UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ESCUELA DE POSGRADO

TESIS

Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016

Para optar el grado académico de maestro en:

Gestión Empresarial

Autor: Augurio Oscar RIVERA DAVILA

Asesor: Mg. Fortunato Tarcisio INGA JACAY

Cerro de Pasco - Perú – 2019

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ESCUELA DE POSGRADO

TESIS

Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016

Sustentada y aprobada ante los miembros del jurado:

Dr. José Luis GUERRERO FEBRES
PRESIDENTE

Dr. Humberto Rafael YUPANQUI VILLANUEVA
MIEMBRO

Mg. Jesús Moisés SALAZAR ALCARAZ
MIEMBRO

A mis padres.

Por su apoyo incondicional en mi vida. Quienes me inculcaron fortaleza, en el desarrollo y superación constante, para el logro de mis sueños hecho realidad; que serán aportes para la Sociedad.

RECONOCIMIENTO

El reconocimiento profundo al alma mater, la Universidad Nacional Daniel Alcides Carrión, y las enseñanzas de los profesores de especialidad, quienes con su sacrificio abnegado hicieron realidad, para llegar a los lauros del triunfo; asimismo, veo realizado mis deseos de llegar a cumplir el objetivo de obtener el grado de maestro, mediante el presente trabajo de investigación.

El reconocimiento a mi asesor por compartir sus experiencias y consejos recibidos para el desarrollo y culminación del presente trabajo, y gracias a toda la familia de post grado que me brindaron su apoyo moral e intelectual en forma incondicional.

De manera muy especial van mis sinceros reconocimientos a los señores Jurados por haber tenido el elevado criterio profesional para evaluar el presente trabajo y dictaminar positivamente, buscando siempre el desarrollo del conocimiento en nuestra Universidad.

RESUMEN

La presente investigación tiene como finalidad proponer una metodología de gestión en riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha.

De lo precedentemente anotado, la investigación refleja los cambios a nivel social y tecnológico que ha afectado al proceso evolutivo de la sociedad. De igual manera, la metodología de gestión propuesta en la presente investigación comprende un análisis de enfoques en los riesgos de ciberseguridad. A ello, se adiciona toda una información sobre indicadores de gestión a nivel de alta dirección, áreas funcionales y operativas, también comprende la aplicación práctica sobre los siete pasos de control de calidad para la solución de problemas.

Todo ello en conjunto e interactuando sinérgicamente debe brindar a la empresa un alto grado de eficacia a nivel de gestión con suficiente capacidad de respuesta de manera tal que le permita afrontar y adaptarse a los cambios del mundo actual inmerso en el proceso de la globalización.

PALABRAS CLAVES: Riesgos, ciberseguridad, prevención, fraudes.

SUMMARY

The purpose of this research is to propose a methodology for managing cybersecurity risks and their consequences in the prevention of fraud in industrial companies in the Yanacancha district.

From the foregoing, the research reflects the changes at a social and technological level that have affected the evolutionary process of society. In the same way, the management methodology proposed in this research includes an analysis of approaches to cybersecurity risks. To this, all information about management indicators at the level of senior management, functional and operational areas is added, it also includes the practical application on the seven steps of quality control for the solution of problems.

All this together and interacting synergistically must provide the company with a high level of efficiency at the management level with sufficient response capacity in a way that allows it to face and adapt to the changes of the current world immersed in the process of globalization.

KEY WORDS: Risks, cybersecurity, prevention, fraud.

INTRODUCCIÓN

En el mundo actual están presentándose cambios tan asombrosos y a tal velocidad de tiempo que sus implicaciones son inexorables para nuestra vida profesional y empresarial en el distrito de Yanacancha, transformaciones que no podían imaginarse hace unos cuantos años, meses o apenas semanas atrás están sucediendo de manera vertiginosa. En estos momentos se generan dichos cambios con tal grado de intensidad y fugacidad que verdaderamente enriquecen las oportunidades para la humanidad, los países, las organizaciones y para cada uno de nosotros.

Con relación al nuevo ambiente global, las empresas enfrentan una paradoja, tienen oportunidades nunca antes vistas para aprovechar los nuevos mercados, y entre tanto, los mercados tradicionales cambian de manera sustancial, reduciéndose o haciéndose intensamente competitivos. Además, los reducidos márgenes de beneficios, paralelos a las crecientes exigencias del cliente por productos y servicios de calidad, determinan presiones inexorables en muchas empresas.

Es por ello, que la presente investigación consciente de que vivimos en plena vorágine de los cambios en todo aspecto, tiene como finalidad trasladar información en base a la experiencia laboral, profesional y vivencial por los que me he desempeñado. Trasladar información teórico práctico para que traiga como resultado una investigación cuidadosa y lleve conocimiento a quienes lo lean y poder a quienes lo apliquen.

La estricta concordancia con el título de tesis y con la formulación de hipótesis planteada, la investigación realizada en esencia establece una

metodología de gestión para los riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha – Pasco 2016, puedan informarse, conocer y aplicar variables competitivas de gestión para su desarrollo empresarial los cuales permitirán adaptarse al presente tiempo caracterizado por la globalización y la competitividad en que vive la humanidad.

En tal sentido, para mejor apreciación y comprensión del desarrollo del presente trabajo de investigación está comprendido por los siguientes puntos:

Así tenemos en el primer capítulo: Problema de investigación, en ella tratamos, identificación y determinación del problema, delimitaciòn de la investigación, la formulación del problema, objetivos, justificación del estudio, y limitaciones de la investigación.

En el segundo capítulo: Marco teórico, comprende antecedentes de estudio, bases teóricas científicas, definición de términos básicos, formulación de hipótesis, identificación de variables y operacionalización de variable e indicadores.

Asimismo en el tercer capítulo: Metodología y técnicas de investigación, abarco, tipo de investigación, nivel de investigación, diseño de investigación, población y muestra, métodos de investigación, técnicas e instrumentos de recolección de datos, técnicas de procesamiento y análisis de datos y selección y validación de los instrumentos de investigación.

Finalmente, en el cuarto capítulo: Descripción del trabajo de campo, presentación, análisis e interpretación de resultados obtenidos en el trabajo

de campo, prueba de hipótesis y discusión de resultados. Concluyendo con las conclusiones y recomendaciones.

Espero que el aporte, contribuya a mejorar la labor de los profesionales inmersos en el tema de riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha, y sirva de punto de partida para otros trabajos; que contribuya a estudiantes y profesionales en la investigación.

INDICE

Pág.

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

CAPÍTULO IV

RESULTADOS Y DISCUSIÒN

CAPITULO I

PROBLEMA DE INVESTIGACIÓN

1.1 Identificación y planteamiento del problema.

Todos hemos sido testigos de que el Internet ha revolucionado la informática y las comunicaciones como ningún otro invento del siglo XX. La invención del telégrafo, teléfono, radio y finalmente el computador sentó las bases sin precedentes, para alcanzar esta integración de funcionalidades. Además, Internet es una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica. Internet representa uno de los ejemplos más exitosos de los beneficios de una inversión y un compromiso continuo en el campo de la investigación y el desarrollo de la infraestructura de la

información. INTERNET ha cambiado el mundo y nuestra sociedad. Ya hemos entrado en una nueva era, … La era digital.

INTERNET no tiene reglas ni límites, está creando nuevos paradigmas: ¡parece ser un “Far-west” en donde la única ley es la del más fuerte!

Han emergido nuevos:

- *Modos de consumo. - La interconexión de objetos a internet para obtener información en tiempo real, se ha comenzado a consolidar como una innovación en el mercado de consumo. La tendencia del internet de las cosas no sólo está en gadgets o dispositivos móviles, incluso hay casas, automóviles, lavadoras y refrigeradores conectados a internet que ayudan a simplificar las actividades del día a día.*
- *Conceptos económicos. - La INTERNET permite mejorar el nivel de vida de una población en concreto, y es tenida en cuenta como una variable de interés en los estudios de desarrollo económico, ya que el acceso a la información y la capacidad para transformarla permite a las personas mejorar sus capacidades personales y profesionales, así como en las empresas que hacen un buen uso de las TIC se experimentan notables mejoras de eficiencia.*
- *Modelo de negocios. -*
    - *Modelos de negocio basados en la publicidad.*
    - *Modelos de negocio basados en el comercio.*

- *Modelos de negocio basados en la intermediación.*
- *Otros Modelos de negocio basados en la prestación de servicios.*
- *Modelos de negocio basados en la Comunidad y el P2P.*
- *Otros modelos de negocio relacionados.*

Internet, está transformando y lo seguirá haciendo en el futuro, la dirección y organización de empresas y la competencia entre las mismas (Cohen, De Long, & Zysman, 2000). La economía digital está afectando a las empresas u organizaciones, a las decisiones de localización, tamaño, estructura organizativa y relaciones con otras empresas, a la estructura de los mercados, a los precios de los bienes y servicios y a las características del mercado laboral, entre otros (Haltiwanger & Jarmen, 2000).

Concretamente, se puede plantear el impacto de la economía digital en las empresas y en su entorno (general y específico) a partir del análisis de las características de la economía digital.

Nuevas maneras de trabajar … hacia una nueva economía digitalizada, desmaterializada

Los nuevos actores son empresas de intermediación que se interponen entre los profesionales y los consumidores, ofreciendo un servicio a ambas partes aprovechando la tecnología: las plataformas.

Las plataformas ponen en contacto oferta y demanda de servicios en la red, algo tan básico en una economía de mercado, han

proliferado en los últimos tiempos en internet y se han convertido en un importante nicho de negocio para los emprendedores. La ausencia de barreras geográficas y de tiempo para intercambiar, comprar o vender son la base de estas actividades que son impulsadas por el desarrollo de webs de intermediación en la que se encuentran las partes interesadas en ofrecer o demandar servicios.

Las webs de servicios mediante intermediación se han convertido en una fuente de desarrollo de negocios para numerosos emprendedores que lanzan start ups, empresas de base tecnológicas, dirigidas a sectores concretos de consumo.

Los nuevos paradigmas económicos son:

- *Acceso permanente.*
- *Disponibilidad total.*
- *Oferta ilimitada.*
- *Pago "on-line".*

Este mundo nuevo es muy atractivo, por un lado, pero... … conlleva sus peligros.

El conjunto de nueva tecnología es ofertado por pocos actores de Internet, tales como: Microsoft, IBM, Apple, Google, Amazon, Facebook los cuales nos han creado una vinculación de dependencia, concentrando de esa manera los riesgos.

Estos colosos han invertido miles de millones de dólares en centros de datos y hardware computacional para administrar sus propias

operaciones y, a la vez, proveer servicios gratuitos o a bajo costo a startups y muchas grandes corporaciones.

El mayor problema de Internet hoy en día es un problema de riesgos, falta seguridad, por lo que se requiere de !Ciberseguridad!.

