un riesgo, aumentar el nivel de potencia y el factor de exposición. López (2011) afirma:

> La vulnerabilidad y las vulnerabilidades están interrelacionadas, formando parte del problema de las vulnerabilidades explotadas por las amenazas, ya que una vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto a cualquier sistema de información. Esto es lo que los expertos en temas de seguridad de la

información se denominan la relación de efecto causal entre los elementos en el análisis de riesgo. En consecuencia, el próximo paso será integrar estos elementos para analizar y definir los niveles de riesgo, que luego permitirán implementar procedimientos que ayuden a mitigar dichos riesgos y eliminar las vulnerabilidades. (p.17)

II.- GESTIÓN DE RIESGO

2.1 Definición

Es un proceso que genera un equilibrio entre lo que la empresa "quiere ganar" ante lo que "está dispuesta a sufrir".

Es una herramienta para la seguridad de la información porque indica la amenaza de integridad, disponibilidad y confidencialidad de la información crítica sobre la organización, y también administra y supervisa el cumplimiento de los requisitos reglamentarios a medida que se expone y afecta directamente a su continuidad (que se encuentra en básicamente el objetivo de toda la información de la estrategia de seguridad).

Para alcanzar el éxito de la gestión de riesgos es vital para considerar tanto la cultura y la estructura organizativa, los objetivos de la misión y de negocios se han elaborado, la definición de procesos organizacionales y el conocimiento de estructuras de buenas prácticas generalmente aceptadas.

En el escenario que una amenaza materializa, la gestión de riesgos va a asegurar que el impacto se tome internamente (en la organización) será manejable, es decir, para ser encuadrado dentro de los límites de costos aceptables sin interrumpir la continuidad de los negocios.

La Gestión de Riesgos también es tener un autoconocimiento considerable, es decir, la necesidad de conocer las propias amenazas y vulnerabilidades. En consecuencia, la Administración implicará el conocimiento de la naturaleza de los riesgos con el fin de cuantificar el impacto sobre los negocios. De esta forma, los riesgos pueden ser manejados de forma eficiente. Este es un paso crucial y preliminar para la determinación de la estrategia y los planes de seguridad.

Debemos tener en cuenta que la gestión de riesgos debe llevar tan vinculado en sí, un mensaje para transmitir el equilibrio entre el costo que sería necesario para

implementar controles y contramedidas y exposiciones al riesgo que la organización tiene.

Para muchas organizaciones, las informaciones y tecnologías que la soportan representan los activos más valiosos de la empresa.

Por supuesto, estos sistemas deben protegerse. Sin embargo, los recursos para garantizar que estos sistemas sean finitos y es necesario establecer un mecanismo que nos permita ser eficientes en este proceso. Es decir, es necesario determinar objetivamente cuáles son los recursos de TI que presentan un riesgo mayor para la organización y, a partir de eso, tomar acciones que permitan gestionar ese riesgo.

En la actualidad, el Campus Estado de México tiene cerca de 55 servidores que sirven diferentes servicios, entre los que se incluyen: comunicación, firewalls, nombres de dominio, información, tales como bases de datos, servicios de directorio, servicios de Internet / Intranet , como FTP, correo electrónico, web, colaboración, etc., laboratorios y software especializado de la academia, desarrollado en el hogar y aplicaciones proveedores externos, servidores para el desarrollo de sistemas de uso, soluciones de copia de seguridad, etc. Implementado en diferentes plataformas, tecnologías y sistemas operativos, destacándose como la principal plataforma de Intel, aunque todavía existen servidores con procesadores PowerPC y sistemas operativos, destacan principalmente servidores Linux y Windows. (Guerra Farias, 2006)

La administración de estos equipos es complicada y costosa debido a la cantidad y la gama de servicios que se centrarán en la protección, disponibilidad y seguridad de los mismos.

Como parte de la definición de gestión de TI realizada por el IT Governance Institute [2], es importante destacar dos puntos importantes: "El valor que implica para la empresa y reducir los riesgos de TI. El primer punto es la adaptación estratégica enfocada de "TI con el negocio. Y el otro se enfoca en la implementación de la responsabilidad en la empresa. En ambos casos, el apoyo a los recursos suficientes se mide para garantizar los resultados deseados".

Esto confirma la necesidad de que Campus tenga un modelo o sistema que identifique de manera objetiva el orden en el que deben estar protegidos y

priorice los recursos informáticos en función de la definición de factores y variables que ayuden a determinar y medir el nivel de riesgo de los activos de TI en el campus. (Guerra Farias, 2006)

2.2 Fases de la Gestión de Riesgos:

a) Determinar contexto de aplicación.
b) Identificar los riesgos.
c) Analizar y clasificar los riesgos.
d) Tratar los riesgos (implementar controles).
e) Aceptar riesgos residuales.
f) Monitorear y revisar los riesgos.
g) Comunicar a los actores involucrados.

La importancia de la gestión de riesgos está en transformar la seguridad de la información en un facilitador de negocios, en una entidad que agrega valor a ella. Permite dirigir acciones que impidan de manera razonable las amenazas de seguridad a las que la empresa está expuesta; es decir, hasta cierto punto, dirige los planes de seguridad.

2.3 Políticas de Seguridad

2.3.1 Políticas de integridad

Se propone que la compañía se adhiera a las siguientes pautas para mantener la integridad de su información:

- El acceso al sistema debe hacerse con nombre de usuario y contraseña.
- El nombre de usuario y la contraseña se proporcionarán a la llegada a la empresa.
- En el caso de la terminación del empleo, debe ser notificado por escrito, especificar el motivo y ser firmado por la persona responsable y el jefe del Departamento de Recursos Humanos. El cambio cambia el estado de la información de acceso a deshabilitado. Una vez deshabilitado, esta información no se puede cambiar a ningún otro estado.

- Cuando intenta ingresar al sistema, solo puede escribir la contraseña hasta cinco veces. Cuando se complete el límite, el usuario bloqueará.
- El bloqueo de un usuario solo se puede desactivar mediante un mensaje escrito que indique la causa del bloqueo firmado por la persona responsable y el jefe del departamento designado. Este documento debe ser entregado a la persona a cargo del área del sistema.
- La información de acceso es totalmente responsable del empleado al que fue asignada y no debe ser divulgada a ningún tercero.
- La información de acceso se considera secreta y poco práctica.

2.3.2Políticas de disponibilidad

Las políticas de disponibilidad detallan las especificaciones para mantener la información correcta para quienes la puedan consultar:

- La entrada o modificación de la información del sistema será un proceso en línea.
- La información de los clientes es considerada de carácter privado.
- En caso de modificación de la información del sistema, el registro o los registros utilizados se bloquearán para evitar errores en el cambio de datos.

2.4 Aplicaciones Varias

2.4.1. Gestión de Riesgos Financieros

La gestión de riesgos financieros es una rama especializada de finanzas corporativas, que se dedica a la gestión o cobertura de riesgos financieros. Por esta razón, un gerente de riesgo financiero es responsable de asesorar y administrar la exposición a riesgos corporativos o corporativos mediante el uso de instrumentos financieros derivados.

En cuanto a la suma de dinero que una organización pública o privada debe en relación a su tamaño, y cuanto mayor la tasa de interés que debe pagar por ella, mayor es la probabilidad de que la suma de intereses y amortización del principal se convierta en problema para la la empresa y más probablemente el valor de mercado de sus inversiones (el valor de mercado de la empresa) flotará.

2.4.2. Gestión de Riesgos Económicos

El riesgo económico es una consecuencia directa de las decisiones de inversión. Por lo tanto, la estructura de los activos de la empresa es responsable del nivel y la movilidad del beneficio operativo. Este es un tipo de riesgo particular o no sistemático, ya que se aplica solo a cualquier inversión, o compañía, en particular. Debido a que es único, la exposición varía según la inversión o la compañía en la que se invierte, lo que afectará la política de elección específica de cada inversionista individual. Tenga en cuenta que este tipo de riesgo puede causar grandes pérdidas en un corto período de tiempo. Por ejemplo, la aparición del mercado de un producto más avanzado y más barato que la primavera puede reducir significativamente las ventas de nuestros productos, causando grandes pérdidas en la empresa. Además, si hay una recesión económica, las ganancias corporativas también reducen sus impuestos, lo que significa que las autoridades centrales, autónomas y locales ven que su capacidad económica se reduce para servir a la sociedad. Así, el riesgo financiero afecta indirectamente a las instituciones estatales.

2.3 Definición de términos básicos

Auditoria. - Inspección o verificación de la contabilidad de una empresa.

Ataque. - Cualquier acción que explote una vulnerabilidad.

Amenaza. - Cualquier circunstancia con potencial suficiente para causar pérdida o daño al sistema.

Código malicioso. - Software diseñado para acciones maliciosas e incluye programas como virus, gusanos, troyanos y spyware.

Integridad. – Protección de la totalidad y la precisión de la información que se está manejando.

Riesgo. –Es la probabilidad de que se produzca un daño o contratiempo.

Seguridad. - Es la ausencia del peligro.

Virus. - Son un tipo más del conjunto de software denominado como “malware” los virus en sí son programas informáticos cuyos objetivos son la reproducción y el provocar algún tipo de daño en el sistema informático.

Vulnerabilidad. - Debilidad en un activo que lo hace susceptible de ser atacado.

2.4 Hipótesis de investigación

2.4.1 Hipótesis general

Existe relación directa entre Auditoria en seguridad informática y la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

2.4.2 Hipótesis específicas

a) Existe relación directa entre la auditoria en seguridad lógica y la gestión de riesgo en el Hospital regional de Huacho.

b) La auditoría en seguridad de aplicaciones tiene relación directa con la gestión de riesgo en el Hospital regional de Huacho.

c) Existe relación directa entre la auditoria en administración del centro de procesamiento y la gestión de riesgo en el Hospital Regional de Huacho.

2.5 Operacionalización de las variables

VARIABLES	DIMENSION	INDICADORES	ITEMS
Vi : V1 **AUDITORIA EN SEGURIDAD INFORMÁTICA**	Seguridad Lógica	✓ Identificación de usuarios. ✓ Passwords. ✓ Segregación de funciones.	1. ¿En el hospital regional de huacho existe la identificación de usuarios?. 2. ¿En el hospital regional de huacho se utilizan los password para el acceso de los usuarios? 3. ¿En el hospital regional de huacho se utiliza la segregación de funciones para darle responsabilidades a los usuarios.?
	Seguridad de las aplicaciones	✓ Software. ✓ Seguridad de bases de datos. ✓ Control de aplicaciones en PC'S. ✓ Control de datos en las aplicaciones.	1. ¿Los softwares que se utilizan en el hospital regional de huacho son seguros y confiables.? 2. ¿La base de datos del hospital regional de huacho está totalmente segura.? 3. ¿Las aplicaciones instaladas en las PC's del Hospital regional de Huacho están totalmente controladas.? 4. ¿Los datos de las aplicaciones instaladas

		✓ Antivirus. ✓ Firewall. ✓ Ataques de red.	en las PC's del Hospital regional de Huacho están salvaguardados.? 5. ¿Las PC's del hospital regional de huacho tienen antivirus que están en constante actualización.? 6. ¿Los firewalls de las PC's del hospital regional de Huacho están siempre activados.? 7. ¿Las aplicaciones del Hospital regional de huacho están siempre protegidas a ataques de red.?
	Administración del Centro de Procesamiento	✓ Administración del CPD. ✓ Capacitación de usuarios. ✓ Backup. ✓ Tratamiento de la documentación.	1. ¿EL CPD(centro de procesamiento de datos) del Hospital regional de Huacho está correctamente administrado.? 2. ¿Los usuarios del CPD(centro de procesamiento de datos) del Hospital regional de Huacho están en constante capacitación.? 3. ¿Los backups del CPD(centro de procesamiento de datos) del hospital regional de Huacho están totalmente protegidos.? 4. ¿El tratamiento de la documentación del CPD(centro de procesamiento de datos) del hospital regional de huacho es el más adecuado.?
Vd : V2 **GESTIÓN DE RIESGO**	Identificación del riesgo	✓ Detección de elementos peligrosos ✓ ¿Qué puede suceder? ✓ ¿Por qué puede suceder?	1. ¿La auditoría en seguridad informática previene la detección de elementos peligrosos en el hospital regional de huacho.? 2. ¿La auditoría en seguridad informática nos ayuda a saber que puede suceder si se detecta un elemento

		✓ ¿Dónde puede suceder? ✓ ¿A quién puede suceder?	peligroso en el hospital regional de huacho.? 3. ¿La auditoría en seguridad informática nos ayuda a saber por qué se ha detectado algún elemento peligroso en el hospital regional de huacho.? 4. ¿La auditoría en seguridad informática nos ayuda a saber dónde se puede detectar un elemento peligroso en el hospital regional de huacho.? 5. ¿La auditoría en seguridad informática nos ayuda a saber a quién le puede suceder si se detecta un elemento peligroso en el hospital regional de huacho.?
	Analizar Riesgos	✓ Se puede eliminar el riesgo ✓ Necesidades para eliminar el riesgo ✓ ¿Qué o quién puede ser dañado?	1. ¿La auditoría en seguridad informática nos ayuda a saber si se puede eliminar el riesgo en el hospital regional de huacho.? 2. ¿La auditoría en seguridad informática nos ayuda a identificar las necesidades para eliminar el riesgo en el hospital regional de huacho.? 3. ¿La auditoría en seguridad informática nos ayuda a saber qué o quién puede ser dañado en el hospital regional de huacho.?
	Evaluar Riesgos	✓ Metodología de evaluación. ✓ Probabilidad. ✓ Consecuencia.	1. ¿La auditoría en seguridad informática nos ayuda a conocer la metodología al evaluar un riesgo en el hospital regional de huacho.? 2. ¿La auditoría en seguridad informática nos ayuda a conocer la probabilidad que pueda suceder un riesgo en el hospital regional de huacho.?

			3. ¿La auditoría en seguridad informática nos ayuda a conocer las consecuencias que puede ocasionar un riesgo en el hospital regional de huacho.?
	Control del Riesgo	✓ Medidas preventivas a aplicar. ✓ Control periódico del riesgo. ✓ Información y consulta.	1. ¿La auditoría en seguridad informática nos ayuda a saber las medidas preventivas a aplicar ante un riesgo en el hospital regional de huacho.? 2. ¿La auditoría en seguridad informática nos ayuda a conocer el control periódico que se debe realizar ante un riesgo en el hospital regional de huacho.? 3. ¿La auditoría en ¿seguridad informática nos ayuda a conocer la información y consulta de un riesgo en el hospital regional de huacho.?

CAPÍTULO III
METODOLOGÍA

3.1 Diseño metodológico

No experimental correlacional.

3.2 Población y muestra

3.2.1 Población

Está constituida por el personal del área de estadística e informática del Hospital regional de Huacho.

Unidad de Estadística e Informática	Personal
Supervisor de programa sectorial	1
Especialista Administrativo	1
Asistente Administrativo	3
Asistente en servicios de salud	1
Técnico en estadística	2
Técnico Administrativo	13
Operador PAD	3
Secretaria	2
Auxiliar de Sistema Administrativo	2
Total	28

3.2.2 Muestra

Según Hernández, expresa que "si la población es menor a cincuenta (50) individuos, la población es igual a la muestra" (p.69), por lo tanto, la muestra seria de 28 personas.

3.3 Técnicas de recolección de datos

Para la recolección de datos se realizará utilizando la técnica de la observación sistemática, y se la empleará para recoger información sobre la variable Auditoria en Seguridad Informática por parte de los empleados que laboran en las oficinas de estadística e informática, así como para medir la gestión de riesgo de información en el hospital regional de huacho.

3.4 Técnicas para el procesamiento de la información

1. Estadísticos de tendencia central
   - Media
   - Mediana
   - Moda
2. Estadísticos de dispersión.
   - Desviación estándar
   - Varianza.
3. Tabla de frecuencias.
4. Razones y proporciones.

CAPÍTULO IV

RESULTADOS

4.1 Análisis de resultados

I.- AUDITORIA EN SEGURIDAD INFORMATICA

1.1 Seguridad Lógica

1.- En el hospital regional de huacho existe la identificación de usuarios

Tabla Nº 01: *Identificación de usuarios*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	6	0,21	21
b	Casi siempre	10	0,36	36
c	A veces	10	0,36	36
d	Casi nunca	2	0,07	7
e	Nunca	0	0,00	0
	total	28	1,00	100

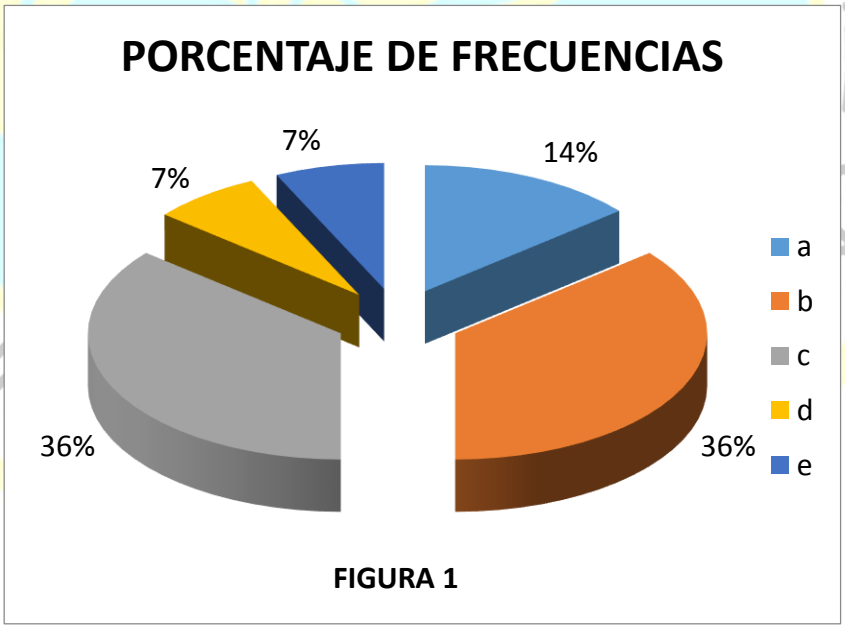

FIGURA 1

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: En el hospital regional de huacho existe la identificación de usuarios, contestaron de la siguiente manera: 10(36%) dijeron a veces; 10(36%) dijeron casi siempre; 6(21%) dijeron siempre; 2(7%) dijo casi nunca y 0(0%) dijo nunca.

2.- En el hospital regional de huacho se utilizan los password para el acceso de los usuarios

Tabla Nº 02: *Acceso de usuarios mediante password*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	9	0,32	32
b	Casi siempre	13	0,46	46
c	A veces	5	0,18	18
d	Casi nunca	1	0,04	4
e	Nunca	0	0,00	0
	total	28	1,00	100

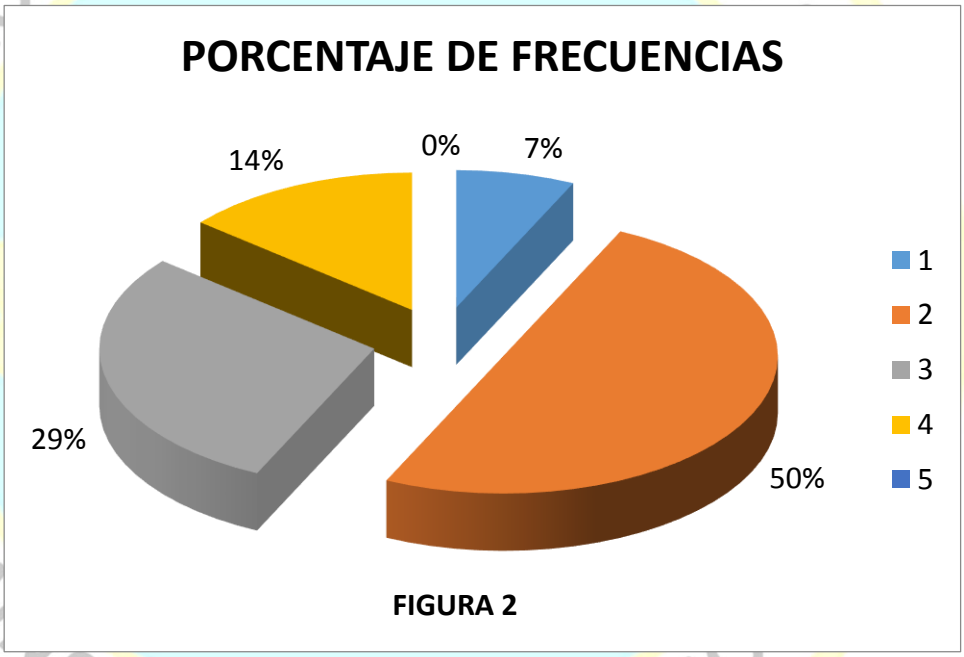

FIGURA 2

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: En el hospital regional de huacho se utilizan los password para el acceso de los usuarios, contestaron de la siguiente manera: 13(46%)dijeron casi siempre; 9(32%) dijeron siempre; 5(18%) dijeron a veces; 1(4%) dijo casi nunca y 0(0%) dijo nunca.

3.- En el hospital regional de huacho se utiliza la segregación de funciones para darle responsabilidades a los usuarios

Tabla Nª 03: *Segregación de funciones*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	8	0,29	29
b	Casi siempre	8	0,29	29
c	A veces	6	0,21	21
d	Casi nunca	6	0,21	21
e	Nunca	0	0,00	0
		28	1,00	100

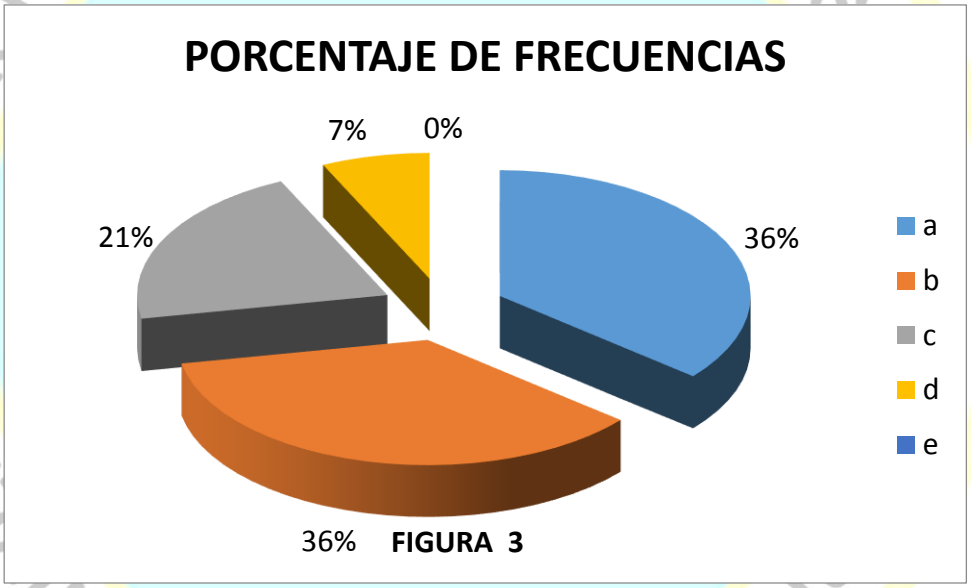

FIGURA 3

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: En el hospital regional de huacho se utiliza la segregación de funciones para darle responsabilidades a los usuarios, contestaron de la siguiente manera: 8(29%) siempre; 8(29%) dijeron casi siempre; 6(21%)dijeron a veces; 6(21%) dijo casi nunca y 0(0%) dijo nunca.

1.2 Seguridad de las aplicaciones

4.-Los softwares que se utilizan en el hospital regional de huacho son seguros y confiables

Tabla Nª 04: *Softwares seguros.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	1	0,04	4
b	Casi siempre	14	0,50	50
c	A veces	13	0,46	46
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
	Total	28	1,00	100

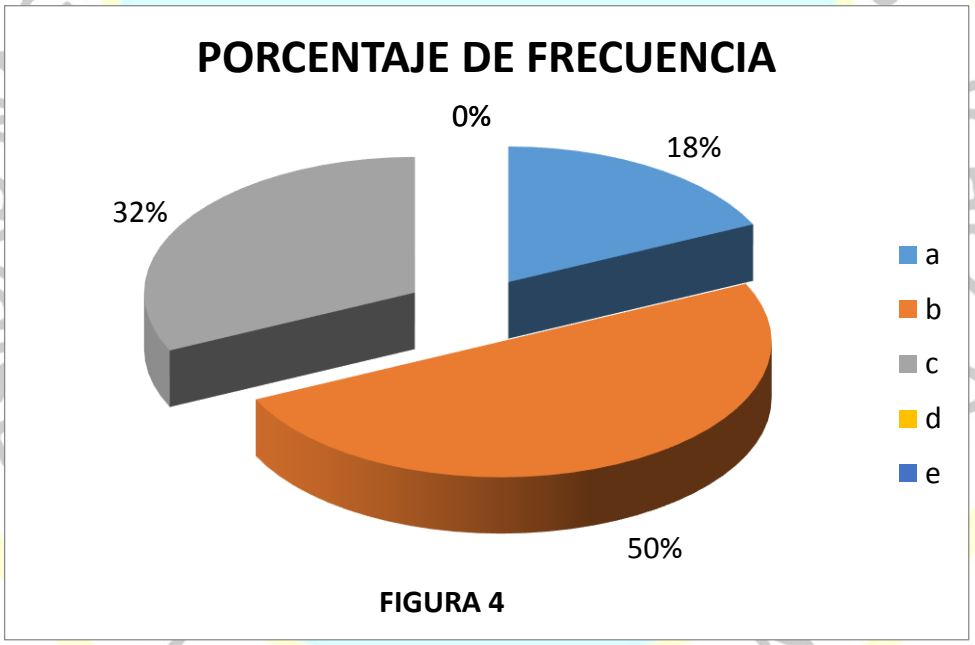

FIGURA 4

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Los softwares que se utilizan en el hospital regional de huacho son seguros y confiables, contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 13(46%) dijeron a veces; 1(4%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

5.- La base de datos del hospital regional de huacho está totalmente segura

Tabla Nª 05: *Seguridad de la Base de datos.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	6	0,21	21
b	Casi siempre	10	0,36	36
c	A veces	9	0,32	32
d	Casi nunca	3	0,11	11
e	Nunca	0	0,00	0
	Total	28	1,00	100

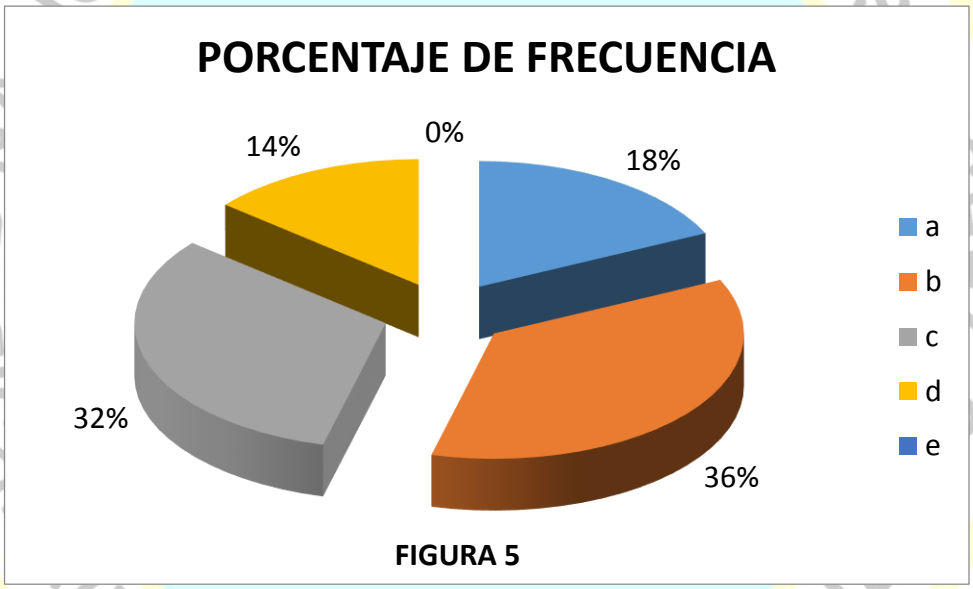

FIGURA 5

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La base de datos del hospital regional de huacho está totalmente segura, contestaron de la siguiente manera: 10(36%)dijeron casi siempre; 9(32%) dijeron a veces; 6(21%) dijeron siempre; 3(11%) dijo casi nunca y 0(0%) dijo nunca.