1.2. Delimitación de la investigación.

Frente a la problemática planteada la investigación metodológicamente las he delimitado en los siguientes aspectos:

a) Delimitación espacial.

El presente trabajo de investigación abarco al distrito de Yanacancha.

b) Delimitación temporal.

Es una investigación de actualidad, el período que comprendió el estudio abarco el 2017, siendo el inicio del trabajo en agosto del 2017 y termino en enero del 2018.

c) Delimitación social.

Comprendió a las empresas industriales.

d) Delimitación conceptual.

En el manejo del material teórico-conceptual, estuvo comprendido en los alcances de los siguientes conceptos:

- **Riesgos de ciberseguridad.**

Deficiente control de acceso a las aplicaciones un 48% de los Participantes ha detectado que el acceso de los trabajadores a las Aplicaciones, en su compañía, tendría que estar más mejor Controlado.

Control de acceso a la red las empresas afirman estar en riesgo Debido a la falta de control de los accesos a la red corporativa Por parte de empleados y proveedores. Los filtros de informativos Sufren una gran vulnerabilidad, lo que provoca que el fraude y Robo de la información, sean mas comunes de lo que parece.

- **Prevención de fraudes.**
    - Para combatirlo de manera adecuada es imprescindible que las compañías cuenten con un marco de integridad del negocio y de cumplimiento normativo el cual les permitirá:
    - Comprender los riesgos del fraude
    - Reducir la exposición ante las obligaciones corporativas, las sanciones y los litigios
    - Obtener un verdadero valor de las compañías en materia de cumplimiento
    - Alcanzar los altos niveles de integridad empresarial mediante solidas practicas de gobierno corporativo, control interno y transparencia
    - Evaluar si los controles antifraude son realmente efectivos

1.3. Formulación del problema.

1.3.1. Problema principal.

¿De qué manera los riesgos de ciberseguridad tienen consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha?

1.3.2. Problemas específicos.

a. ¿De qué manera el diseño y aplicación de las normas de la economía digital influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha?

b. ¿De qué manera el conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de fraudes en las empresas industriales del distrito de Yanacancha?

c. ¿De qué manera la realización de una evaluación de riesgos influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha?

1.4. Formulación de objetivos.

1.4.1. Objetivos generales.

Conocer de qué manera los riesgos de ciberseguridad tienen consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha.

1.4.2 Objetivos específicos.

a. Conocer de qué manera el diseño y aplicación de las normas de la economía digital influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha.

b. Conocer de qué manera el conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de fraudes en las empresas industriales del distrito de Yanacancha.

c. Conocer de qué manera la realización de una evaluación de riesgos influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha.

1.5. Justificación de la investigación.

Esta investigación es importante porque una cuestión de gestión de riesgos de información en las empresas requiere el adecuado equilibrio de compensación y mitigación de los controles. Los auditores de tecnología de información, así como los gerentes financieros que interactúan con ellos (por ejemplo: directores financieros, contralores, contadores públicos, auditores internos, gerentes de línea de negocio) continúan dedicando mucha atención a los riesgos que conlleva de seguridad cibernética. Pese a que muchos de los componentes que originan riesgos de seguridad cibernética se inician con la tecnología, estos ejecutivos y otros interesados (incluyendo clientes, entidades reguladoras, inversores, empleados, y financieros) reconocen que estos riesgos deben ser manejados como parte de la estrategia de negocio, en lugar de

tratarlos únicamente como cuestiones de tecnología, por lo de la participación de los ejecutivos y contadores se hace más necesario.

1.6. Limitaciones de la investigación.

Por el momento las únicas limitaciones que se presentaron, se encuentran referidas al acopio de material bibliográfico; poca bibliografía sobre riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales, sin embargo, no constituyen impedimento que afecten su desarrollo. Por otro lado, los gastos económicos que va generando el presente estudio.

CAPITULO II

MARCO TEORICO

2.1. Antecedentes de estudio.

Respecto al tema específico materia de investigación elegida, no se han encontrado antecedentes al respecto específicamente para el distrito de Yanacancha. Por lo que, considero inédita la presente investigación. Cabe aclarar que se ha recurrido a las bibliotecas de la Facultad de Ciencias Económicas y Contables y otros centros de información donde no existe bibliografía suficiente al respecto.

2.2. Bases teóricas científicas relacionadas.

2.2.1 Ciberseguridad

ISACA define la Ciberseguridad como la “Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se

procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados".

Una definición más amplia es dada por la Unión Internacional de Telecomunicaciones como:

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- *Disponibilidad;*
- *Integridad, que puede incluir la autenticidad y el no repudio;*
- *Confidencialidad.*

Las infraestructuras críticas de nuestro país se encuentran agrupadas en los siguientes 12 sectores: administración, alimentación, energía, espacio, sistema financiero y tributario, agua, industria nuclear, industria química, instalaciones de investigación, salud, transporte y tecnologías de la información y las comunicaciones. En cualquiera de estos sectores, el grado de penetración del ciberespacio, tanto para la gestión interna como para la provisión de servicios, alcanzó su grado crítico ya hace tiempo. Cualquier contingencia que pudiese afectar a alguno de los activos pertenecientes a cualquiera de los 12 sectores estratégicos podría comprometer la seguridad nacional.

Activo de Información es todo aquello que posea valor para la organización. Por tanto debe protegerse. Ejemplo:

- *Información física y digital.*
- *Software hardware.*
- *Servicios de información.*
- *Servicios de comunicaciones.*
- *Servicios de almacenamiento.*
- *Personas.*
- *Imagen.*

En tanto que los sistemas de Información establecen las aplicaciones, servicios, activos, etc. y utiliza otros elementos que faciliten el manejo de la información.

Debe tomarse medidas de protección de la información contra una gran variedad de amenazas con el fin de asegurar:

- *Continuidad del negocio,*
- *Minimizar el riesgo; y,*
- *Maximizar el retorno de inversiones y oportunidades de negocio.*

Existen documentos que apoyan la necesidad de que los auditores de TI apliquen sus conocimientos para gestionar y comunicar los riesgos tecnológicos.

Las nuevas amenazas incluyen:

- *El uso de funciones automatizadas permite incurrir en mayores pérdidas en un corto periodo de tiempo,*
- *Dependencia de terceros para salvaguardar los datos (cliente o empresa) y su reputación,*
- *Evolución de las estrategias de seguros que permitan ayudar los riesgos de transferencia.*

Los riesgos de Ciberseguridad deben ser consideradas en términos de:

- *Tecnología,*
- *Objetivos del Negocio (incluyendo finanzas, a prestación de servicios, adquisición de clientes y relaciones), y*
- *Fraude;*

La gestión de riesgos de ciberseguridad debe responder a las siguientes preguntas:

- *¿Cómo la tecnología facilita la consecución de sus objetivos de negocio?*
- *¿Cuál es su tolerancia para sufrir pérdidas relacionadas con la tecnología?*

Con la finalidad de asignar fondos y tiempo de gestión para mitigar el riesgo.

Los gerentes y auditores deben entender a qué amenazas que se enfrentan y qué costos en que se incurrirá para poder minimizarlas.

El auditor debe tener presente el triángulo del fraude (Figura 1):

- *Donde Incentivo/Presión representa las posibilidades de beneficios propios o presión externa a la realización del fraude.*
- *Racionalización/Actitud es el factor subjetivo, responsabilidad, ética del empleado*
- *Oportunidad por la parte de controles en el proceso o concentración indebida de funciones.*

Figura 1 Triangulo del Fraude

La gran mayoría de las grandes empresas disponen de una organización interna suficientemente madura que les permite implementar las actividades y medidas que se enmarcan dentro de las prácticas de “information security e information assurance.” En el caso de las pequeñas y medianas empresas (el 99% del total), la falta de recursos económicos y humanos impiden la implementación de ciberseguridad aunque sus actividades se sustentan, fundamentalmente, en las TIC. El Perú no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad.

Cuadro 1 Elementos fundamentales de la Ciberseguridad

Capacidad de un sistema para	Objetivos de la seguridad	Medios de seguridad
Poder utilizarse	• Disponibilidad	• Dimensionamiento
	• Perdurabilidad	• Redundancia
	• Continuidad	• Procedimientos de explotación y copia de seguridad
	• Confianza	
Ejecutar acciones	• Seguridad de funcionamiento	• Concepción
	• Fiabilidad	• Prestaciones
	• Perdurabilidad	• Ergonomía
	• Continuidad	• Calidad de servicio
	• Exactitud	• Mantenimiento operacional
Permitir el acceso de entidades autorizadas (Ningún acceso ilícito)	• Confidencialidad (preservación del secreto)	• Control de acceso
		• Autenticación
		• Control de errores
	• Integridad (ninguna modificación)	• Control de coherencia
		• Encriptación
Demostrar las acciones	• No rechazo	• Certificación
	• Autenticidad (ninguna duda)	• Grabación, rastreo
	• Ninguna contestación	• Firma electrónica
		• Mecanismos de prueba

Tomado de (Guía de ciberseguridad para los países en desarrollo, 2007)

2.2.2 Riesgos multidimensionales.

En general, la evolución de la tecnología y el aumento de la dependencia de las empresas a dicha tecnología impulsa a esta preocupación. A pesar de los giros modernos y lenguaje técnico empleado en la definición del problema de los riesgos tecnológicos, los riesgos de seguridad cibernética son algo similares a los riesgos de negocio tradicionales que enfrentan las organizaciones en el mundo pre-automatizado de pre-Internet. Las responsabilidades de la custodia de los activos, la autorización de las transacciones, y registros de actividades se han utilizado tradicionalmente para asegurar que la información utilizada y reportado por la empresa era válida, completa y precisa. Lo mismo sucede en un entorno electrónico; las amenazas específicas a ese entorno, son diferentes y requieren una adaptación de las estrategias tradicionales de control interno. Estas amenazas pueden incluir a las siguientes:

a. *El uso de funciones automatizadas permite incurrir en mayores pérdidas en un corto periodo de tiempo,*
b. *Dependencia de terceros para salvaguardar los datos (cliente o empresa) y su reputación,*
c. *Evolución de las estrategias de seguros que permitan ayudar los riesgo de transferencia,*

Desafortunadamente, para muchos ejecutivos financieros y comités de auditoría, las herramientas utilizadas para comunicar los riesgos de seguridad cibernética y estrategias de mitigación del riesgo con las partes interesadas no son tan maduros y bien comprendidos. Así por ejemplo el COSO publicó un documento de reflexión para proporcionar orientación sobre cómo el Control Interno - Marco Integrado (2013) y la gestión del riesgo empresarial - Marco Integrado (2004) pueden ayudar a las organizaciones con eficacia y eficiencia evaluar y gestionar el ciberriesgo (Mary E. Galligan y Kelly Rau, "COSO en la era cibernética", una investigación encargada por COSO y escrito por Deloitte, 2015, http://bit.ly/1XjhIL0). El documento de reflexión indicado sentó las bases para mirar a la ciberseguridad como una cuestión de gestión de riesgos que requiere el adecuado equilibrio de compensación y mitigación de los controles. Los beneficios de usar el enfoque COSO incluyen objetivos, asunto de comunicación, tolerancia al riesgo, análisis de las deficiencias, y priorización en la corrección.

Los riesgos de seguridad cibernética y muchos de los controles basados en la tecnología utilizada para mitigar estos riesgos se deben traducir en un lenguaje que puede ser fácilmente entendido por los encargados del gobierno y de los objetivos de negocio en su implementación y gestión. Sin

embargo, los delitos informáticos también tienen que ser reconocidos por lo que realmente corresponden: un tipo de fraude. De acuerdo con gestión del riesgo empresarial de fraude: Una guía práctica, el fraude es "todo acto u omisión intencional diseñada para engañar a los demás, lo que resulta en la víctima sufre una pérdida y el autor lograr una ganancia" (IIA, AICPA y ACFE 2008, http://bit.ly/23eKbIR). Sobre la base de esta definición, los riesgos ciberseguridad deben ser considerados en términos de tecnología, objetivos de negocios (incluyendo finanzas, a prestación de servicios, adquisición de clientes y relaciones), y el fraude; sin embargo, muchas evaluaciones continúan realizándose sólo para examinar e informar sobre las amenazas de ciberseguridad como si fueran una sola dimensión.

2.2.3. Realización de una evaluación de riesgos.

La primera y más importante estrategia en la gestión de riesgos ciberseguridad es asegurar que la organización entiende perfectamente cómo la tecnología facilita la consecución de sus objetivos de negocio y cuál es su tolerancia para sufrir pérdidas relacionadas con la tecnología. Para de esta manera asignar correctamente los fondos y el tiempo de gestión para mitigar el riesgo. Los ejecutivos y los miembros de la junta deben entender plenamente las amenazas que enfrentan y los costos en que se incurrirá.

Algunas empresas ya están obligadas a cumplir con los requisitos establecidos. Por ejemplo, En el caso de que las pequeñas empresas acepten pagos con tarjeta de crédito deben cumplir con un protocolo de seguridad, así como los proveedores de salud, incluyendo los médicos y sus proveedores de servicios

La mayor parte de los requisitos normativos identificados anteriormente requieren que se realice una evaluación del riesgo. Aunque los procedimientos específicos no siempre se dan, la intención es proporcionar un mecanismo para que el negocio de auto-evaluar sus estrategias de mitigación de riesgos. Por lo general, estas evaluaciones se llevan a cabo en contra de un marco reconocido que permite a la organización demostrar la debida diligencia adecuada en caso de necesidad (por ejemplo, demanda o solicitud de regulación).

Los miembros del comité de auditoría pueden determinar la calidad de las evaluaciones de riesgos realizadas por la administración al considerar las cuestiones identificadas por las evaluaciones. La probabilidad de no identificar cualquier problema es muy remota, y dicho incumplimiento debe poner en tela de juicio la calidad y utilidad de la evaluación en sí. El informe resultante de la evaluación de riesgos facilitará la discusión entre los miembros del comité de auditoría. Se podría incorporar factores tales como la dependencia de cada etapa

del ciclo económico en la tecnología, la presencia de datos propietarios, la normativa aplicable, así como la suficiencia de las prácticas de riesgo actuales. El Cuadro 1 muestra un informe de ejemplo.

CUADRO 1

Traslación de controles de seguridad críticos (CSC) en Temas de Negocio

Control	Preguntas de Gestión de Negocios	Brechas Identificadas	Riesgo residual	Fecha Planeada de la reparación
CSC1 -Inventario de	¿A cuanto asciende el presupuesto de TI?	Necesita un software para controlar los cambios		El software será incluida en la solicitud
	¿Podemos reconciliar el inventario con el registro contable?	El proceso del control de cambios necesita ser mejorada		de presupuesto del próximo año. En
los equipos y el	¿Hemos asignado responsabilidades de custodia?		Alto	tanto que el proceso de control de
software				cambio deberá ser remediado antes del final del 3er trimestre.
CSC2- Inventario de	¿Tenemos la "mezcla perfecta" de licencias?	Necesita herramienta de seguimiento para supervisar		Los elementos de acción serán diferidos
				para el próximo año, cuando vamos a
				contratar a un consultor calificado para
				revisar las estrategias y monitoreo de
Software empleado		las licencias de software.		licencias generales.
	¿Podríamos ser demandados?	Necesidad de conciliar los pagos a los vendedores al software existente.	Medio	
	¿Sabemos lo que se está ejecutando en nuestros	Necesidad de mejorar los controles sobre el software		Las configuraciones se cambiarán para
				prohibir que los usuarios finales
				puedan instalar software en sus
				computadoras para el final del
en la entidad	sistemas?	de escritorio y los riesgos relacionados		trimestre actual
CSC3-	¿Cómo determinamos que hemos configurado	Las estrategias de configuración deben		Configuraciones estándares de
				configuración se desarrollarán el
				próximo trimestre.Debido al
	conseguridad?	ser desarrollados y estandarizados.		impacto potencial sobre los sistemas
	¿Revisa a alguien lo que se configura?	Se necesita de una herramienta automatizada		La disponibilidad y la
Configuraciones			Medio	implementación será gradual a lo
				largo de un período de un año en base
		para vigilar el cumplimiento de la política necesaria.		a los datos de clasificación de riesgo.
	¿Cómo nos comparamos contra las	Necesidad de procesos de excepción		Plan de proyecto de alto nivel será
	prácticas externas (por ejemplo, buenas prácticas,			proporcionado en la reunión de
Seguras	etc.)?			comité próxima auditoría
CSC4-	Lo que es aceptable y lo que no lo es?	prácticas de la vulnerabilidad de remediación violan		consultores operativo de seguridad
		las políticas establecidas de manera significativa.		participarán en este trimestre para
	Son las vulnerabilidades indicativo de otros	Sólo el 40% de los activos de garantía se escanean.	Alto	ayudar a identificar los cuellos de
				botella y debilidades en los procesos
vulnerabilidades	problemas?			actuales.
CSC5- Privilegios	¿Limitamos el acceso sólo a la base de dato que se requiere tener?	Todas las prácticas se ajustan a las expectativas y las políticas actuales.	Bajo	No se requiere accion.
	¿Estamos haciendo cumplir la segregación de responsabilidades?			
	¿Tenemos pistas de auditoría para mantener			
Administrativos	actualizados?			

Para asegurar una adecuada consideración de las amenazas, los ejecutivos financieros pueden optar por aprovechar el triángulo del fraude tradicional (Ver figura 1) (y derivados relacionados). Estas herramientas ayudan a identificar fuentes

potenciales de amenazas por una mejor comprensión de la motivación y la racionalización detrás de fraude. Siendo realistas, sin embargo, la implementación de prácticas que puede reducir la posibilidad de que los atacantes a menudo es la única parte del triángulo del fraude que los ejecutivos financieros pueden administrar, supervisar e informar.

2.2.4. Protección de los activos digitales.

La responsabilidad de proteger los activos digitales y la lucha contra las amenazas de ciberseguridad se distribuye entre varios individuos dentro de la organización e incluso fuera de los proveedores de servicios (aunque la rendición de cuentas, especialmente en lo que se refiere a la protección de la información del cliente, no puede ser compartida con otros o asignado a una tercera fiesta).

Esta distribución de responsabilidades puede causar problemas para un comité de auditoría para determinar la responsabilidad por las acciones correctivas y asegurar que el entorno de una organización se prueba suficiente y apropiadamente. El Cuadro N° 2 muestra varios aspectos del riesgo de la seguridad cibernética (que varía según la organización), para ello se ha utilizado colores para resaltar los problemas y el servicio responsable de la verificación.

2.2.5 Escogiendo que proteger.

Proteger todas las áreas de la organización es demasiado oneroso para la organización, para ser considerada como práctica común. Por lo tanto, una adecuada identificación y gestión de amenazas y asegurar que los riesgos asociados a estas amenazas se gestionan de acuerdo con los objetivos de negocio de la organización y las tolerancias al riesgo es la clave.

Algunos comités de auditoría continúan siendo cuestionados por la naturaleza técnica de los controles de seguridad crítica y usar esto para excusar no cuestionar la gestión como en la medida en que se han implementado los controles y están funcionando. Cada uno de los cinco primeros controles, sin embargo, pueden traducirse en problemas de negocio que los miembros del comité de auditoría y ejecutivos financieros están muy a gusto con lo que confirma que, además, en su núcleo, los controles de seguridad cibernética son controles fundamentales de gestión empresarial. Anexo 1 ilustra la relación entre los controles, las posibles preguntas de la administración, las carencias actuales, el nivel general de riesgo residual y la fecha prevista de remediación, proporcionando una herramienta para gobernar la seguridad cibernética y reducir al mínimo la jerga técnica.

¿Quién es el responsable por la Ciberseguridad?

El director financiero fue más a menudo identificado como la posición dentro de la organización responsable de la seguridad cibernética (38%), seguido por el Director de Informática en el 36%. (Ver Figura N°2.)

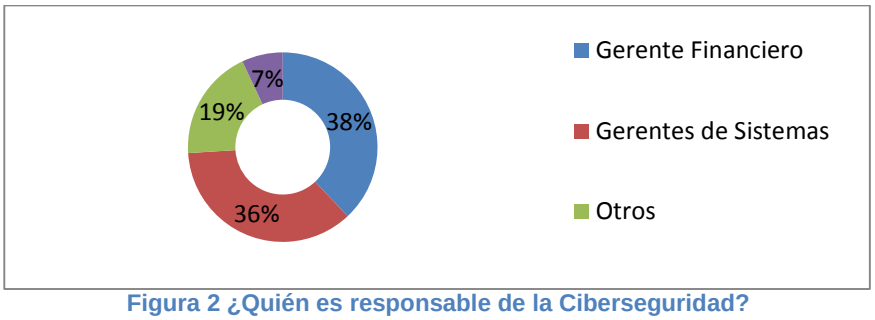


Figura 2 ¿Quién es responsable de la Ciberseguridad?

Estas respuestas muestran que los directores financieros son cada vez más identificados como los defensores de la estratégica e implementación de medidas de seguridad cibernética de sus organizaciones – este cambio se debe a su posición de visibilidad interna y externa con sus organizaciones.

¿Quién está más involucrado en iniciativas de seguridad cibernética?

En la gran mayoría de las organizaciones, el departamento de TI está más involucrado con la seguridad informática (95%), seguido de las finanzas (63%) y legal (34%). (Ver Figura N°3.)