6. Las aplicaciones instaladas en las PC's del Hospital regional de Huacho están totalmente controladas

Tabla Nª 06: *Control de PC's*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	3	0,11	11
b	Casi siempre	9	0,32	32
c	A veces	13	0,46	46
d	Casi nunca	3	0,11	11
e	Nunca	0	0,00	0
	Total	28	1,00	100

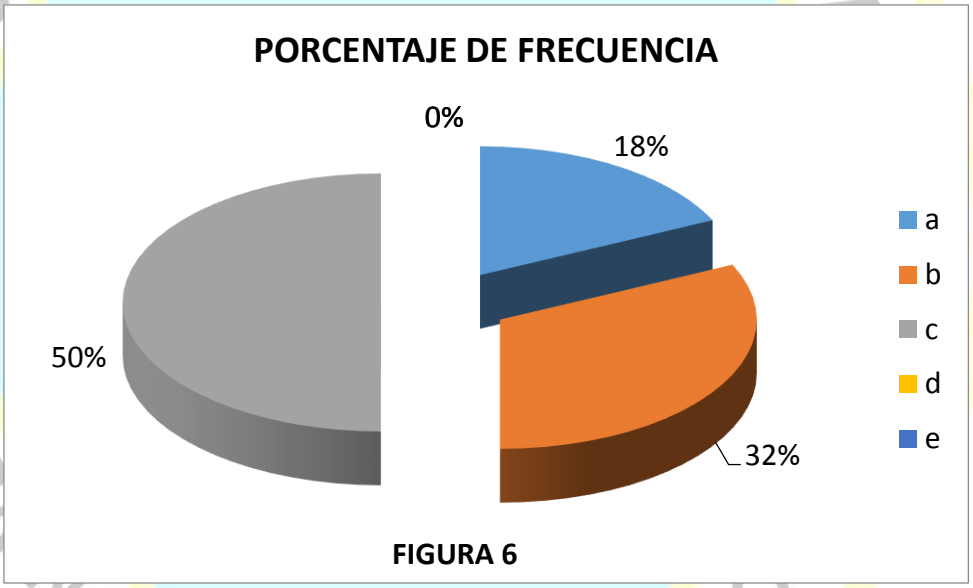

FIGURA 6

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Las aplicaciones instaladas en las PC's del Hospital regional de Huacho están totalmente controladas, contestaron de la siguiente manera: 13(46%)dijeron a veces; 9(32%) dijeron casi siempre; 3(11%) dijeron siempre; 3(11%) dijo casi nunca y 0(0%) dijo nunca.

7. Los datos de las aplicaciones instaladas en las PC’s del Hospital regional de Huacho están salvaguardados

Tabla Nª 07: *Aplicaciones instaladas.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	4	0,14	14
b	Casi siempre	14	0,50	50
c	A veces	10	0,36	36
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
Total		28	1,00	100

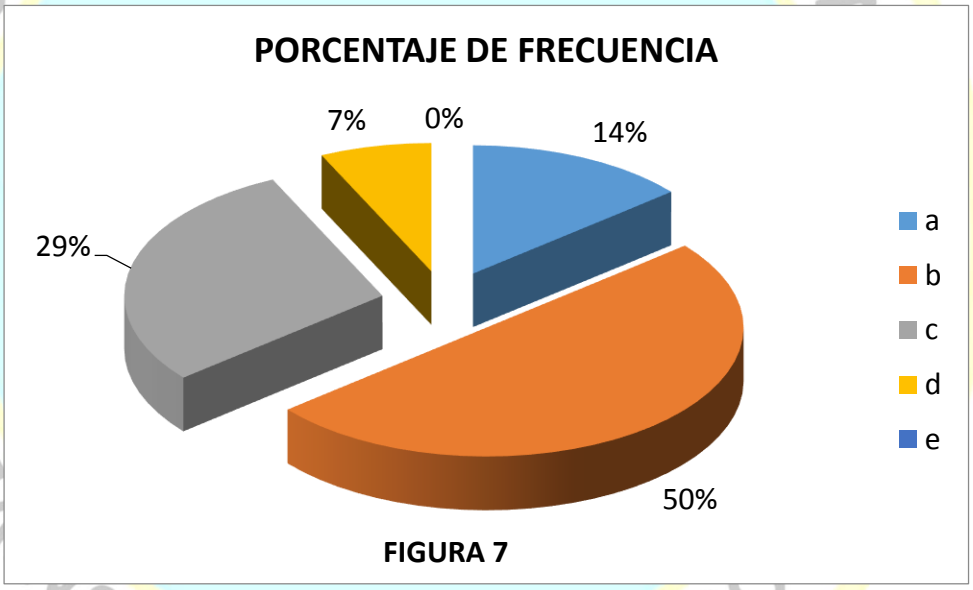

FIGURA 7

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Los datos de las aplicaciones instaladas en las PC’s del Hospital regional de Huacho están salvaguardados; contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 10(36%) dijeron a veces; 4(14%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

8. Las PC’s del hospital regional de huacho tienen antivirus que están en constante actualización.

Tabla Nª 08: *Actualización de antivirus*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	0	0,00	0
b	Casi siempre	10	0,36	36
c	A veces	16	0,57	57
d	Casi nunca	0	0,00	0
e	Nunca	2	0,07	7
Total		28	1,00	100

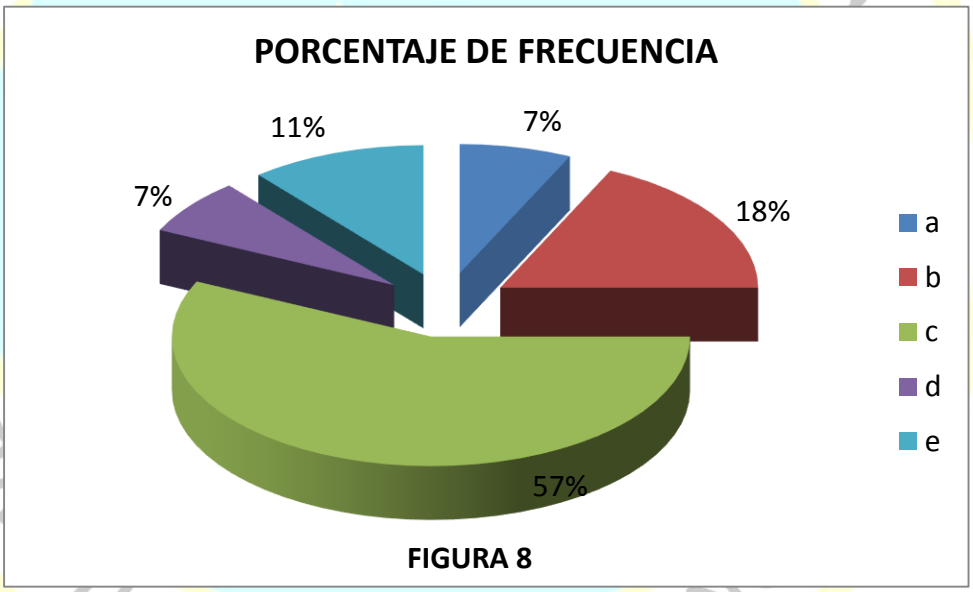

FIGURA 8

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Las PC’s del hospital regional de huacho tienen antivirus que están en constante actualización, contestaron de la siguiente manera: 36(57) dijeron a veces; 10(36%) dijeron casi siempre; 2(7%) dijeron nunca; 0(0%) dijo casi nunca y 0(0%) dijo siempre.

9. El firewall de las PC’s del hospital regional de Huacho están siempre activado

Tabla Nª 09: *Firewall*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	5	0,18	18
b	Casi siempre	12	0,43	43
c	A veces	6	0,21	21
d	Casi nunca	5	0,18	18
e	Nunca	0	0,00	0
Total		28	1,00	100

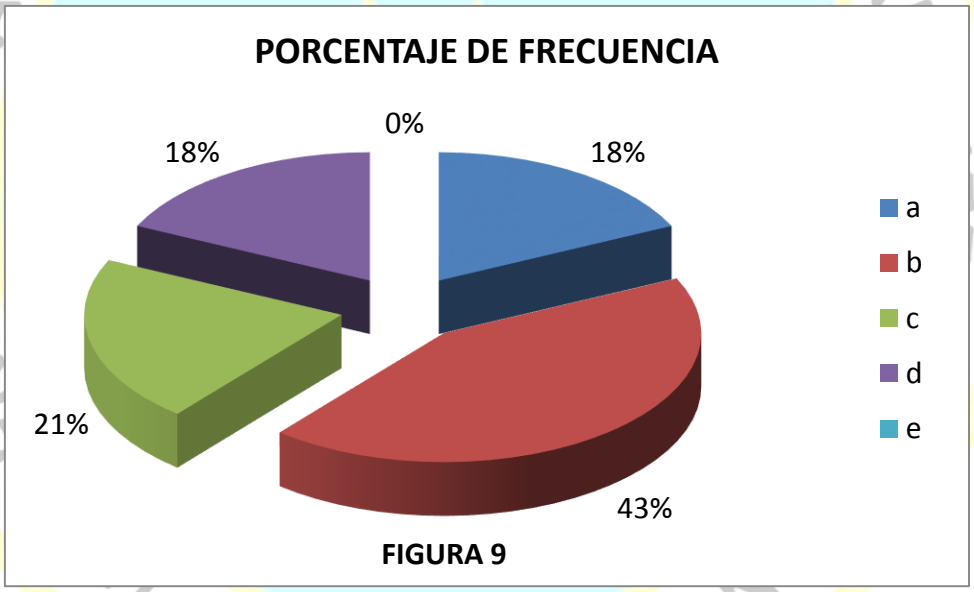

FIGURA 9

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: El firewall de las PC’s del hospital regional de Huacho están siempre activado, contestaron de la siguiente manera: 12(43%)dijeron casi siempre; 6(21%) dijeron casi nunca; 5(18%) dijeron casi nunca; 5(18%) dijo siempre y 0(0%) dijo nunca.

10. Las aplicaciones del Hospital regional de huacho están siempre protegidas a ataques de red.

Tabla Nª 10: *Ataques de red.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	5	0,18	18
b	Casi siempre	15	0,54	54
c	A veces	2	0,07	7
d	Casi nunca	6	0,21	21
e	Nunca	0	0,00	0
	Total	28	1,00	100

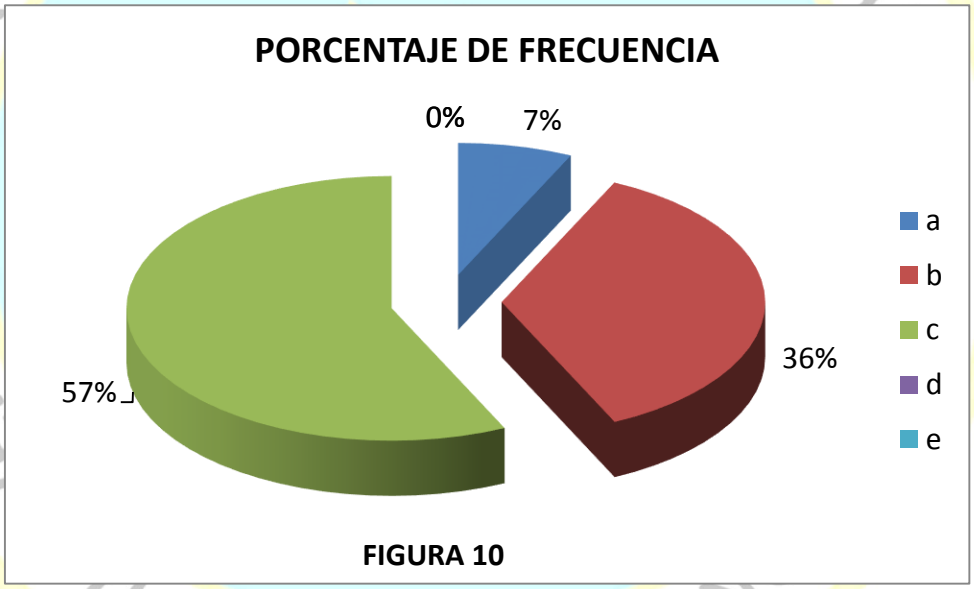

FIGURA 10

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Las aplicaciones del Hospital regional de huacho están siempre protegidas a ataques de red, contestaron de la siguiente manera: 15(54%)dijeron casi siempre; 6(21%) dijeron casi nunca; 5(18%) dijeron siempre; 2(7%) dijo a veces y 0(0%) dijo nunca.

1.3 Administración del centro de procesamiento

11. EL CPD(centro de procesamiento de datos) del Hospital regional de Huacho está correctamente administrado

Tabla Nª 11: *Administración del CPD*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	2	0,07	7
b	Casi siempre	14	0,50	50
c	A veces	12	0,43	43
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
	Total	28	1,00	100

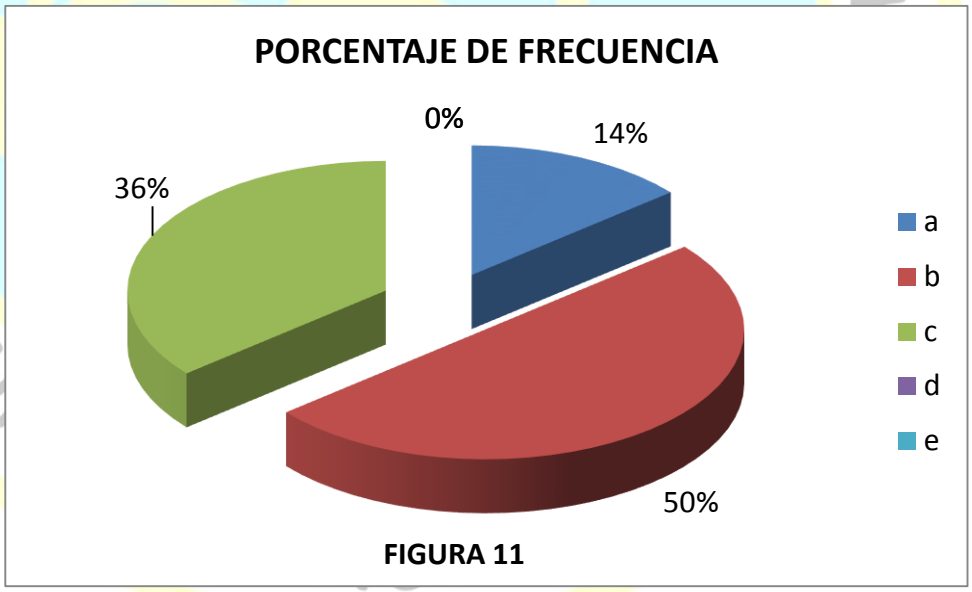

FIGURA 11

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: EL CPD(centro de procesamiento de datos) del Hospital regional de Huacho está correctamente administrado; contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 12(43%) dijeron a veces; 2(7%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

12. Los usuarios del CPD(centro de procesamiento de datos) del Hospital regional de Huacho están en constante capacitación

Tabla Nª 12: *Capacitación de usuarios del CPD*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	1	0,04	4
b	Casi siempre	11	0,39	39
c	A veces	10	0,36	36
d	Casi nunca	6	0,21	21
e	Nunca	0	0,00	0
	Total	28	1,00	100

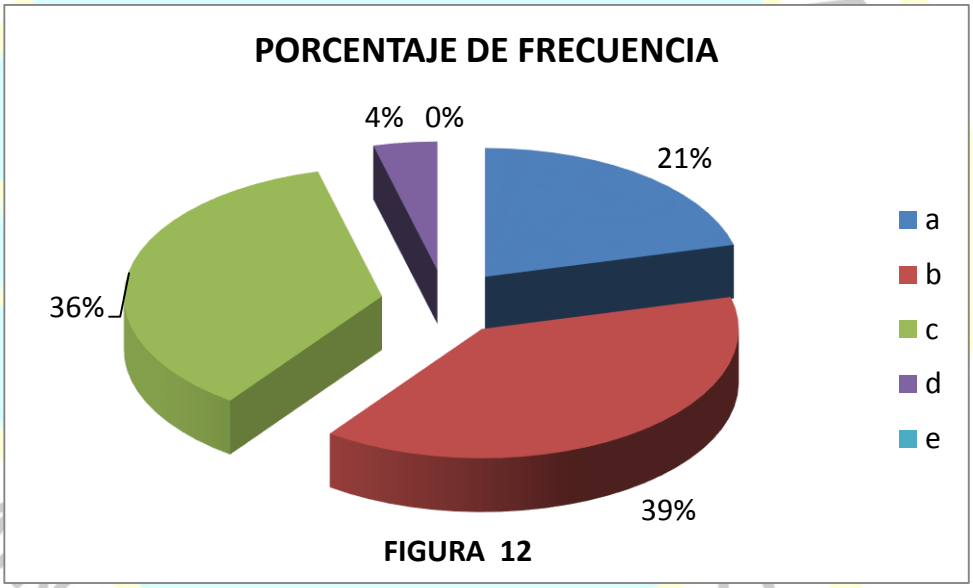

FIGURA 12

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Los usuarios del CPD(centro de procesamiento de datos) del Hospital regional de Huacho están en constante capacitación, contestaron de la siguiente manera: 11(39%)dijeron casi siempre; 10(36%) dijeron a veces; 6(21%) dijeron casi nunca; 1(4%) dijo siempre y 0(0%) dijo nunca.

13. Los backups del CPD(centro de procesamiento de datos) del hospital regional de Huacho están totalmente protegidos

Tabla Nª 13: *Protección de los backups.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	10	0,36	36
b	Casi siempre	10	0,36	36
c	A veces	6	0,21	21
d	Casi nunca	2	0,07	7
e	Nunca	0	0,00	0
	Total	28	1,00	100

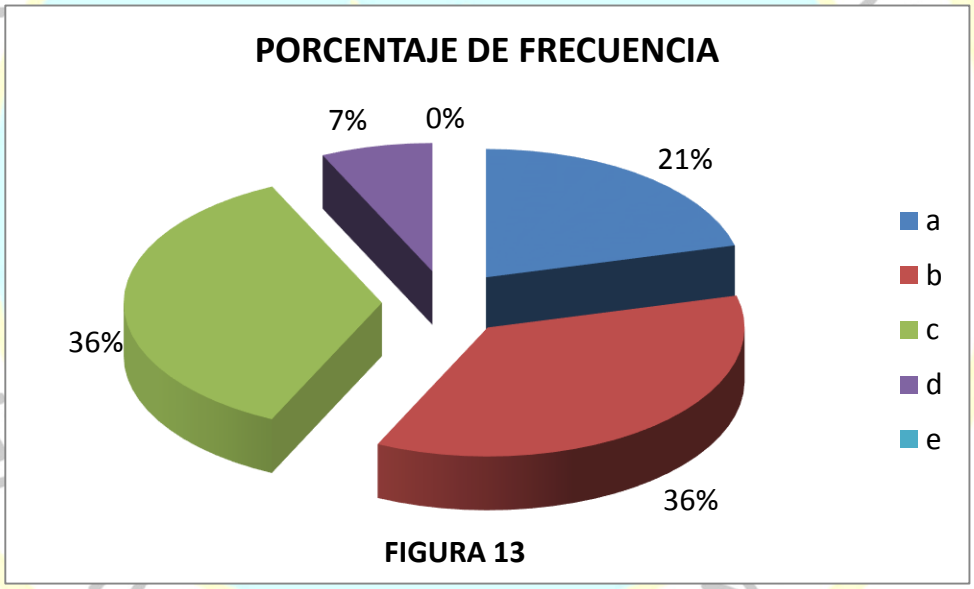

FIGURA 13

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: Los backups del CPD(centro de procesamiento de datos) del hospital regional de Huacho están totalmente protegidos, contestaron de la siguiente manera:10(36%)dijeron siempre; 10(36%) dijeron casi siempre; 6(21%) dijeron a veces; 2(7%) dijo casi nunca y 0(0%) dijo nunca.

14. El tratamiento de la documentación del CPD(centro de procesamiento de datos) del hospital regional de huacho es el más adecuado

Tabla Nª 14: *Tratamiento de la documentación del CPD.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	1	0,04	4
b	Casi siempre	13	0,46	46
c	A veces	8	0,29	29
d	Casi nunca	6	0,21	21
e	Nunca	0	0,00	0
	Total	28	1,00	100

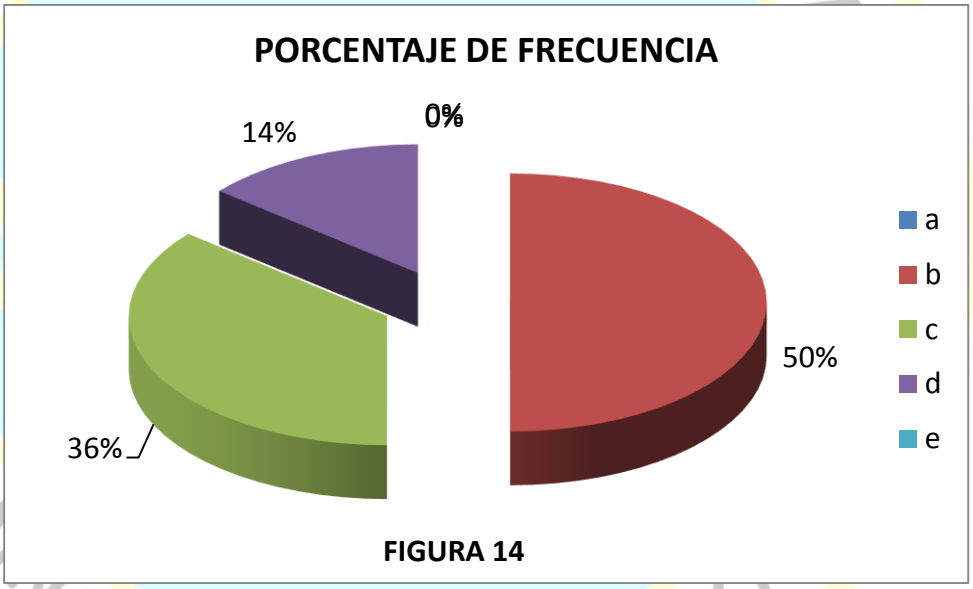

FIGURA 14

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: El tratamiento de la documentación del CPD(centro de procesamiento de datos) del hospital regional de huacho es el más adecuado, contestaron de la siguiente manera: 13(46%)dijeron casi siempre; 8(29%) dijeron a veces; 6(21) dijeron casi nunca; 1(4%) dijo siempre y 0(0%) dijo nunca.

II.- GESTIÓN DE RIESGO

1.1 Identificación del Riesgo

1.- La auditoría en seguridad informática previene la detección de elementos peligrosos en el hospital regional de huacho

Tabla Nª 15: *Detección de elementos peligrosos*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	4	0,14	14
b	Casi siempre	10	0,36	36
c	A veces	10	0,36	36
d	Casi nunca	2	0,07	7
e	Nunca	2	0,07	7
	total	28	1,00	100

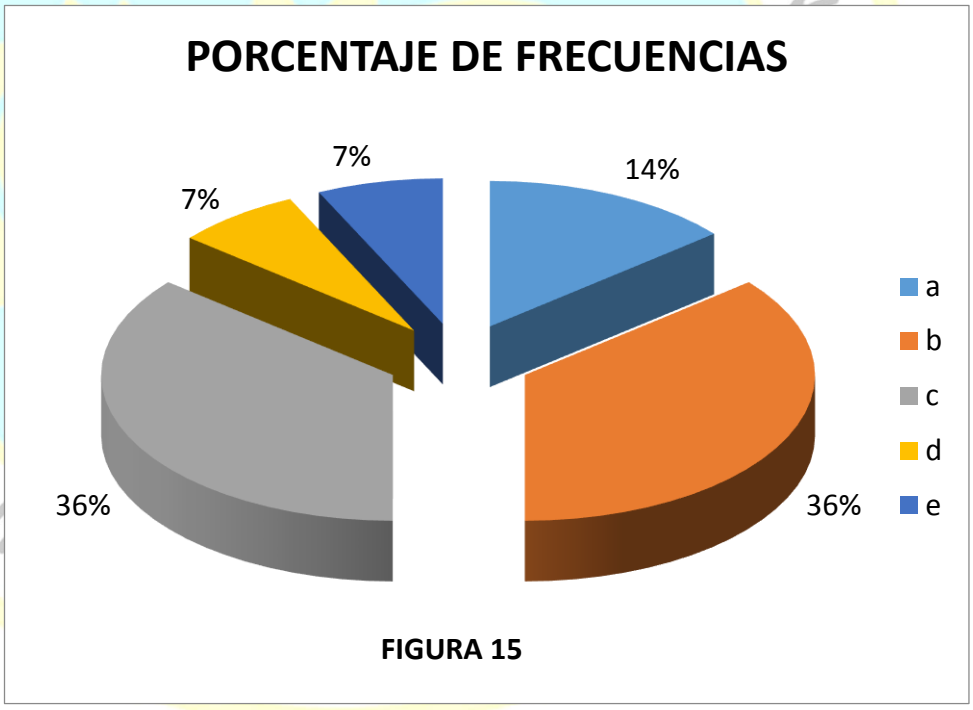

FIGURA 15

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática previene la detección de elementos peligrosos en el hospital regional de huacho, contestaron de la siguiente manera: 10(36%) dijeron a veces; 10(36%) dijeron casi siempre; 4(14%) dijeron siempre; 2(7%) dijo casi nunca y 2(7%) dijo nunca.