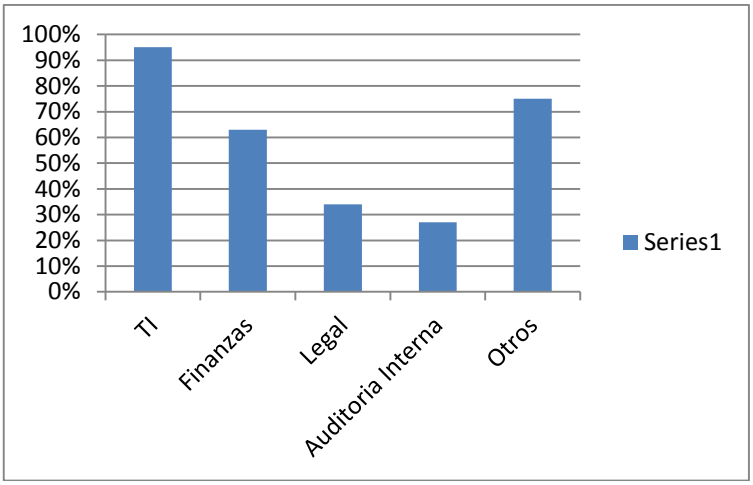


Figura 3 Oficinas involucradas en iniciativas de seguridad cibernética

Más de tres cuartas partes (76%) de los encuestados indican que más de un departamento está involucrado. Las tres cuartas partes seleccionadas "otro" y citan la participación de los papeles dispares, incluyendo recursos humanos, operaciones, dirección general, Dirección de riesgos y otros.

CUADRO 2

Asignación de Responsabilidades de Riesgos

	Márketing	CIO	Oficial de Seguridad de Información	Usuario	Vendedor	Auditoría interna
Web	X			X	X	?
Routers		X	X			?
Firewalls		X	X			?
Servers		X	X		X	?
Desktop	X	X		X	X	?
Core Applica	X	X	X	X	?	
Cloud	X		X	X	X	?
Mobile		X	X	X	X	?
Testing			X			X

2.3. Definición de términos básicos.

Auditoría de tecnologías de información.

La Auditoria de las tecnologías de información, mejor conocida como “Auditoria de TI” o “Auditoria informática” es una actividad de control Que comprende la evaluación de las tecnologías de Información (TI)

Así como de las tecnologías de la Información (SI) dentro de una Organización.

Permite contar con una evaluación objetiva e independiente respecto

A los procesos, servicios, aplicaciones, infraestructura e información Identificado los principales riesgos de negocio relacionado con la TI,

Resultado de posibles debilidades de control

Ciberseguridad.

La ciberseguridad busca proteger la información digital en los Sistemas interconectados. Está comprendida dentro de la Seguridad de la información**.**

Fraude

Es un delito cometido por el encargado de vigilar la ejecución De contratos ya sean públicos o privados, para representar Intereses opuestos. El fraude, por lo tanto, este penado por la Ley.

Nos encontramos con el hecho de que existen múltiples tipos de Fraude. Así entre los mismos se hallan los pagos de sueldos a Personal que no trabaja, la anulación de facturas que han sido Cobradas, la doble facturación, los pasivos registrados sin Documentación soporte, las ventas de servicios que no son Declarados impuestos o los sueldos pagados a personas que no Existen.

Prevención de fraudes.

La prevención es toda medida tendiente a atacar los factores Causales del crimen, incluidas las oportunidades para la Comisión de conductas delictivas y contra productivas.

Realizar una evaluación periódica de la exposición al riego fraude, Con el fin de identificar potenciales actuaciones y fraudes Específicos que la organización necesita mitigar.

Implantar técnicas de prevención que eviten en la medida de lo Posible, posibles fraudes y mitiguen los impactos en la organización Tanto economicos como reputacionales).

2.4. Formulación de hipótesis.

2.4.1 Formulación de hipótesis general.

Los riesgos de ciberseguridad tienen consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha.

2.4.2 Formulación de hipótesis específicos.

a. El diseño y aplicación de las normas de la economía digital influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha.

b. El conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de fraudes en las empresas industriales del distrito de Yanacancha.

c. La realización de una evaluación de riesgos influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha.

2.5. Identificación de variables.

Variable independiente.

Riesgos de ciberseguridad.

Variable dependiente.

Prevención de fraudes.

2.6 Definición operacional de variables e indicadores.

Variable independiente.

X Riesgos de ciberseguridad.

Indicadores.

X_1 Diseño y aplicación de normas.

X_2 Conocimiento de componentes.

X_3 Evaluación de riesgos.

X_4 Clasificación de riesgos cibernéticos.

X_5 Tipos de riesgos cibernéticos.

X_6 Control de riesgos.

X_7 Planes de contingencia.

Variable dependiente.

Y Prevención de fraudes.

Indicadores

Y_1 Mitigación sectorial.

Y_2 Minimización integral.

Y_3 Controles de seguridad.

Y_4 Definición de estrategias.

Y_5 Pruebas de vulnerabilidad.

Y_6 Habilidades de gestión.

Y_7 Experiencia profesional.

CAPITULO III

METODOLOGIA Y TECNICAS DE INVESTIGACIÓN

3.1. Tipo de investigación.

El tipo de investigación será descriptivo porque se someterá a un análisis en el que se mide y evalúa diversos aspectos o componentes tales como cuerpos legales y normativas vigentes del problema a investigar.

El tipo de investigación será explicativa porque se explicará cómo ocurre un fenómeno (mejorar la competitividad) y en qué condiciones se da éste. Dado que la naturaleza de la investigación es explicativa surge la necesidad de plantear una investigación correlacional que consiste en evaluar el grado de relación entre dos variables. Es explicativa porque se dará a conocer las definiciones y conceptos legales y técnicos referentes al sistema de control.

3.2. Método de la investigación.

En la presente investigación, se empleó el método descriptivo en su modalidad de estudios correlacionales

3.3. Diseño de investigación.

Se tomo una muestra en la cual:

M = Ox r Oy

Donde:

M = Trabajadores.

O = Observación.

X = Riesgos de ciberseguridad.

Y = Prevención de fraudes.

R = Relación de variables

3.4. Población y muestra.

3.4.1. Población.

La población estará constituida por 325 representantes y trabajadores de las empresas industriales del distrito de Yanacancha.

3.4.2. Muestra.

Para el cálculo del tamaño de la muestra se utilizó el muestreo aleatorio simple a través de la siguiente fórmula:

$$n = \frac{Z^2 N pq}{E^2 (N-1) + Z^2 pq}$$

Donde:

n = Tamaño de la muestra

N = Población (325)

Z = Nivel de confianza (1.96)

p = Tasa de prevalencia de objeto estudiado

(0.50)

q = (1-p) = 0.50

E = Error de precisión 0.05

Entonces:

$$n = \frac{(1.96)^2 \ (325) \ (0.50) \ (0.50)}{(0.05)^2 \ (325 - 1) + (1.96)^2 \ (0.50) \ (0.50)}$$

$$n = \frac{312.13}{0{,}81 + 0.9604}$$

$$n = \frac{312.13}{1.7704}$$

$$n = 176$$

3.5. Técnicas e instrumentos de recolección de datos.

Técnicas

Las principales técnicas que se utilizó en este estudio fueron la encuesta y el análisis documental.

Instrumentos

Se empleo básicamente el cuestionario y la guía de análisis documental. Del mismo modo el software estadístico SPSS 23 para poder sistematizar todos los datos registrados.

3.6. Técnicas de procesamiento y análisis de datos.

Después de haber realizado la recolección de datos empíricos, se han utilizado las principales técnicas de procesamiento

y análisis de datos como las siguientes: Codificación, tabulación y elaboración complementariamente con cuadros estadísticos para el análisis e interpretación de las variables en estudio y luego describir, predecir y explicar con imparcialidad la información obtenida y de esta manera llevar a conclusiones y recomendaciones, para los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, relacionados al tema de investigación, como resultado y cumplimiento de los objetivos propuestos y respuestas reales a los problemas planteados, sobre la base de los resultados obtenidos, las mismas que aparecen en el capítulo IV del presente trabajo.

3.7 Tratamiento estadístico.

Para contrastar las hipótesis se usó la distribución ji cuadrada puesto que los datos disponibles para el análisis están distribuidos en frecuencias absolutas o frecuencias observadas. La estadística ji cuadrada es más adecuada para esta investigación porque las variables son cualitativas.

3.8 Selección y validación de los instrumentos de investigación.

Se realizo la validez y confiabilidad del cuestionario por juicio de expertos mediante la Prueba de Chi Cuadrado, determinando la validez del cuestionario, para ello se contó con el juicio de expertos acerca del cuestionario.

CAPITULO IV

RESULTADOS Y DISCUSIÒN

4.1 Descripción del trabajo de campo.

Antes de ejecutar la aplicación de las técnicas e instrumentos de recolección de datos, primero hemos procedido a la elaboración de los instrumentos de recolección de información para luego validar adecuadamente conforme los procedimientos que exige un trabajo de investigación rigurosa e imparcial, que conduce a la demostración de las hipótesis, en cumplimiento a los objetivos del presente trabajo; por lo que detallamos metodológicamente el trabajo desarrollado:

1) Se han elaborado previamente los instrumentos de recolección de datos para la aplicación de la encuesta a los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, integrantes de la muestra, para posteriormente validarlos.

2) Luego, se ha aplicado una “Prueba Piloto” con los instrumentos previamente elaborados, con el objetivo de realizar algunas correcciones pertinentes si hubiera dicha necesidad y así como poder calcular el tiempo necesario que se requiere para la aplicación y recopilación de las respuestas entre el primero y el último que entrega la encuesta, para lo cual se ha tomado el 10 por ciento del total de la muestra.

3) De igual manera, se han convocado a una entrevista no estructurada a los integrantes de la muestra representativa, tomando como base sólo el 10 por ciento del total de la muestra con la finalidad de recibir algunas sugerencias o dificultades que hubiera en el instrumento de recolección de datos, con la finalidad de evitar posteriores errores en la captación de la información.

En el trabajo de campo, después de validar los instrumentos se han realizado con toda normalidad la encuesta, logrando con éxito todo lo planificado para cumplir con los objetivos de la investigación, permitiendo realizar la aplicación de los siguientes instrumentos previstos para el presente trabajo:

1. **El cuestionario.** Fueron aplicados a los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, mediante preguntas lógicamente agrupadas, para garantizar la imparcialidad de los informantes y de los datos empíricos en estudio, del total de los integrantes de la muestra y establecida dentro del universo de la presente investigación.

2. **Guía de análisis documental.** Se han registrado algunos datos indispensables relacionados con las variables e indicadores en estudio, con la finalidad de reforzar y garantizar la imparcialidad de los datos registrados en el instrumento anterior aplicados en la presente investigación. Las técnicas e instrumentos seleccionados en la presente investigación, fueron elegidos teniendo en cuenta el método de investigación utilizada en el presente trabajo.

4.2 Presentación, análisis e interpretación de resultados obtenidos en el trabajo de campo.

Este capítulo tiene el propósito de presentar el proceso que conduce a la demostración de la hipótesis en la investigación “RIESGOS DE CIBERSEGURIDAD Y SUS CONSECUENCIAS EN LA PREVENCIÓN DE FRAUDES EN LAS EMPRESAS INDUSTRIALES DEL DISTRITO DE YANACANCHA – PASCO 2016”.

Este capítulo comprende el cumplimiento de los siguientes objetivos:

a. Conocer de qué manera el diseño y aplicación de las normas de la economía digital influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha.

b. Conocer de qué manera el conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de

fraudes en las empresas industriales del distrito de Yanacancha.

c. Conocer de qué manera la realización de una evaluación de riesgos influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha.

Los logros obtenidos en el desarrollo de cada objetivo específico, nos conducen al cumplimiento del objetivo general de la investigación; ya que cada objetivo específico constituye un sub capítulo de este análisis y consecuentemente nos permitirá contrastar la hipótesis de trabajo para aceptarla o rechazarla con un alto grado de significación.

RIESGOS DE CIBERSEGURIDAD

4.2.1 Conocimiento del diseño y aplicación de normas.

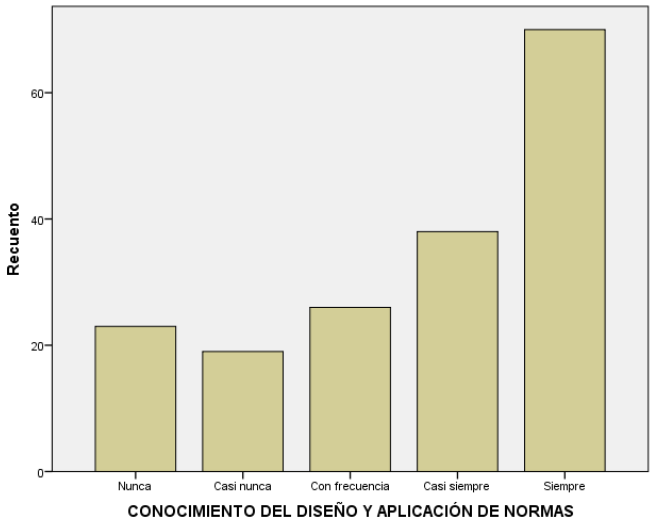
A la pregunta: ¿Es importante el conocimiento del diseño y aplicación de normas relacionadas a la ciberseguridad?

CUADRO Nº 01

CONOCIMIENTO DEL DISEÑO Y APLICACIÓN DE NORMAS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	23	13,1	13,1	13,1
	Casi nunca	19	10,8	10,8	23,9
	Con frecuencia	26	14,8	14,8	38,6
	Casi siempre	38	21,6	21,6	60,2
	Siempre	70	39,8	39,8	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 01



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 40% respondieron siempre es importante el conocimiento del diseño y aplicación de normas relacionadas a la ciberseguridad, 22% casi siempre, 15% con frecuencia, 11% casi nunca y 13% nunca.

4.2.2 Conocimiento de los componentes.

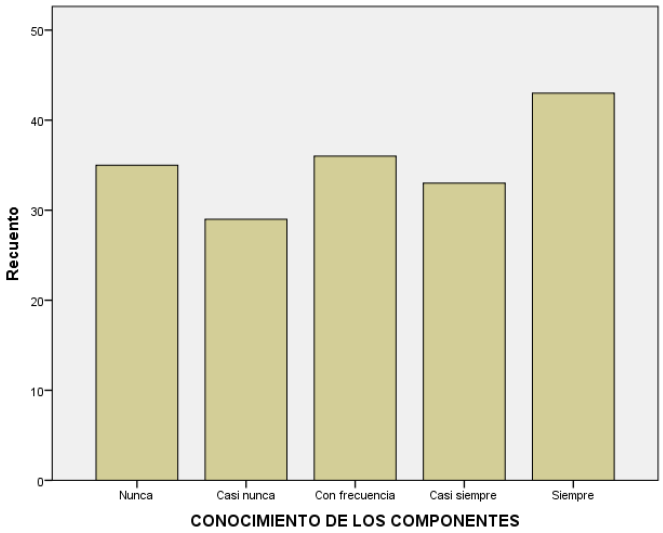
A la pregunta ¿Se tiene conocimiento de los componentes relacionados a la ciberseguridad?

CUADRO Nº 02

CONOCIMIENTO DE LOS COMPONENTES

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	35	19,9	19,9	19,9
	Casi nunca	29	16,5	16,5	36,4
	Con frecuencia	36	20,5	20,5	56,8
	Casi siempre	33	18,8	18,8	75,6
	Siempre	43	24,4	24,4	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 02



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 24% respondieron siempre se tiene conocimiento de los componentes relacionados a la ciberseguridad, 19% casi siempre, 21% con frecuencia, 17% casi nunca y 20% nunca.

4.2.3 Evaluación de riesgos.

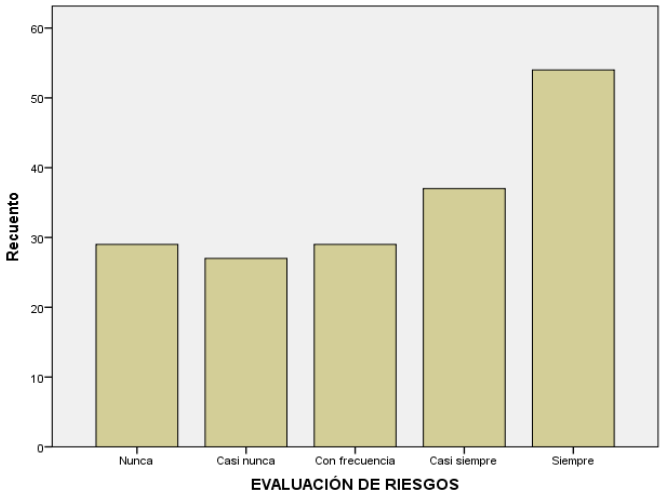
A la pregunta ¿Se vienen desarrollando evaluación de riesgos en cada una de las áreas de la empresa?

CUADRO Nº 03

EVALUACIÓN DE RIESGOS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	29	16,5	16,5	16,5
	Casi nunca	27	15,3	15,3	31,8
	Con frecuencia	29	16,5	16,5	48,3
	Casi siempre	37	21,0	21,0	69,3
	Siempre	54	30,7	30,7	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 03



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 31% respondieron siempre se vienen desarrollando evaluación de riesgos en cada una de las áreas de la empresa, 21 casi siempre, 17% con frecuencia, 15% casi nunca y 17% nunca.

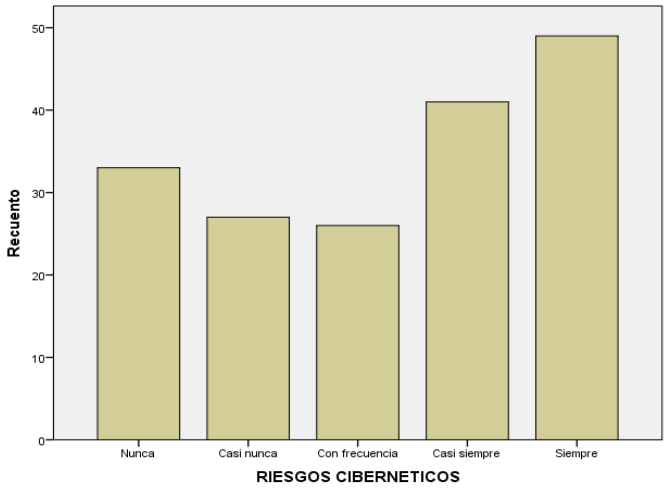
4.2.4 Clasificación de los riesgos cibernéticos.

A la pregunta ¿Se vienen clasificando los riesgos cibernéticos en la gestión de la empresa?

CUADRO Nº 04
RIESGOS CIBERNETICOS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	33	18,8	18,8	18,8
	Casi nunca	27	15,3	15,3	34,1
	Con frecuencia	26	14,8	14,8	48,9
	Casi siempre	41	23,3	23,3	72,2
	Siempre	49	27,8	27,8	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 04



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 28% respondieron siempre se vienen clasificando los riesgos cibernéticos en la gestión de la empresa, 23% casi siempre, 15% con frecuencia, 15% casi nunca y 19% nunca.

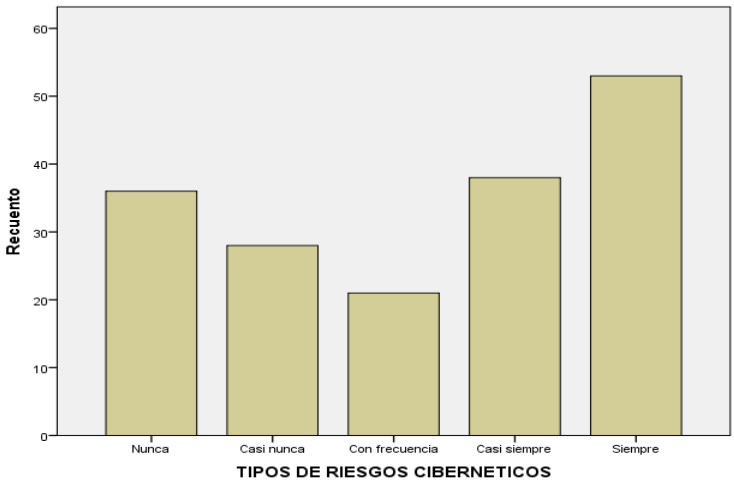
4.2.5 Tipos de riesgos cibernéticos.

A la pregunta ¿Se vienen identificando los tipos de riesgos cibernéticos en la empresa?

CUADRO Nº 05
TIPOS DE RIESGOS CIBERNETICOS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	36	20,5	20,5	20,5
	Casi nunca	28	15,9	15,9	36,4
	Con frecuencia	21	11,9	11,9	48,3
	Casi siempre	38	21,6	21,6	69,9
	Siempre	53	30,1	30,1	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 05



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 30% respondieron siempre se vienen identificando los tipos de riesgos cibernéticos en la empresa, 22% casi siempre, 12% con frecuencia, 16% casi nunca y 21% nunca.

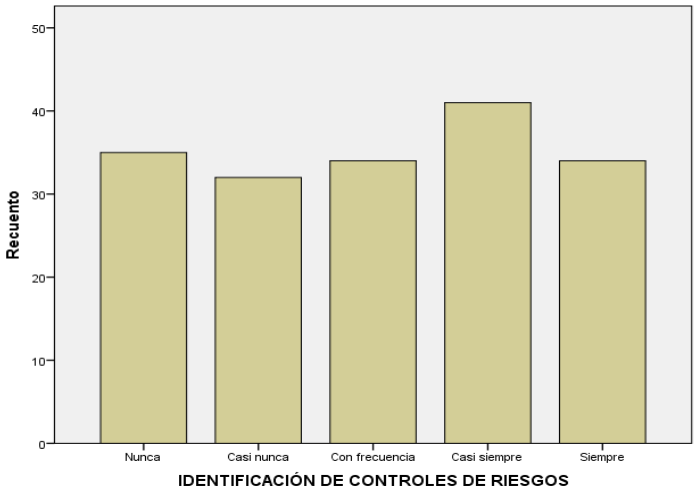
4.2.6 Identificación de controles de riesgos.