2.- La auditoría en seguridad informática nos ayuda a saber que puede suceder si se detecta un elemento peligroso en el hospital regional de huacho

Tabla Nª 16: *Detección de elementos peligrosos*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	2	0,07	7
b	Casi siempre	14	0,50	50
c	A veces	8	0,29	29
d	Casi nunca	4	0,14	14
e	Nunca	0	0,00	0
	total	28	1,00	100

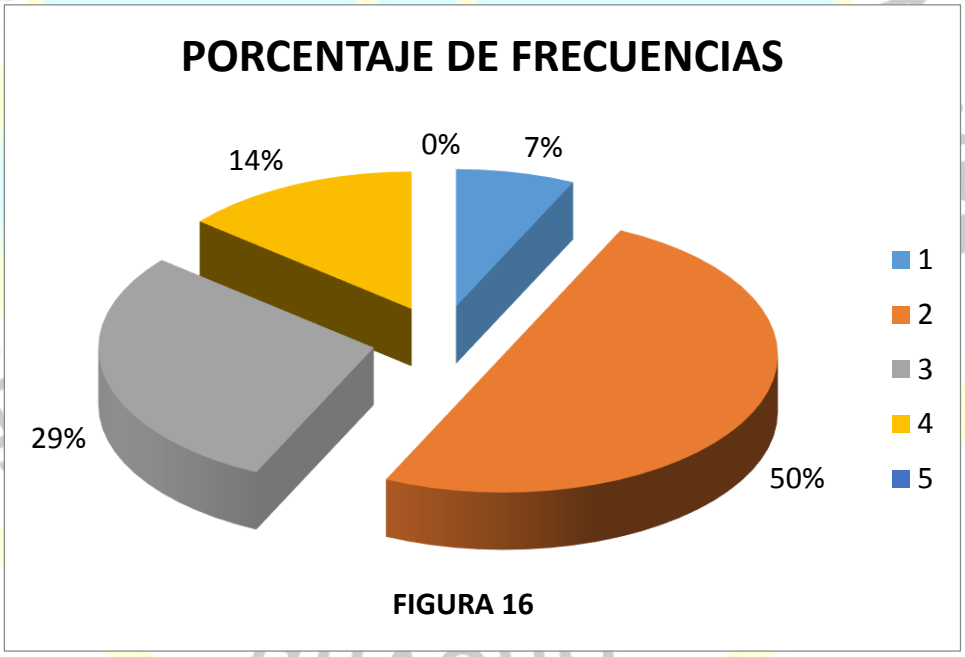

FIGURA 16

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a saber que puede suceder si se detecta un elemento peligroso en el hospital regional de huacho, contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 8(29%) dijeron a veces; 4(14%) dijeron casi nunca; 2(7%) dijo siempre y 0(0%) dijo nunca.

3.- La auditoría en seguridad informática nos ayuda a saber por qué se ha detectado algún elemento peligroso en el hospital regional de huacho

Tabla Nª 17: *Porque se detecta un elemento peligroso.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	10	0,36	36
b	Casi siempre	10	0,36	36
c	A veces	6	0,21	21
d	Casi nunca	2	0,07	7
e	Nunca	0	0,00	0
		28	1,00	100

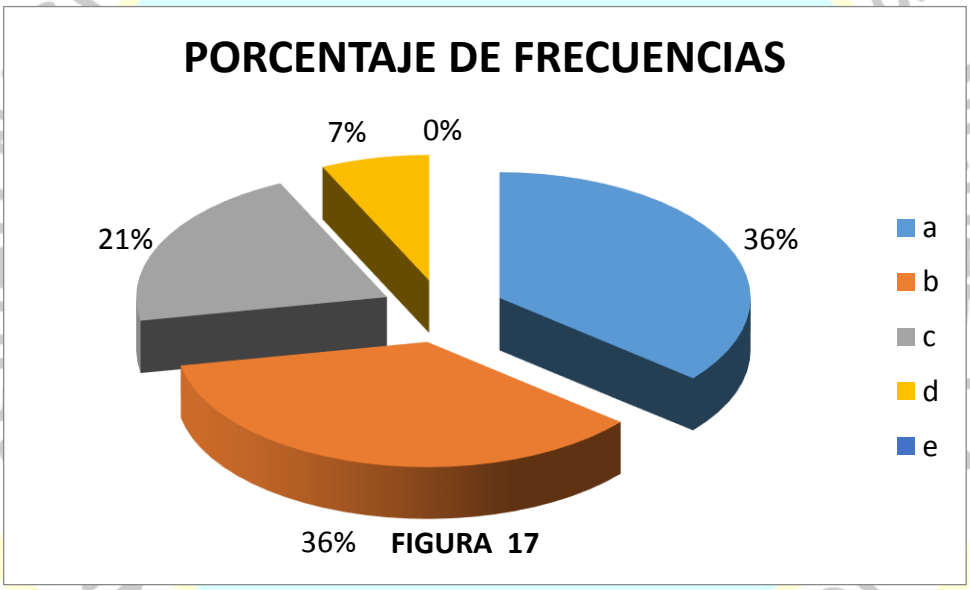

FIGURA 17

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a saber por qué se ha detectado algún elemento peligroso en el hospital regional de huacho, contestaron de la siguiente manera: 10(36%) siempre; 10(36%) dijeron casi siempre; 6(21%)dijeron a veces; 2(7%) dijo casi nunca y 0(0%) dijo nunca.

4.-La auditoría en seguridad informática nos ayuda a saber dónde se puede detectar un elemento peligroso en el hospital regional de huacho

Tabla Nª 18: *Donde se puede detectar algún elemento peligroso*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	5	0,18	18
b	Casi siempre	14	0,50	50
c	A veces	9	0,32	32
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
	Total	28	1,00	100

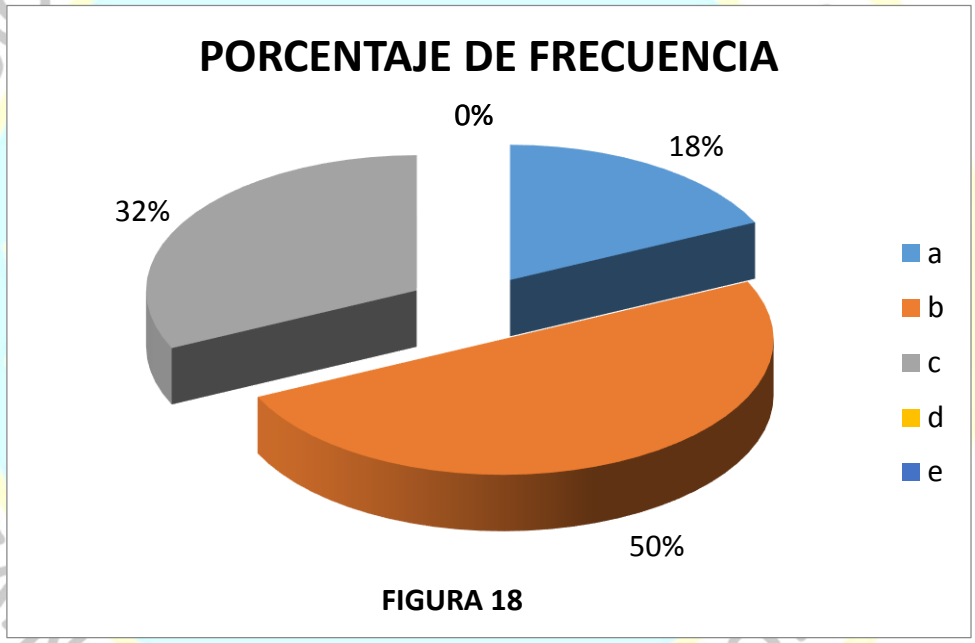

FIGURA 18

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a saber dónde se puede detectar un elemento peligroso en el hospital regional de huacho, contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 9(32%) dijeron a veces; 5(18%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

5.- La auditoría en seguridad informática nos ayuda a saber a quién le puede suceder si se detecta un elemento peligroso en el hospital regional de huacho

Tabla Nª 19: *A quien se le puede detectar algún elemento peligroso.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	5	0,18	18
b	Casi siempre	10	0,36	36
c	A veces	9	0,32	32
d	Casi nunca	4	0,14	14
e	Nunca	0	0,00	0
	Total	28	1,00	100

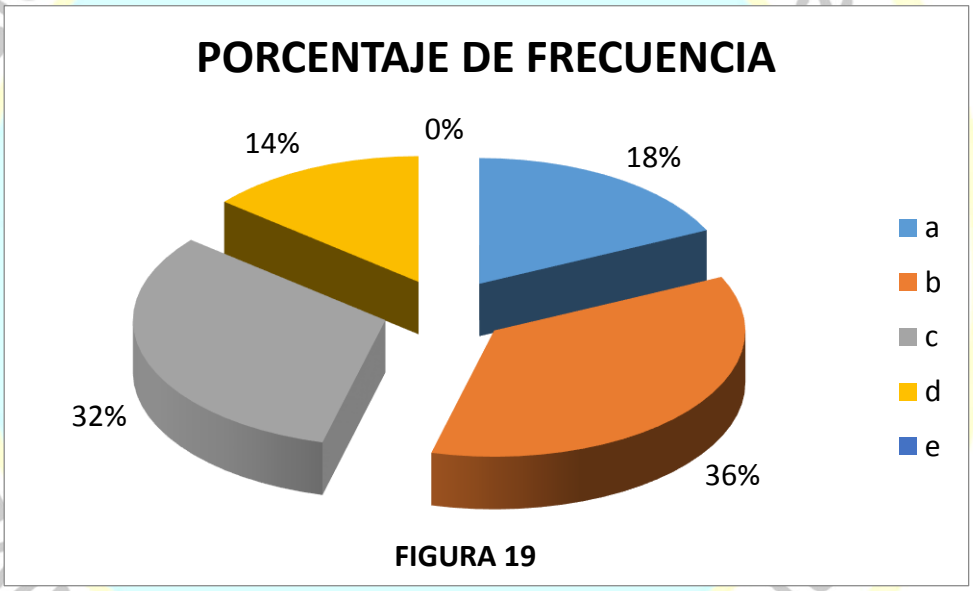

FIGURA 19

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La base de datos del hospital regional de huacho está totalmente segura, contestaron de la siguiente manera: 10(36%)dijeron casi siempre; 9(32%) dijeron a veces; 5(18%) dijeron siempre; 4(14%) dijo casi nunca y 0(0%) dijo nunca.

1.2 Analizar riesgos

6. La auditoría en seguridad informática nos ayuda a saber si se puede eliminar el riesgo en el hospital regional de huacho

.

Tabla Nª 20: *opciones de eliminar el riesgo.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	5	0,18	18
b	Casi siempre	9	0,32	32
c	A veces	14	0,50	50
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
	Total	28	1,00	100

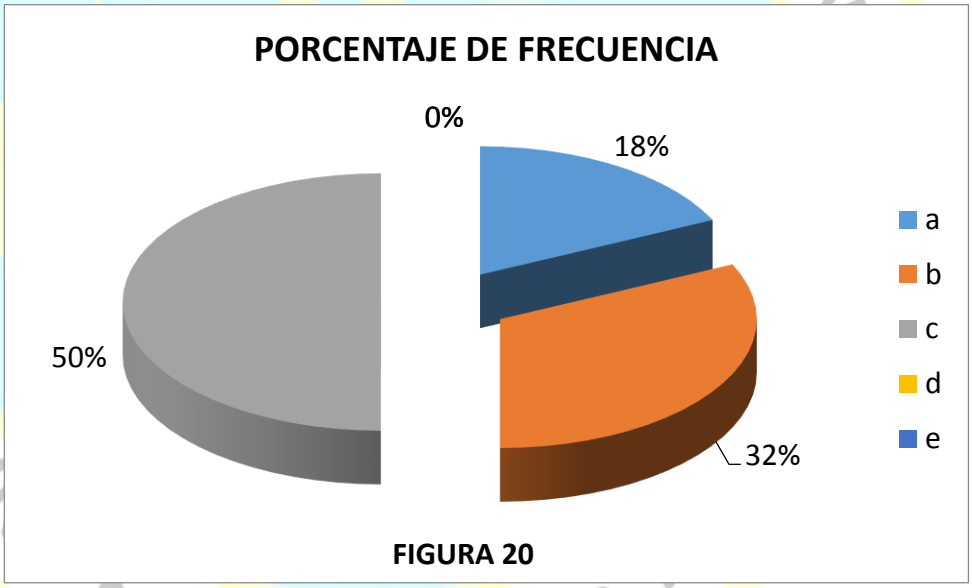

FIGURA 20

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a saber si se puede eliminar el riesgo en el hospital regional de huacho, contestaron de la siguiente manera: 14(50%)dijeron a veces; 9(32%) dijeron casi siempre; 5(18%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

7. La auditoría en seguridad informática nos ayuda a identificar las necesidades para eliminar el riesgo en el hospital regional de huacho

Tabla Nª 21: *Necesidades para eliminar un riesgo*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	4	0,14	14
b	Casi siempre	14	0,50	50
c	A veces	8	0,29	29
d	Casi nunca	2	0,07	7
e	Nunca	0	0,00	0
Total		28	1,00	100

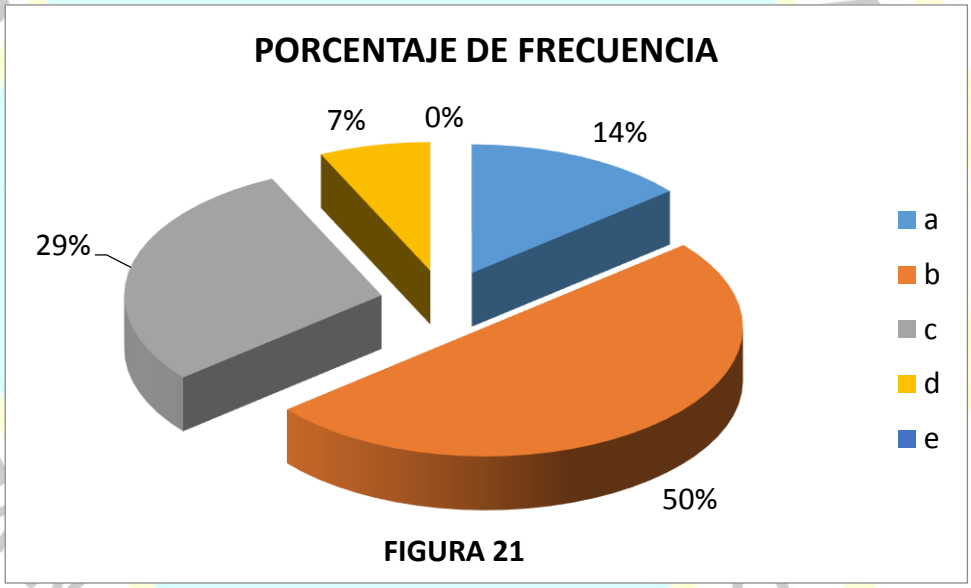

FIGURA 21

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a identificar las necesidades para eliminar el riesgo en el hospital regional de huacho; contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 8(29%) dijeron a veces; 4(14%) dijeron siempre; 2(7%) dijo casi nunca y 0(0%) dijo nunca.