A la pregunta: ¿Se tiene identificado los controles de riesgo en la empresa donde labora?

CUADRO Nº 06
IDENTIFICACIÓN DE CONTROLES DE RIESGOS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	35	19,9	19,9	19,9
	Casi nunca	32	18,2	18,2	38,1
	Con frecuencia	34	19,3	19,3	57,4
	Casi siempre	41	23,3	23,3	80,7
	Siempre	34	19,3	19,3	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 06



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, 19% respondieron siempre, y en su mayoría 23% respondieron casi siempre se tiene identificado los controles de riesgo en la empresa donde labora, 19% con frecuencia, 18% casi nunca y 20% nunca.

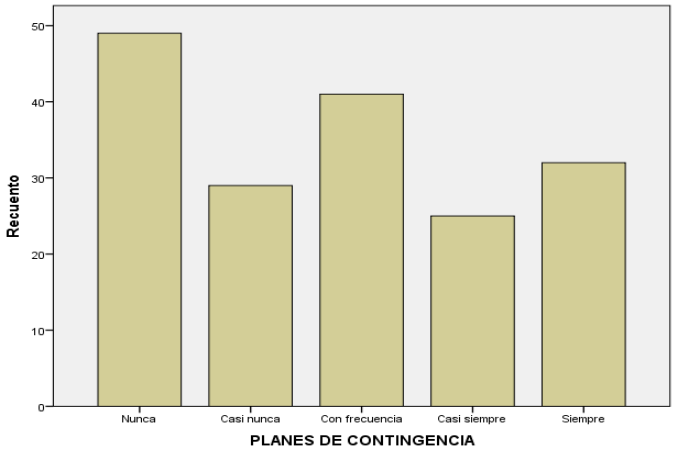
4.2.7 Planes de contingencia.

A la pregunta ¿Se tiene contemplado los planes de contingencia para algunas eventualidades en la gestión?

CUADRO Nº 07
PLANES DE CONTINGENCIA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	49	27,8	27,8	27,8
	Casi nunca	29	16,5	16,5	44,3
	Con frecuencia	41	23,3	23,3	67,6
	Casi siempre	25	14,2	14,2	81,8
	Siempre	32	18,2	18,2	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 07



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, 18% respondieron siempre, 14% casi siempre, 23% con frecuencia, 17% casi nunca y 28% en su mayoría respondieron nunca se tiene contemplado los planes de contingencia para algunas eventualidades en la gestión.

PREVENCIÓN DE FRAUDES

4.2.8 Mitigación de fraudes sectoriales.

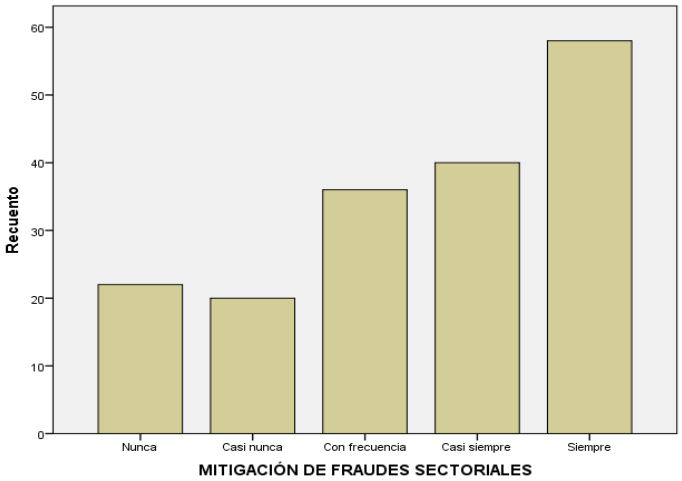
A la pregunta ¿Se viene mitigando los fraudes de manera sectorial en la gestión de la empresa?

CUADRO Nº 08

MITIGACIÓN DE FRAUDES SECTORIALES

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	22	12,5	12,5	12,5
	Casi nunca	20	11,4	11,4	23,9
	Con frecuencia	36	20,5	20,5	44,3
	Casi siempre	40	22,7	22,7	67,0
	Siempre	58	33,0	33,0	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 08



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 33% respondieron siempre se viene mitigando los fraudes de manera sectorial en la gestión de la empresa, 23% casi siempre, 21% con frecuencia, 11% casi nunca y 13% nunca.

4.2.9 Minimización integral de prevención.

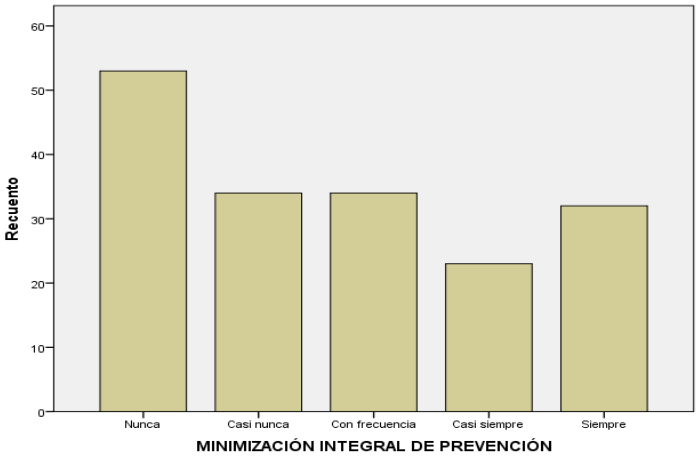
A la pregunta: ¿Existen resultados de minimización integral en la prevención de fraudes en la empresa?

CUADRO Nº 09

MINIMIZACIÓN INTEGRAL DE PREVENCIÓN

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	53	30,1	30,1	30,1
	Casi nunca	34	19,3	19,3	49,4
	Con frecuencia	34	19,3	19,3	68,8
	Casi siempre	23	13,1	13,1	81,8
	Siempre	32	18,2	18,2	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 09



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, 18% respondieron siempre, 13% casi siempre, 19% con frecuencia, 19% casi nunca y 30% en su mayoría respondieron nunca existen resultados de minimización integral en la prevención de fraudes en la empresa.

4.2.10 Eficiencia de controles de seguridad.

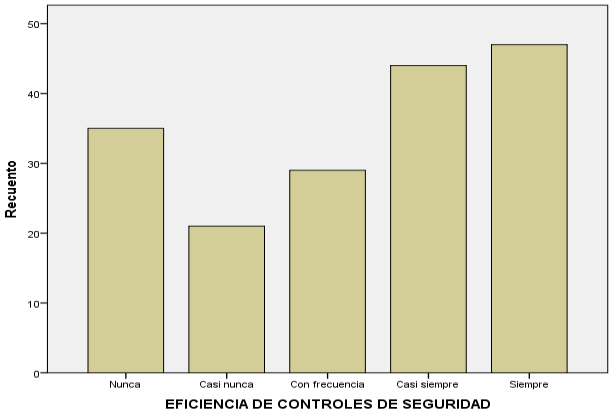
A la pregunta ¿Son eficiente los controles de seguridad en la prevención de fraudes en la organización?

CUADRO Nº 10

EFICIENCIA DE CONTROLES DE SEGURIDAD

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	35	19,9	19,9	19,9
	Casi nunca	21	11,9	11,9	31,8
	Con frecuencia	29	16,5	16,5	48,3
	Casi siempre	44	25,0	25,0	73,3
	Siempre	47	26,7	26,7	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 10



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 27% respondieron siempre son eficiente los controles de seguridad en la prevención de fraudes en la organización, 25% casi siempre, 17% con frecuencia, 12% casi nunca y 20% nunca.

4.2.11 Estrategias en la prevención de fraudes.

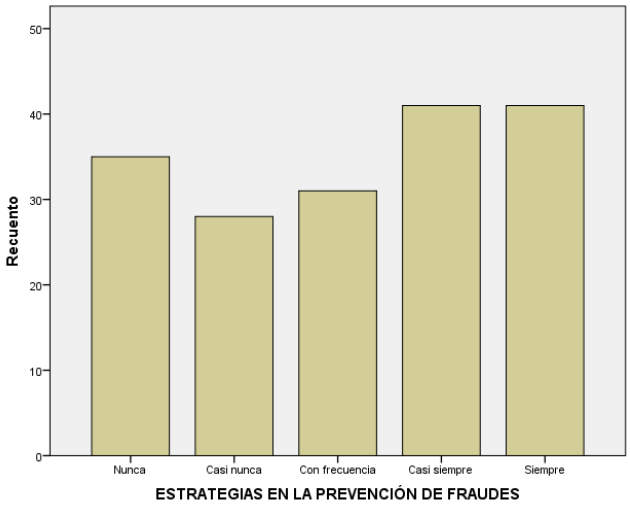
A la pregunta ¿Se vienen definiendo las estrategias a seguir en la prevención de fraudes en la empresa?

CUADRO Nº 11

ESTRATEGIAS EN LA PREVENCIÓN DE FRAUDES

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	35	19,9	19,9	19,9
	Casi nunca	28	15,9	15,9	35,8
	Con frecuencia	31	17,6	17,6	53,4
	Casi siempre	41	23,3	23,3	76,7
	Siempre	41	23,3	23,3	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 11



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 23% respondieron siempre Se vienen definiendo las estrategias a seguir en la prevención de fraudes en la empresa, 23% casi siempre, 18% con frecuencia, 16% casi nunca y 20% nunca.

4.2.12 Desarrollo de pruebas de vulnerabilidad.

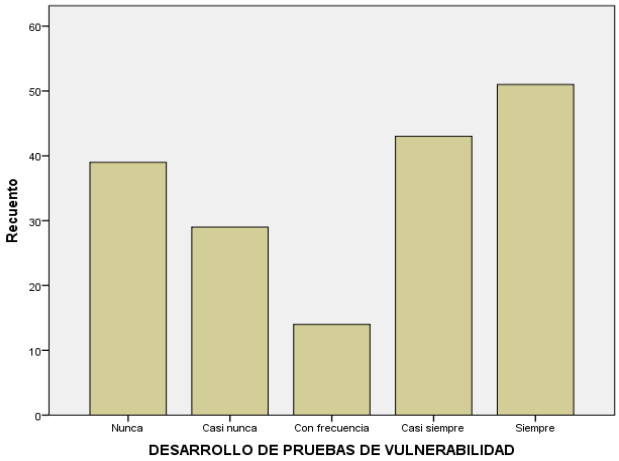
A la pregunta ¿Se vienen desarrollando pruebas de vulnerabilidad en cuanto a la prevención de fraudes?