8. La auditoría en seguridad informática nos ayuda a saber qué o quién puede ser dañado en el hospital regional de huacho.

Tabla Nª 22: *Qué o quién puede ser dañado.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	2	0,07	7
b	Casi siempre	5	0,18	18
c	A veces	16	0,57	57
d	Casi nunca	2	0,07	7
e	Nunca	3	0,11	11
Total		28	1,00	100

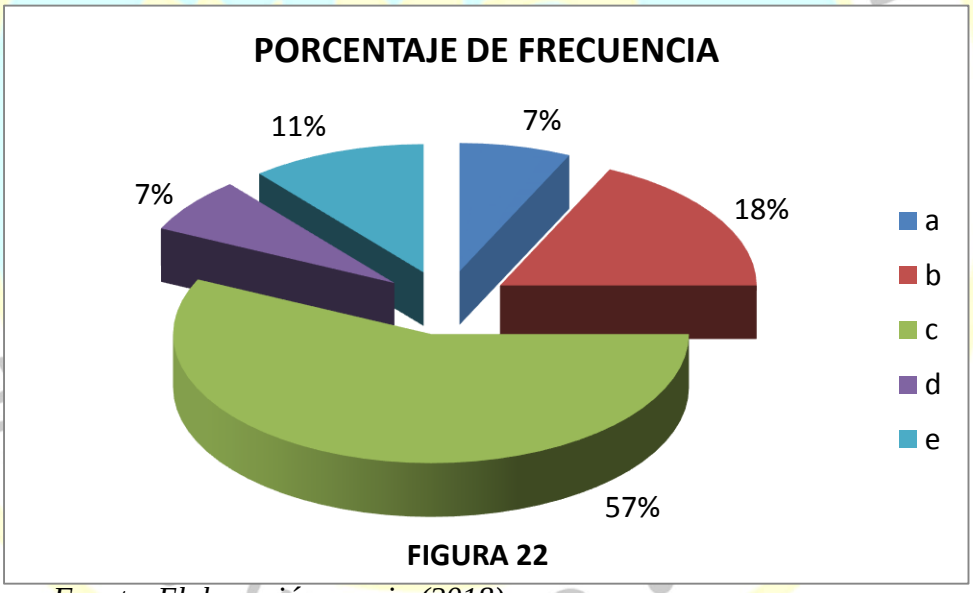

FIGURA 22

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a saber qué o quién puede ser dañado en el hospital regional de huacho, contestaron de la siguiente manera: 16(57) dijeron a veces; 5(18%) dijeron casi siempre; 3(11%) dijeron nunca; 2(7%) dijo casi nunca y 2(7%) dijo siempre.

1.3 Evaluar riesgos

9. La auditoría en seguridad informática nos ayuda a conocer la metodología al evaluar un riesgo en el hospital regional de huacho

Tabla Nª 23: *Evaluación del riesgo.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	5	0,18	18
b	Casi siempre	12	0,43	43
c	A veces	6	0,21	21
d	Casi nunca	5	0,18	18
e	Nunca	0	0,00	0
Total		28	1,00	100

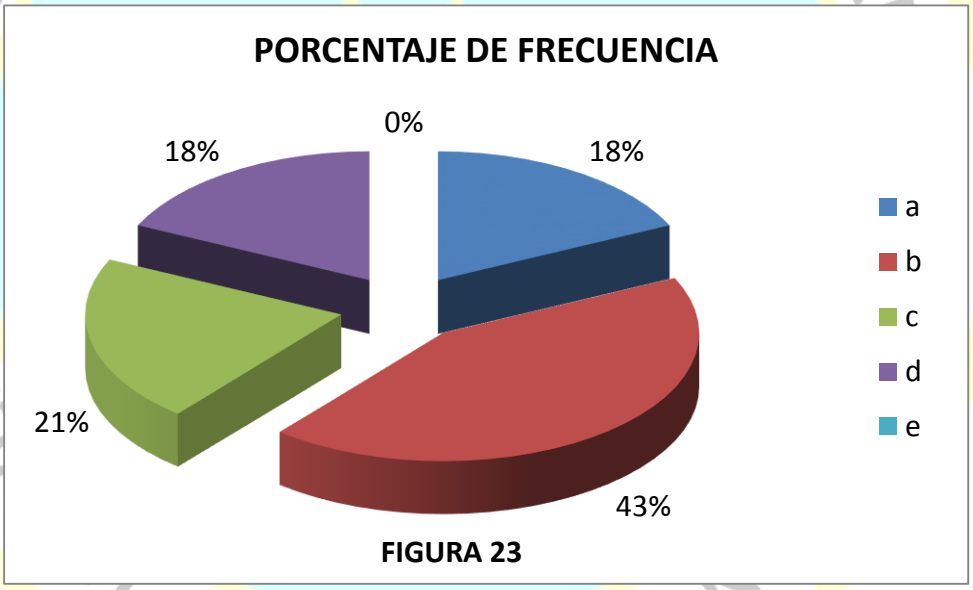

FIGURA 23

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a conocer la metodología al evaluar un riesgo en el hospital regional de huacho, contestaron de la siguiente manera: 12(43%)dijeron casi siempre; 6(21%) dijeron casi nunca; 5(18%) dijeron casi nunca; 5(18%) dijo siempre y 0(0%) dijo nunca.

10. La auditoría en seguridad informática nos ayuda a conocer la probabilidad que pueda suceder un riesgo en el hospital regional de huacho.

Tabla Nª 24: *Probabilidad que suceda un riesgo.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	2	0,07	7
b	Casi siempre	10	0,36	36
c	A veces	16	0,57	57
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
	Total	28	1,00	100

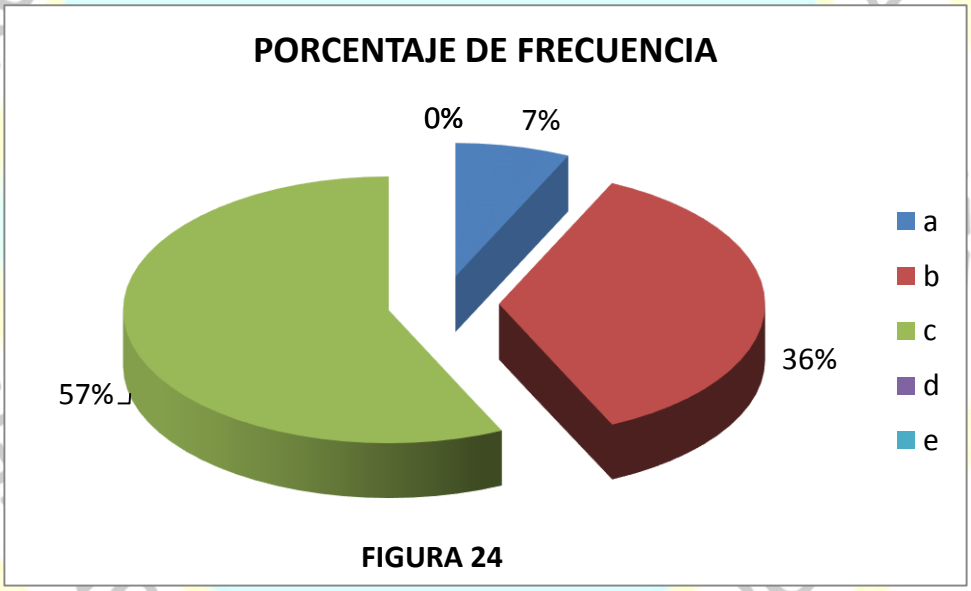

FIGURA 24

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a conocer la probabilidad que pueda suceder un riesgo en el hospital regional de huacho, contestaron de la siguiente manera: 16(57%)dijeron casi a veces 10(36%) dijeron casi siempre; 2(7%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

11. La auditoría en seguridad informática nos ayuda a conocer las consecuencias que puede ocasionar un riesgo en el hospital regional de huacho

Tabla Nª 25: *Consecuencias que ocasiona un riesgo*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	4	0,14	14
b	Casi siempre	14	0,50	50
c	A veces	10	0,36	36
d	Casi nunca	0	0,00	0
e	Nunca	0	0,00	0
	Total	28	1,00	100

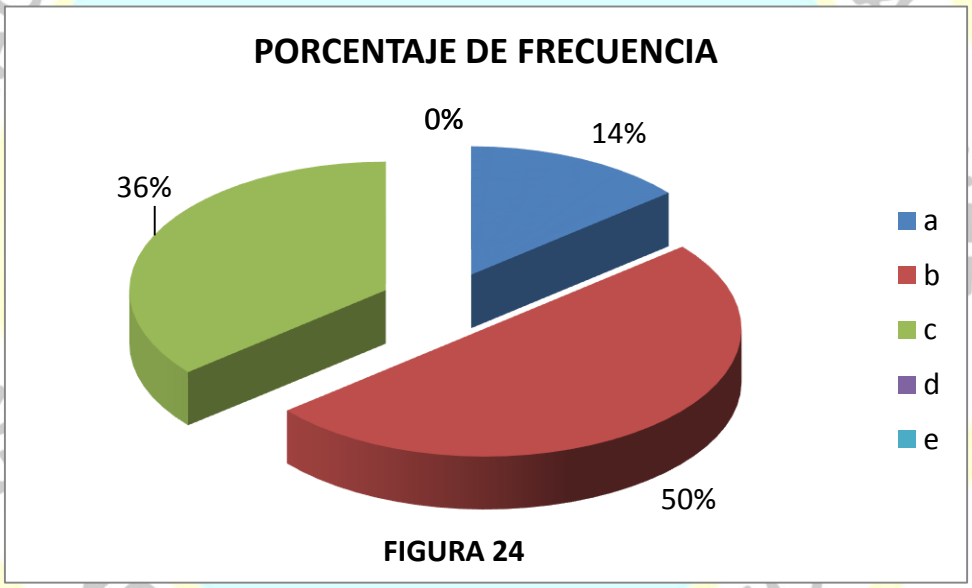

FIGURA 24

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a conocer las consecuencias que puede ocasionar un riesgo en el hospital regional de huacho; contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 10(36%) dijeron a veces; 4(14%) dijeron siempre; 0(0%) dijo casi nunca y 0(0%) dijo nunca.

1.4 Control del riesgo

12. La auditoría en seguridad informática nos ayuda a saber las medidas preventivas a aplicar ante un riesgo en el hospital regional de huacho

Tabla Nª 26: *Medidas preventivas ante un riesgo.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	6	0,21	21
b	Casi siempre	11	0,39	39
c	A veces	10	0,36	36
d	Casi nunca	1	0,04	4
e	Nunca	0	0,00	0
	Total	28	1,00	100

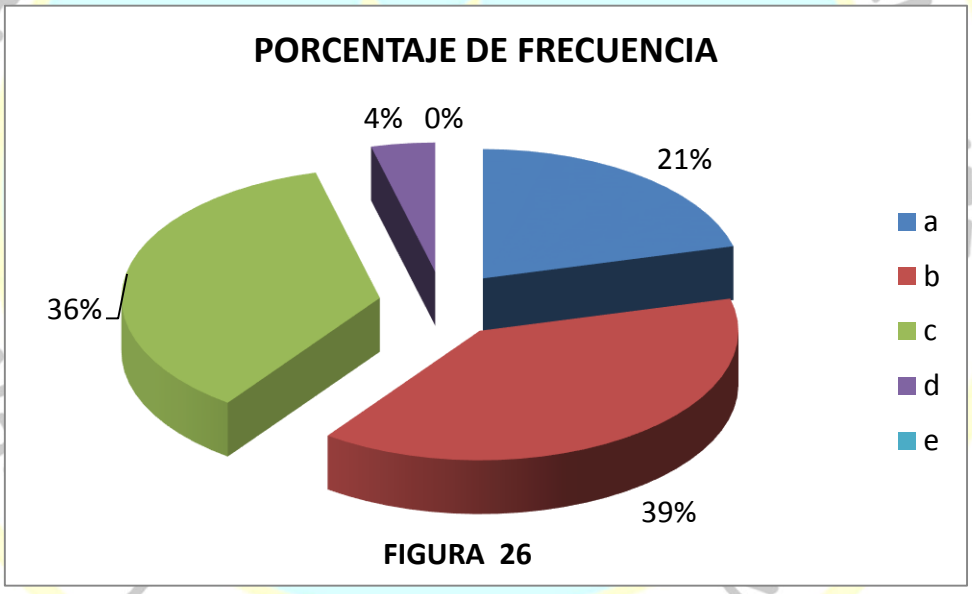

FIGURA 26

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a saber las medidas preventivas a aplicar ante un riesgo en el hospital regional de huacho, contestaron de la siguiente manera: 11(39%)dijeron casi siempre; 10(36%) dijeron a veces; 1(4%) dijeron casi nunca; 6(21%) dijo siempre y 0(0%) dijo nunca.

13. La auditoría en seguridad informática nos ayuda a conocer el control periódico que se debe realizar ante un riesgo en el hospital regional de huacho

Tabla Nª 27: *Control periódico a realizar ante un riesgo.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	6	0,21	21
b	Casi siempre	10	0,36	36
c	A veces	10	0,36	36
d	Casi nunca	2	0,07	7
e	Nunca	0	0,00	0
	Total	28	1,00	100

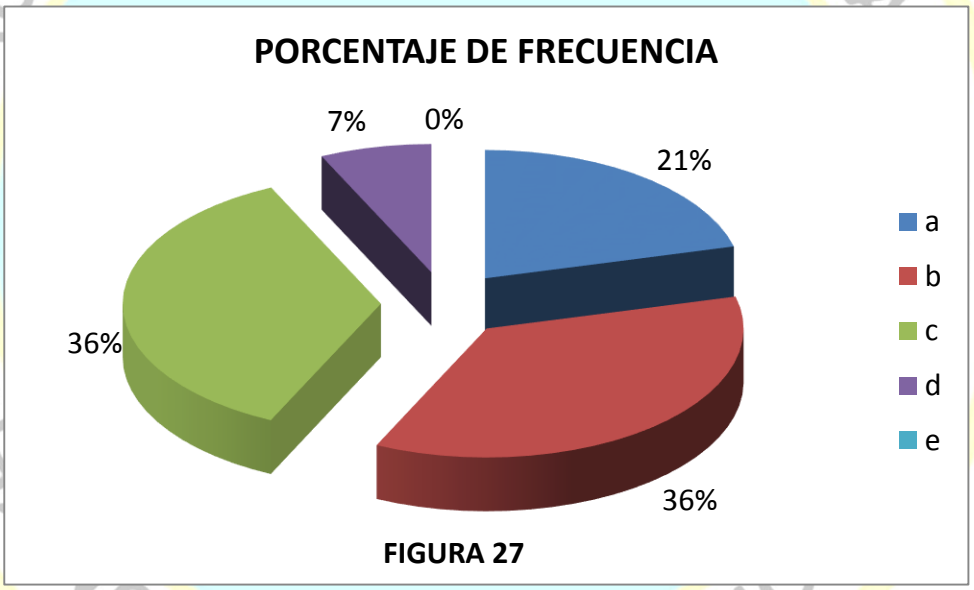

FIGURA 27

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a conocer el control periódico que se debe realizar ante un riesgo en el hospital regional de huacho, contestaron de la siguiente manera:10(36%)dijeron casi siempre; 10(36%) dijeron a veces; 6(21%) dijeron siempre; 2(7%) dijo casi nunca y 0(0%) dijo nunca.

14. La auditoría en seguridad informática nos ayuda a conocer la información y consulta de un riesgo en el hospital regional de huacho

Tabla Nª 28: *Información y consulta del riesgo.*

Código	Categoría	Frecuencia y porcentaje		
		ni	hi	%
a	Siempre	0	0,00	0
b	Casi siempre	14	0,50	50
c	A veces	10	0,36	36
d	Casi nunca	4	0,14	14
e	Nunca	0	0,00	0
	Total	28	1,00	100

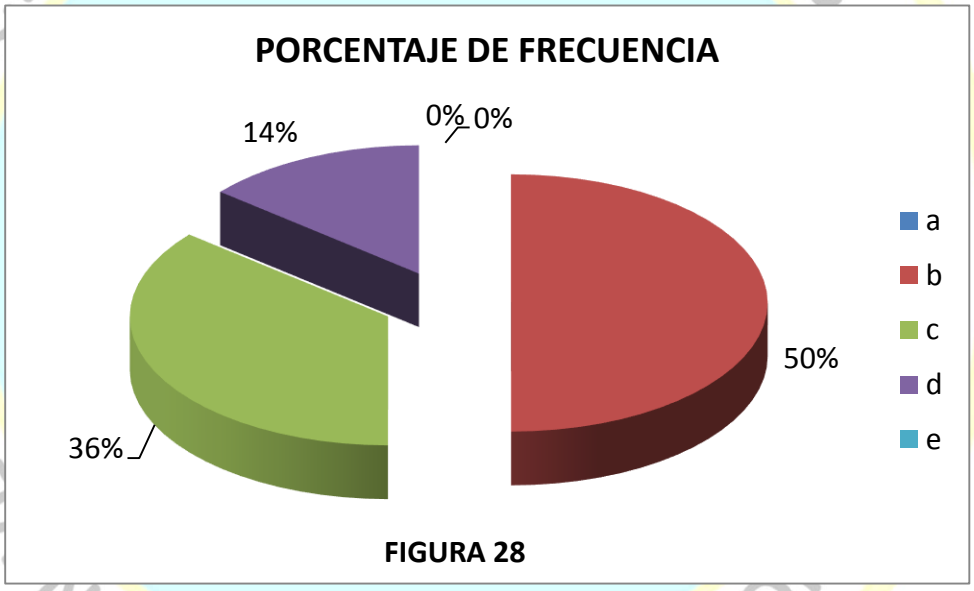

FIGURA 28

Fuente. Elaboración propia (2018).

Interpretación

De una muestra de 28 trabajadores respecto al enunciado: La auditoría en seguridad informática nos ayuda a conocer la información y consulta de un riesgo en el hospital regional de huacho, contestaron de la siguiente manera: 14(50%)dijeron casi siempre; 10(369%) dijeron a veces; 4(14%) dijeron casi nunca; 0(4%) dijo siempre y 0(0%) dijo nunca.

Validez del Instrumento

La validez del instrumento (Instrumento para la toma de datos) de la presente investigación, se realizó por medio del juicio de expertos, en donde ellos evaluaron y a criterio propio calificaron el contenido del cuestionario empleado. Los expertos que realizaron fueron los siguientes:

Experto 1: Ing. Huamán Tena Ángel – CIP N° 41456.

Experto 2: Ing. Huamán Tena Noé – CIP N° 16758.

Experto 3: Doc. Carraco Díaz Sergio Oswaldo – CAL Nº 35145

Las calificaciones para los criterios de validación, que se mencionan en la hoja de juicio de experto (Juicio de Expertos) con respecto al contenido del instrumento, se muestran en la siguiente tabla:

TABLA 1: Calificación de los Expertos

Nª PREGUNTA Y ALTERNATIVAS	EXPERTOS			TA
	E1	E2	E3	
V1 Pregunta Nº 1 y sus alternativas	1	1	1	3
V1 Pregunta Nº 2 y sus alternativas	1	1	1	3
V1 Pregunta Nº 3 y sus alternativas	1	1	1	3
V1 Pregunta Nº 4 y sus alternativas	1	1	1	3
V1 Pregunta Nº 5 y sus alternativas	1	1	0	2
V1 Pregunta Nº 6 y sus alternativas	1	1	1	2
V1 Pregunta Nº 7 y sus alternativas	1	1	1	3
V1 Pregunta Nº 8 y sus alternativas	1	1	1	3
V1 Pregunta Nº 9 y sus alternativas	1	0	1	2
V1 Pregunta Nº 10 y sus alternativas	1	1	1	3
V1 Pregunta Nº 12 y sus alternativas	1	1	1	3
V1 Pregunta Nº 13 y sus alternativas	1	1	1	3
V1 Pregunta Nº 14 y sus alternativas	1	0	1	2
V2 Pregunta Nº 1 y sus alternativas	1	1	1	3
V2 Pregunta Nº 2 y sus alternativas	1	1	1	3
V2 Pregunta Nº 3 y sus alternativas	1	1	1	3
V2 Pregunta Nº 4 y sus alternativas	1	1	1	3
V2 Pregunta Nº 5 y sus alternativas	1	1	1	3
V2 Pregunta Nº 6 y sus alternativas	0	1	1	2
V2 Pregunta Nº 7 y sus alternativas	1	1	1	3

V2 Pregunta Nº 8 y sus alternativas	1	1	1	3
V2 Pregunta Nº 9 y sus alternativas	1	1	1	3
V2 Pregunta Nº 10 y sus alternativas	1	1	1	3
V2 Pregunta Nº 12 y sus alternativas	1	1	1	3
V2 Pregunta Nº 13 y sus alternativas	1	1	1	3
V2 Pregunta Nº 14 y sus alternativas	1	1	1	3
Totalmente de Acuerdo (TA)=	27	26	27	80

FUENTE: Elaboración propia

Donde: 1 = Totalmente de Acuerdo (TA)

0 = Totalmente en Desacuerdo (TD)

CÁLCULO DEL COEFICIENTE DE VALIDEZ

$$Validez = \frac{Total\ de\ Acuerdo}{Total\ de\ Acuerdo\ (TA) + Total\ de\ Desacuerdo\ (TD)}$$

$$Variable = \frac{80}{84+2} = 0.95 = 95\%$$

Con una validez general de 95% según la escala de validez el instrumento tiene Validación Perfecta; de acuerdo al criterio de los expertos.

TABLA 2: Calificación de los Expertos

ESCALA	INDICADOR
0.00 - 0.53	Validez Nula
0.54 - 0.64	Validez Baja
0.65 - 0.69	Válida
0.70 - 0.80	Muy Válida
0.81 - 0.94	Excelente Validez
0.95 - 1.00	Validez Perfecta

FUENTE: (Herrera, 1998)

4.2 Contrastación de hipótesis

Para la prueba de hipótesis, tanto general como específicas se empleará la Prueba T.

PRUEBA DE LAS HIPOTESIS ESPECÍFICAS

PRUEBA DE NORMALIDAD

Si n<=50, se analiza la prueba de Shapiro-Wilk y si el sig. es menor de 0.05, se puede afirmar que los datos no proceden de una distribución normal, como en este caso. Si la muestra es mayor a 50, la prueba de Kolmogorov-Smirnov[a] es la sugerida.

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Auditoria en seguridad informática	,224	28	,001	,883	28	,005
Seguridad lógica	,215	28	,002	,869	28	,002
Seguridad de aplicaciones	,246	28	,000	,874	28	,003
Administración del centro de procesamiento	,245	28	,000	,879	28	,004
Gestión de riesgo	,239	28	,000	,853	28	,001
Identificación del riesgo	,248	28	,000	,884	28	,005
Analizar riesgos	,280	28	,000	,838	28	,001
Evaluar riesgos	,239	28	,000	,853	28	,001
Control del riesgo	,239	28	,000	,873	28	,003

a. Corrección de significación de Lilliefors

PRIMERA HIPÓTESIS ESPECÍFICA

a) Hipótesis específica nula.

La seguridad lógica **no se relaciona** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

b) Hipótesis específica alternativa.

La seguridad lógica **se relaciona** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

c) Regla para contrastar la hipótesis

Si el valor p > 0,04, se acepta Ho. Si el valor p < 0,04 se rechaza Ho.

d) Estadístico para contrastar la hipótesis.

Correlaciones

		Seguridad Lógica	Gestión de Riesgo
Seguridad Lógica	Correlación de Pearson	1	,848**
	Sig. (bilateral)		,000
	N	28	28
Gestión de Riesgo	Correlación de Pearson	,848**	1
	Sig. (bilateral)	,000	
	N	28	28

**. La correlación es significativa al nivel 0,01 (bilateral).

Interpretación:

Como el valor de p = 0,000 < 0,04, se rechaza la hipótesis nula y podemos afirmar, con un 96% de probabilidad que:

1. La seguridad lógica se relaciona directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.
2. La correlación de la seguridad lógica con la Gestión de Riesgo es de 84,8%.

SEGUNDA HIPÓTESIS ESPECÍFICA

a) Hipótesis específica nula

La seguridad de aplicaciones **no se relaciona** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

b) Hipótesis específica alternativa

La seguridad de aplicaciones **se relaciona** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

c) Regla para contrastar la hipótesis

Si el valor p > 0,04, se acepta Ho. Si el valor p < 0,04 se rechaza Ho.

d) Estadístico para contrastar la hipótesis.

Correlaciones

		Seguridad de aplicaciones	Gestión de Riesgo
Seguridad de aplicaciones	Correlación de Pearson	1	,905**
	Sig. (bilateral)		,000
	N	28	28
Gestión de Riesgo	Correlación de Pearson	,905**	1
	Sig. (bilateral)	,000	
	N	28	28

**. La correlación es significativa al nivel 0,01 (bilateral).

e) Interpretación

Como el valor de p = 0,000 < 0,04, se rechaza la hipótesis nula y podemos afirmar, con un 96% de probabilidad que:

1. La seguridad de aplicaciones se relaciona directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.
2. La correlación de la seguridad lógica con la Gestión de Riesgo es de 90,5%.

TERCERA HIPOTESIS ESPECÍFICA

a) Hipótesis específica nula

La administración del centro de procesamiento **no se relaciona** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

b) Hipótesis específica alternativa

La administración del centro de procesamiento **se relaciona** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

c) Regla para contrastar la hipótesis

Si el valor p > 0,04, se acepta Ho. Si el valor p < 0,04 se rechaza Ho.

d) Estadístico para contrastar la hipótesis.

Correlaciones

		Administración del centro de procesamiento	Gestión de Riesgo
Administración del centro de procesamiento	Correlación de Pearson	1	,957**
	Sig. (bilateral)		,000
	N	28	28
Gestión de Riesgo	Correlación de Pearson	,957**	1
	Sig. (bilateral)	,000	
	N	28	28

**. La correlación es significativa al nivel 0,01 (bilateral).

e) Interpretación

Como el valor de p = 0,000 < 0,04, se rechaza la hipótesis nula y podemos afirmar, con un 96% de probabilidad que:

1. La Administración del centro de procesamiento se relaciona directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.
2. La correlación de la Administración del centro de procesamiento con la Gestión de Riesgo es de 95,7%.

PRUEBA DE HIPÓTESIS GENERAL

a) Hipótesis específica nula

La Auditoria en seguridad informática **no se relacionan** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

b) Hipótesis específica alternativa

La Auditoria en seguridad informática **se relacionan** directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

c) Regla para contrastar la hipótesis

Si el valor p > 0,04, se acepta Ho. Si el valor p < 0,04 se rechaza Ho.

d) Estadístico para contrastar la hipótesis.

Correlaciones

		Auditoria en seguridad informática	Gestión de Riesgo
Auditoria en seguridad informática	Correlación de Pearson	1	,936**
	Sig. (bilateral)		,000
	N	28	28
Gestión de Riesgo	Correlación de Pearson	,936**	1
	Sig. (bilateral)	,000	
	N	28	28

**. La correlación es significativa al nivel 0,01 (bilateral).

e) Interpretación

Como el valor de p = 0,000 < 0,04, se rechaza la hipótesis nula y podemos afirmar, con un 96% de probabilidad que:

1. La Auditoria en seguridad informática se relaciona directamente con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.
2. La correlación de la Auditoria en seguridad informática con la Gestión de Riesgo es de 93,6%.