CUADRO Nº 12

DESARROLLO DE PRUEBAS DE VULNERABILIDAD

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	39	22,2	22,2	22,2
	Casi nunca	29	16,5	16,5	38,6
	Con frecuencia	14	8,0	8,0	46,6
	Casi siempre	43	24,4	24,4	71,0
	Siempre	51	29,0	29,0	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 12



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, en su mayoría 29% respondieron siempre se vienen desarrollando pruebas de vulnerabilidad en cuanto a la prevención de fraudes, 24% casi siempre, 8% con frecuencia, 17% casi nunca y 22% nunca.

4.2.13 Habilidades para identificar fraudes.

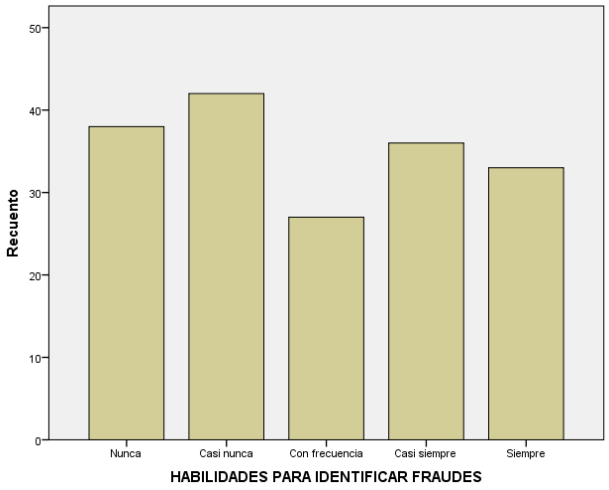
A la pregunta ¿Los trabajadores de la empresa se encuentra capacitados en habilidades de gestión para identificar fraudes?

CUADRO Nº 13

HABILIDADES PARA IDENTIFICAR FRAUDES

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	38	21,6	21,6	21,6
	Casi nunca	42	23,9	23,9	45,5
	Con frecuencia	27	15,3	15,3	60,8
	Casi siempre	36	20,5	20,5	81,3
	Siempre	33	18,8	18,8	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 13



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, 19% respondieron siempre, 21% casi siempre, 15% con frecuencia, 24% en su mayoría respondió casi nunca los trabajadores de la empresa se encuentra capacitados en habilidades de gestión para identificar fraudes y 22% nunca.

4.2.14 Experiencia en prevención de fraudes.

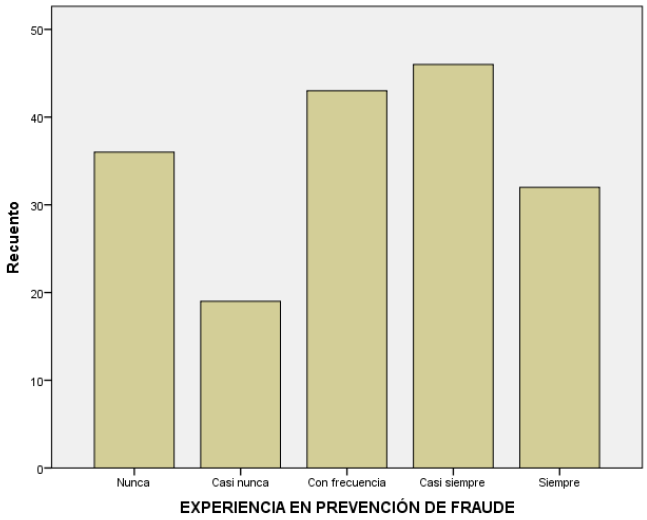
A la pregunta ¿Es importante la experiencia en la gestión y prevención de fraudes en su empresa?

CUADRO Nº 14

EXPERIENCIA EN PREVENCIÓN DE FRAUDE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	36	20,5	20,5	20,5
	Casi nunca	19	10,8	10,8	31,3
	Con frecuencia	43	24,4	24,4	55,7
	Casi siempre	46	26,1	26,1	81,8
	Siempre	32	18,2	18,2	100,0
	Total	176	100,0	100,0	

GRAFICO Nº 14



INTERPRETACIÒN:

El trabajo de campo realizado, ha permitido establecerse que, según los representantes y trabajadores de las empresas industriales del distrito de Yanacancha, 18% respondieron siempre, 26% en su mayoría respondió casi siempre es importante la experiencia en la gestión y prevención de fraudes en su empresa, 24% con frecuencia, 11% casi nunca y 21% nunca.

4.3. Prueba de hipótesis.

Todos los contrastes estadísticos exigen para su correcta aplicación uno o varios requisitos previos que, en el supuesto de no cumplirse, podrían dar lugar a resultados e interpretaciones erróneas. Sin embargo, hay muchas situaciones en las que trabajamos con muestras de datos muy exclusivos como en el presente caso, en las que los mismos no siguen una distribución determinada, en las que las variancias difieren significativamente, en las que las variables están medidas en una escala ordinal.

Teniendo en cuenta la formulación del problema general y específicos, así como los objetivos propuestos en el presente trabajo de investigación, podemos realizar la correspondiente demostración, contrastación y validación de las hipótesis planteadas inicialmente, frente a los resultados obtenidos después de la aplicación del trabajo de campo, la tabulación y procesamiento de datos obtenidos, y su presentación respectiva mediante los cuadros estadísticos que presentamos en el capítulo 4.2 del presente trabajo y para su mayor comprensión en este capítulo; para contrastar las hipótesis se usó la distribución ji cuadrada puesto que los datos disponibles para el análisis están distribuidos en frecuencias absolutas o frecuencias observadas. La estadística ji cuadrada es más adecuada para esta investigación porque las variables son cualitativas.

Hipótesis a:

Ho: El diseño y aplicación de las normas de la economía digital no influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha.

H1: El diseño y aplicación de las normas de la economía digital influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha.

		MITIGACIÓN DE FRAUDES SECTORIALES					
		Nunca	Casi nunca	Con frecuencia	Casi siempre	Siempre	Total
CONOCIMIENTO DEL DISEÑO Y APLICACIÓN DE NORMAS	Nunca	19	0	2	1	1	23
	Casi nunca	0	17	0	2	0	19
	Con frecuencia	3	0	19	4	0	26
	Casi siempre	0	2	1	32	3	38
	Siempre	0	1	14	1	54	70
Total		22	20	36	40	58	176

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	419,502[a]	16	,000
Razón de verosimilitud	322,461	16	,000
Asociación lineal por lineal	114,261	1	,000
N de casos válidos	176		

Para probar la hipótesis planteada seguiremos el siguiente procedimiento:

1. Suposiciones: La muestra es una muestra aleatoria simple.
2. Estadística de prueba: La estadística de prueba es:

$$x^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

3. Distribución de la estadística de prueba: cuando Ho es verdadera, X^2 sigue una distribución aproximada de ji cuadrada con (5-1) (5-1) = 16 grados de libertad.
4. Regla de decisión: A un nivel de significancia de 0.05, rechazar hipótesis nula (Ho) si el valor calculado de X^2 es mayor o igual a 26.296.

5. Calculo de la estadística de pruebas. Al desarrollar la formula tenemos:

$$x^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(O_{ij} - E_{ij})^2}{E_{ij}} = 419.502$$

6. Decisión estadística: Dado que 419.502 > 26.296, se rechaza Ho.

7. Conclusión: El diseño y aplicación de las normas de la economía digital influye en la mitigación sectorial de fraudes en las empresas industriales del distrito de Yanacancha.

Hipótesis b:

Ho: El conocimiento de los componentes que originan riesgos de seguridad cibernética no influye en la minimización integral de fraudes en las empresas industriales del distrito de Yanacancha.

H1: El conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de fraudes en las empresas industriales del distrito de Yanacancha.

		MINIMIZACIÓN INTEGRAL DE PREVENCIÓN					
		Nunca	Casi nunca	Con frecuencia	Casi siempre	Siempre	Total
CONOCIMIENTO DE LOS COMPONENTES	Nunca	32	1	1	1	0	35
	Casi nunca	0	27	1	0	1	29
	Con frecuencia	0	1	32	2	1	36
	Casi siempre	12	2	0	19	0	33
	Siempre	9	3	0	1	30	43
Total		53	34	34	23	32	176

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	422,014[a]	16	,000
Razón de verosimilitud	345,986	16	,000
Asociación lineal por lineal	66,513	1	,000
N de casos válidos	176		

Para probar la hipótesis planteada seguiremos el siguiente procedimiento:

1. Suposiciones: La muestra es una muestra aleatoria simple.
2. Estadística de prueba: La estadística de prueba es:

$$x^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

3. Distribución de la estadística de prueba: cuando Ho es verdadera, X^2 sigue una distribución aproximada de ji cuadrada con (5-1) (5-1) = 16 grados de libertad.
4. Regla de decisión: A un nivel de significancia de 0.05, rechazar hipótesis nula (Ho) si el valor calculado de X^2 es mayor o igual a 26.296.
5. Calculo de la estadística de pruebas. Al desarrollar la formula tenemos:

$$x^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(O_{ij} - E_{ij})^2}{E_{ij}} = 422.014$$

6. Decisión estadística: Dado que 422.014 > 26.296, se rechaza Ho.

7. Conclusión: El conocimiento de los componentes que originan riesgos de seguridad cibernética influye en la minimización integral de fraudes en las empresas industriales del distrito de Yanacancha.

Hipótesis c:

Ho: La realización de una evaluación de riesgos no influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha.

H1: La realización de una evaluación de riesgos influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha.

		EFICIENCIA DE CONTROLES DE SEGURIDAD					
		Nunca	Casi nunca	Con frecuencia	Casi siempre	Siempre	Total
EVALUACIÓN DE RIESGOS	Nunca	29	0	0	0	0	29
	Casi nunca	0	20	2	5	0	27
	Con frecuencia	2	0	20	6	1	29
	Casi siempre	4	0	0	32	1	37
	Siempre	0	1	7	1	45	54
Total		35	21	29	44	47	176

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	447,232[a]	16	,000
Razón de verosimilitud	367,283	16	,000
Asociación lineal por lineal	126,191	1	,000
N de casos válidos	176		

Para probar la hipótesis planteada seguiremos el siguiente procedimiento:

1. Suposiciones: La muestra es una muestra aleatoria simple.

2. Estadística de prueba: La estadística de prueba es:

$$x^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

3. Distribución de la estadística de prueba: cuando Ho es verdadera, X^2 sigue una distribución aproximada de ji cuadrada con (5-1) (5-1) = 16 grados de libertad.

4. Regla de decisión: A un nivel de significancia de 0.05, rechazar hipótesis nula (Ho) si el valor calculado de X^2 es mayor o igual a 26.296.