CAPÍTULO V

DISCUSIÓN

5.1 Discusión de resultados

Al realizar el proceso de prueba de hipótesis, tanto de las específicas como de la general, se ha determinado que existe relación directa entre cada uno de los indicadores de la Variable Independiente Auditoria en seguridad informática y la variable dependiente Gestión de Riesgo, con los que se han formulado las hipótesis específicas.

Los resultados obtenidos son de trascendente importancia puesto que nos proporcionan la base informativa necesaria para poder plantear las alternativas de solución al problema de investigación que ha sido la razón de nuestro trabajo de tesis. Alternativas que estarán directamente relacionadas con la Auditoria en seguridad informática dirigida a mejorar la Gestión de Riesgo.

La Prueba T, nos ha permitido conocer que existe una relación entre las variables, con tendencia ser muy alta, es decir, de 0,936.

Igualmente se ha determinado la relación de las hipótesis específicas en los siguientes términos:

Primera hipótesis específica, presenta una correlación de 0,848, indicando que la correlación es alta. Esta correlación significa la seguridad lógica se relaciona directamente con la Gestión de Riesgo.

Segunda hipótesis específica, presenta una correlación de 0,905, indicando que este resultado expresa una relación de nivel muy alto entre la seguridad de aplicaciones y la Gestión de Riesgo.

Tercera hipótesis específica, presenta una correlación de 0,957, indicando que la correlación es muy alta. Esta correlación significa que la Administración del centro de procesamiento se relaciona directamente con la Gestión de Riesgo.

Con respecto a la hipótesis General se ha obtenido como resultado 0,936, significando la existencia de una relación muy alta entre la variable independiente Auditoria en seguridad informática y la variable dependiente la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

CONCLUSIONES PARCIALES: HIPÓTESIS ESPECÍFICAS

1.1 Se ha demostrado que existe una relación positiva alta (0,848) entre la seguridad lógica y la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

La relación está referida a que la media de puntaje obtenido en la seguridad lógica es de 3,82, sobre el puntaje máximo que es de 5, lo que en su escala valorativa equivale "regular", y la media de la Gestión de Riesgo es de 3.68 que en su escala valorativa es igual a regular, es decir, hay una relación directa, por cuanto se tiene una seguridad lógica con una calificación de regular y una Gestión de Riesgo de nivel también regular.

1.2 Se ha demostrado que existe una relación positiva alta (0,905) entre la seguridad de aplicaciones y la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

La relación está referida a que la media de puntaje obtenido en la seguridad de aplicaciones es de 3,54, sobre el puntaje máximo que es de 5, lo que en su escala valorativa equivale "regular", y la media la Gestión de Riesgo es de 3.68 que en su escala valorativa es igual a regular, es decir, hay una relación directa, por cuanto se tiene una seguridad de aplicaciones con una calificación de regular y una Gestión de Riesgo de nivel también regular.

1.3 Se ha demostrado que existe una relación positiva alta (0,957) entre la Administración del centro de procesamiento y la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

La relación está referida a que la media de puntaje obtenido en la Administración del centro de procesamiento es de 3,61, sobre el puntaje máximo que es de 5, lo que en su escala valorativa equivale "regular", y la media de la Gestión de Riesgo es de 3.68 que en su escala valorativa es igual a regular, es decir, hay una relación directa, por cuanto se tiene una Administración del

centro de procesamiento con una calificación de regular y una Gestión de Riesgo de nivel también regular.

CONCLUSION GENERAL: HIPÓTESIS GENERAL

Se ha comprobado que la Auditoria en seguridad informática tiene una alta correlación (0,936) con la Gestión de Riesgo en el Hospital Regional Huacho, 2018.

La relación está referida a que la media de puntaje obtenido en la aplicación de la Auditoria en seguridad informática es de 3,64 sobre la base de un puntaje máximo de 5, lo que en su escala valorativa es igual a "regular", y la media de notas de la Gestión de Riesgo es de 3,68, que en su escala valorativa también es igual a regular, es decir, hay una relación directa, por cuanto se tiene una Auditoria en seguridad informática con una calificación de regular y una Gestión de Riesgo de nivel también regular.

6.2 Recomendaciones

1. Como la media de calificación de seguridad lógica muestra un nivel de solo regular y una gestión de riesgo también de regular se recomienda la implementación de usuarios y contraseñas para el personal, así como también la segregación de funciones para cada usuario.
2. La seguridad de aplicaciones y la gestión de riesgo apenas alcanza un nivel de regular por lo que se recomienda un mejor control de los softwares que se instalan en las PC's del hospital regional de huacho.
3. En cuanto a la administración del centro de procesamiento, muestra un nivel de solo regular y la gestión de riesgo también muestra un nivel de regular, se recomienda mayor capacitación del personal del centro de procesamiento de datos, y un mejor resguardo de los backups.
4. La Auditoria en seguridad informática y la Gestión de Riesgo en el Hospital Regional Huacho al haber alcanzado una calificación de regular es recomendable tomar consciencia sobre la administración de riesgos, como parte fundamental de las operaciones del departamento. Definir políticas de evaluación y administración de riesgos. Identificar los posibles eventos y sus respectivos impactos que puedan afectar el buen funcionamiento del departamento. Evaluar frecuentemente la posibilidad de ocurrencia de riesgos identificados basados en métodos cuantitativos y cualitativos.

REFERENCIAS

7.1 Fuentes bibliográficas

Alvarez Basaldúa, L. D. (2005). Seguridad en Informática- Auditoría en Sistemas. *Tesis de Maestría*. México: Universidad Iberoamericana .

Aldegani, G. (1997). *Seguridad informática*. Mp. Ediciones.

Cervigón, A; Alegre, M (2011). *Seguridad Informática*. Madrid, España.

Echenique, J (2008). *Auditoria en Informática segunda edición*. México.

Editorial Editex S. A (2010). *Seguridad Informática*. Madrid, España.

Gómez, L., & Andrés, A. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. *Iso 27001*. España: AENOR.

Huaman, Fernando.(2014).Diseño de Procedimientos de Auditoria De Cumplimiento De la Norma NTP-ISO/IEC 17799:207 Como parte del Proceso de implantacion de la Norma Tecnica NTP_ISO/IEC 27991:2008 En Insituciones del Estado Peruano. Tesis de pregrado para obtener el Titulo de Ingeniero Informatico. Peru: Pontifica Universidad Catolica Del Perú.

Lázaro, M (2008). *Seguridad de la Información. Oficina Nacional de Gobierno Electrónico e Informática PCM*. Perú.

Monzón, C. (2009). *Auditoria de seguridad de redes inalámbricas de área local Wireless Local Área Network (WLAN)*. Universidad Mayor de San Andrés. Bolivia.

Muñoz, C. (2010). *Auditoría en Sistemas Computacionales*. México.

Piattini, M (2001). *Auditoria informática. Un enfoque Práctico*. Ra-Ma.

Semillan Giancarlo, Castillo Edwin, L. (2012). Auditoría Informatica Usando Las normas Cobit en el Centro de Sistemas De Informacion Del Hospital Regional Docente Las mercedes de Chiclayo. *Tesis de pregrado para obtener el Titulo de Ingeniero de Sitemas*. Peru: Universidad Nacional “Pedro Ruiz Gallo.

7.2 Fuentes hemerográficas

ISACA (2007). COBIT 4.1 Edición en español.

INDECOPI (2007). EDI. *Tecnología de la Información. Código de buenas Prácticas para la Gestión de la Seguridad de la Información. NTP-ISO/IEC 17799-2007*.Lima, Perú.

7.3 Fuentes referidas a la metodología de investigación

Ander, E. (1982). Técnicas de Investigación Social. 21ava Edición. Buenos Aires Argentina. Humanitas.

Alarcón, R. (1991). Métodos y Diseños de Investigación del Comportamiento. Lima Perú Universidad Cayetano Heredia.

Arias, G. (1991). Fernando. Introducción a la Metodología de la Investigación en Ciencias de la Administración y del Comportamiento. México 1991. Trillas

Boundon, R. y Lazarsfeld, P. Metodología de las Ciencias Sociales, Editorial Lara. Barcelona España, Lara.

Carrasco, S. (2005). Metodología de la Investigación Científica. Aplicación en educación y otras ciencias sociales. Primera Edición. Lima Perú, Editorial San Marcos.

Cervo, A. y Bervian, P. 1979). Metodología de la Investigación Social. Editorial Mc Graw Hill Latinoamericana S. A. Bogotá Colombia.

ANEXOS

UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCALA DE LIKERT

VARIABLE A MEDIR: AUDITORIA EN SEGURIDAD INFORMÁTICA

INSTRUCCIONES: Estimados usuarios a continuación se presentan un conjunto de ítems sobre la **AUDITORIA EN SEGURIDAD INFORMÁTICA** en el Hospital regional de Huacho por favor responda con toda objetividad, pues de ello dependerá el éxito en el presente estudio de investigación. Marque con una (X) su respuesta en los recuadros valorados del 1 al 5

Nº	ITEMS	S	CS	AV	CN	N
		5	4	3	2	1
1.1	**Seguridad Lógica**					
1	En el hospital regional de huacho existe la identificación de usuarios					
2	En el hospital regional de huacho se utilizan los password para el acceso de los usuarios					
3	En el hospital regional de huacho se utiliza la segregación de funciones para darle responsabilidades a los usuarios					
1.2	**Seguridad de las aplicaciones**					
4	Los softwares que se utilizan en el hospital regional de huacho son seguros y confiables					
5	La base de datos del hospital regional de huacho está totalmente segura					
6	Las aplicaciones instaladas en las PC's del Hospital regional de Huacho están totalmente controladas					
7	Los datos de las aplicaciones instaladas en las PC's del Hospital regional de Huacho están salvaguardados					

8	Las PC's del hospital regional de huacho tienen antivirus que están en constante actualización					
9	El firewall de las PC's del hospital regional de Huacho están siempre activado					
10	Las aplicaciones del Hospital regional de huacho están siempre protegidas a ataques de red					
1.3	**Administración del centro de procesamiento**					
11	EL CPD(centro de procesamiento de datos) del Hospital regional de Huacho está correctamente administrado					
12	Los usuarios del CPD(centro de procesamiento de datos) del Hospital regional de Huacho están en constante capacitación.					
13	Los backups del CPD(centro de procesamiento de datos) del hospital regional de Huacho están totalmente protegidos					
14	El tratamiento de la documentación del CPD(centro de procesamiento de datos) del hospital regional de huacho es el más adecuado					

ESCALA VALORATIVA

CÓDIGO	CATEGORÍA	VALORACIÓN CUALITATIVA	PUNTAJE
a	Siempre	Muy bueno	5
b	Casi siempre	Bueno	4
c	A veces	Regular	3
d	Casi nunca	Deficiente	2
e	Nunca	Muy deficiente	1

UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCALA DE LIKERT

VARIABLE A MEDIR: GESTIÓN DE RIESGO

INSTRUCCIONES: Estimados usuarios a continuación se presentan un conjunto de ítems sobre la **GESTIÓN DE RIESGO** en el Hospital regional de Huacho por favor responda con toda objetividad, pues de ello dependerá el éxito en el presente estudio de investigación. Marque con una (X) su respuesta en los recuadros valorados del 1 al 5

Nº	ITEMS	S	CS	AV	CN	N
		5	4	3	2	1
1.1	**Identificación del Riesgo**					
1	La auditoría en seguridad informática previene la detección de elementos peligrosos en el hospital regional de huacho					
2	La auditoría en seguridad informática nos ayuda a saber que puede suceder si se detecta un elemento peligroso en el hospital regional de huacho					
3	La auditoría en seguridad informática nos ayuda a saber por qué se ha detectado algún elemento peligroso en el hospital regional de huacho					
4	La auditoría en seguridad informática nos ayuda a saber dónde se puede detectar un elemento peligroso en el hospital regional de huacho					
5	La auditoría en seguridad informática nos ayuda a saber a quién le puede suceder si se detecta un elemento peligroso en el hospital regional de huacho					
1.2	**Analizar riesgos**					

6	La auditoría en seguridad informática nos ayuda a saber si se puede eliminar el riesgo en el hospital regional de huacho.					
7	La auditoría en seguridad informática nos ayuda a identificar las necesidades para eliminar el riesgo en el hospital regional de huacho.					
8	La auditoría en seguridad informática nos ayuda a saber qué o quién puede ser dañado en el hospital regional de huacho.					
1.3	**Evaluar riesgos**					
9	La auditoría en seguridad informática nos ayuda a conocer la metodología al evaluar un riesgo en el hospital regional de huacho.					
10	La auditoría en seguridad informática nos ayuda a conocer la probabilidad que pueda suceder un riesgo en el hospital regional de huacho.					
11	La auditoría en seguridad informática nos ayuda a conocer las consecuencias que puede ocasionar un riesgo en el hospital regional de huacho.					
1.4	**Control del riesgo**					
12	La auditoría en seguridad informática nos ayuda a saber las medidas preventivas a aplicar ante un riesgo en el hospital regional de huacho.					
13	La auditoría en seguridad informática nos ayuda a conocer el control periódico que se debe realizar ante un riesgo en el hospital regional de huacho.					
14	La auditoría en seguridad informática nos ayuda a conocer la información y consulta de un riesgo en el hospital regional de huacho.					

ESCALA VALORATIVA

CÓDIGO	CATEGORÍA	VALORACIÓN CUALITATIVA	PUNTAJE
a	Siempre	Muy bueno	5
b	Casi siempre	Bueno	4
c	A veces	Regular	3
d	Casi nunca	Deficiente	2
e	Nunca	Muy deficiente	1

El investigador.

Ing. ANGEL HUAMÁN TENA
ASESOR

Ing. JOSE LUIS PEREZ RAMIREZ
PRESIDENTE

Ing. EDWIN IVAN FARRO PACIFICO
SECRETARIO

Ing. PIERRE PAUL LONCAN SALAZAR
VOCAL