5. Calculo de la estadística de pruebas. Al desarrollar la formula tenemos:

$$x^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(O_{ij} - E_{ij})^2}{E_{ij}} = 447.232$$

6. Decisión estadística: Dado que 447.232 > 26.296, se rechaza Ho.

7. Conclusión: La realización de una evaluación de riesgos influye en los controles de seguridad de fraudes en las empresas industriales del distrito de Yanacancha.

4.4 Discusión de resultados.

Los riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del distrito de Yanacancha; se encuentran en pleno proceso de globalización de la economía que ha creado un mercado en donde los competidores se encuentran en cualquier parte del mundo, en la actualidad el comercio mundial se expande a una velocidad que empequeñece a casi todos los demás parámetros del crecimiento; no obstante, la forma en que éste se realice en el futuro es un tema de gran preocupación en el presente y de oportunidades sin precedentes. Pero el estudio realizado nos demuestra que, una gran mayoría de los micros y pequeñas empresas, dejan al descubierto las principales falencias como: Avances tecnológicos, altos índices de productividad, excelentes indicadores de gestión, factores de tipo cultural, disposición natural a la cooperación, solidaridad y confianza en el otro (instituciones y grupos de actores económicos) y muy especialmente, la presencia de una política efectiva de promoción internacional hacia las empresas industriales.

De la misma manera se observa que, las empresas industriales operan mayormente en base a la intuición, teniendo una perspectiva de corto plazo y cuentan con información más de carácter cuantitativo, contable e interno, descuidando el análisis de los resultados en base a otros tipos de factores no contables o externos para la toma de decisiones. Algunas les bastan aprender

de la experiencia y desarrollar la habilidad de adaptarse a su medio ambiente, pero para nuestros tiempos, la velocidad del cambio es mayor que la de la adaptación, de modo que esto no sólo bastara. Se requerirán habilidades más sofisticadas para poder competir con el ritmo acelerado de cambios que caracteriza a la cultura contemporánea. Estas habilidades más sofisticadas son la de anticiparse y predecir, mirando lo que habrá de venir y que se plasmará a través de la visión que fije la empresa.

CONCLUSIONES

1. La economía digital está basada en la digitalización de la información y en la infraestructura de las TIC. Está integrada por empresas que ofrecen productos y servicios puramente digitales, productos y servicios mixtos, empresas que realizan la producción de bienes y la prestación de servicios intensivos en TIC, conjunto de actividades definidas por el término comercio electrónico, y los segmentos de la industria de las TIC que dan soporte al resto de los segmentos identificados (infraestructura física y lógica).
2. *Las principales barreras de entrada en la economía digital para las empresas son la falta de cultura empresarial en relación al comercio electrónico, los hábitos del consumidor, la seguridad y la inexistencia de un marco legal, entre otras. Por tanto, es preciso diseñar y aprobar lo que podríamos denominar «las normas de la economía digital» que afectan a aspectos como la privacidad, la seguridad o los derechos de propiedad intelectual*
3. El gobierno del Perú debe identificar la seguridad de su ciberespacio como un objetivo estratégico de la seguridad nacional, puesto que la materialización de una amenaza sobre nuestro ciberespacio puede afectar muy negativamente al desarrollo social, económico y cultural de nuestro país.
4. La dirección de la ciberseguridad debe realizarse de manera centralizada. Como corolario del principio anterior, el Estado debe crear un organismo con la misión de dirigir la ciberseguridad

nacional, coordinando a las entidades públicas y privadas implicadas.

5. *Pese a que muchos de los componentes que originan riesgos de seguridad cibernética se inician con la tecnología, estos ejecutivos y otros interesados (incluyendo clientes, entidades reguladoras, inversores, empleados, y financieros) reconocen que estos riesgos deben ser manejados como parte de la estrategia de negocio, en lugar de tratarlos únicamente como cuestiones de tecnología, por lo de la participación de los ejecutivos y trabajadores se hace más necesario.*

RECOMENDACIONES

1.- Las empresas industriales del distrito de Yanacancha deben adecuarse al impacto y a la intensidad de la velocidad de cómo están acelerando los cambios fugazmente. Para tal efecto, deberá demostrar una capacidad de respuesta capaz de absorber la incertidumbre que dichos cambios puedan ocasionar para así neutralizar o minimizar los riesgos que pongan en peligro su existencia.

2.- Es necesario que los directivos de las empresas industriales, capaciten a su personal en los riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales; del mismo modo deben organizarse para resolver conflictos situacionales y superar sus debilidades o amenazas, generar propuestas antes de que éstas los desestabilicen y tengan poco margen de adaptabilidad, flexibilidad o reacción para enfrentarlas.

3. Las empresas industriales, deben gestionar bajo el modelo de planeación estratégica, los riesgos de ciberseguridad, cuyo alcance, es fijar el norte empresarial más allá del corto plazo, más allá de lo inmediato, pues existe el riesgo de perderse en las consecuencias del momento.

4. Ante los cambios de los últimos tiempos, las empresas industriales, requieren con urgencia de cambios estructurales, de gestión y de actitud, de manera tal que les permita crecer con rentabilidad y

estabilidad alcanzando un mayor grado de competitividad. Estos cambios se refieren fundamentalmente a la innovación, actualización, conciencia de la utilidad de la información contable de gestión, aplicación de nuevas ideas y tecnologías en la organización de su empresa y en especial, a saber, aprovechar con eficiencia las oportunidades que se les brinda su medio externo, teniendo en cuenta los riesgos de ciberseguridad.

5. El sistema de información gerencial mediante la evaluación por áreas claves de resultados y sus subsistemas organizacionales contribuyen a la solución de problemas para una efectiva toma de decisión o ejecución de un proyecto.

BIBLIOGRAFIA

1. GARCIA BENAU, MARIA YVICOMARTINEZ, ANTONIO. Los Escándalos Financieros y la Auditoria: Perdida y recuperación de la confianza de una profesión en crisis, España 2003 pagina 48.
2. III CONVENCION NACIONAL DE AUDITORIA, AUDITA 2009, realizado en la ciudad de Cusco 101paginas.
3. RUIZ BARBADILLO, EMILIANO. El papel de los Auditores en los Escándalos Financieros. España 2003 pagina 57. En www.:partidadoble.es
4. KLITGAARD, ROBERTO. Controlando la corrupción fundación Hanns Seidel, Editorial Quipus. La paz 1990.
5. TOUSSAINT, ERIC. Enron y Cía.: La debacle de la nueva economía “made in USA” en pagina 16.
6. RANGEL CRUZ, PEDRO A. Los Fraudes Corporativos en el Marco Ideológico del Capitalismo Global Barquisimeto 2005 pagina 88.
7. http://www.transparency.org/ índice de percepción de la corrupción 2010/ transparency international anual reporte 2010.
8. BEATRIZ MERINO I CONFERENCIA ANUAL ANTICORRUPCION LIMA 2010.
9. LOZANO/MERINO (compiladores). La hora de la transparencia en América Latina. Editorial Granica/Ciedla, 1998, Buenos Aires. Pág. 158.

10. TORRES BARDARLES, Colonibol - Orientaciones Básicas de Metodología de la Investigación Científica – Perú 2002 -8va. Edición.
11. TORRES BARDALES, Colonibol. “Metodología de la Investigación Científica. Cuarta Edición. Lima Perú 1995.
12. VELASQUEZ FERNANDEZ, Ángel. “Metodología de la Investigación Científica. Editorial San Marcos. Lima Perú 2005.

ANEXOS

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ESCUELA DE POSGRADO

CUESTIONARIO

A continuación, le formulamos un conjunto de preguntas con varias opciones de respuesta. De dichas opciones, escoja usted la respuesta adecuada y coloque un aspa en el paréntesis correspondiente. La información que usted proporciona es de carácter confidencial.

RIESGOS DE CIBERSEGURIDAD

1. ¿Es importante el conocimiento del diseño y aplicación de normas relacionadas a la ciberseguridad?
   - 5) Siempre ( )
   - 4) Con frecuencia ( )
   - 3) A veces ( )
   - 2) Casi nunca ( )
   - 1) Nunca ( )
2. ¿Se tiene conocimiento de los componentes relacionados a la ciberseguridad?
   - 5) Siempre ( )
   - 4) Con frecuencia ( )
   - 3) A veces ( )
   - 2) Casi nunca ( )
   - 1) Nunca ( )
3. ¿Se vienen desarrollando evaluación de riesgos en cada una de las áreas de la empresa?
   - 5) Siempre ( )
   - 4) Con frecuencia ( )

3) A veces ( )
2) Casi nunca ( )
1) Nunca ( )

4. ¿Se vienen clasificando los riesgos cibernéticos en la gestión de la empresa?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
5. ¿Se vienen identificando los tipos de riesgos cibernéticos en la empresa?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
6. ¿Se tiene identificado los controles de riesgo en la empresa donde labora?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
7. ¿Se tiene contemplado los planes de contingencia para algunas eventualidades en la gestión?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )

PREVENCIÓN DE FRAUDES

8. ¿Se viene mitigando los fraudes de manera sectorial en la gestión de la empresa?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
9. ¿Existen resultados de minimización integral en la prevención de fraudes en la empresa?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
10. ¿Son eficiente los controles de seguridad en la prevención de fraudes en la organización?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
11. ¿Se vienen definiendo las estrategias a seguir en la prevención de fraudes en la empresa?
   5) Siempre ( )
   4) Con frecuencia ( )
   3) A veces ( )
   2) Casi nunca ( )
   1) Nunca ( )
12. ¿Se vienen desarrollando pruebas de vulnerabilidad en cuanto a la prevención de fraudes?

5) Siempre ( )
4) Con frecuencia ( )
3) A veces ( )
2) Casi nunca ( )
1) Nunca ( )

13. ¿Los trabajadores de la empresa se encuentra capacitados en habilidades de gestión para identificar fraudes?
    5) Siempre ( )
    4) Con frecuencia ( )
    3) A veces ( )
    2) Casi nunca ( )
    1) Nunca ( )
14. ¿Es importante la experiencia en la gestión y prevención de fraudes en su empresa?
    5) Siempre ( )
    4) Con frecuencia ( )
    3) A veces ( )
    2) Casi nunca ( )
    1) Nunca ( )

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ESCUELA DE POSGRADO

GUIA DE ANALISIS DOCUMENTAL

1. ¿Qué tipo de documento es?

   ---

2. ¿Qué representa?

   ---

3. ¿Es una obra de rigor científico?

   ---

4. ¿Cuál es su actualidad?

   ---

5. ¿Cuál es su contexto?

   ---

6. ¿Quién es el autor?

   ---

7. ¿Qué relevancia científica tiene en la disciplina?

   ---

8. ¿Con que fines se creó el documento?

   ---

9. ¿Es autentico?

   ---

10. ¿Cuán original es?
