

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS
Y CONTABLES
ESCUELA PROFESIONAL DE CONTABILIDAD



“EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGIÓN DE UCAYALI, AÑO 2020”

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE CONTADOR PÚBLICO

AUTORES:

ALEXIS CELSO MARIN AMPUERO
ESTEFANY SANTA MARIA FLORES

ASESOR:

DR. MIGUES AREVALO RIOS

PUCALLPA – PERÚ

2021



UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

COMISION DE GRADOS Y TITULOS

“Año del Fortalecimiento de la Soberanía Nacional”

**ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE:
CONTADOR PÚBLICO**

Siendo las 12:00 P.M. del día Lunes 17 de Enero del 2022, en los ambientes del Salón de Grados y Títulos de la Facultad de Ciencias Económicas, Administrativas y Contables, en cumplimiento con lo señalado en los Artículos 17º y 18º del Reglamento de General de Grado Académico de Bachiller, Título Profesional y Título de segunda Especialidad Profesional, se reunió el jurado integrado por los docentes: **Dr. Juan José Palomino Ochoa (Presidente)**, **Mg. Severino Antonio Guerra Da Silva (Miembro)** y **CPC. Jorge Armando Palacios Valera (Miembro)**

Se realizó la Sustentación de la Tesis Titulada: **“EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGIÓN DE UCAYALI, AÑO 2020”.**, por el/la/los Bachilleres en Contabilidad: **Alexis Celso Marin Ampuero, EN FORMA PRESENCIAL:**

Qué; según el Artículo 21º del Reglamento General de Grado Académico de Bachiller, Título Profesional y Título de Segunda Especialidad Profesional, que a la letra dice:

“La evaluación se hará de acuerdo a la siguiente escala de calificaciones:


- a) Sobresaliente con felicitación escrita y recomendaciones de publicación
- b) Aprobado por unanimidad
- c) Aprobado por mayoría
- d) Desaprobado...”

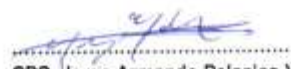
El/la defensor(a) de la Tesis, ha obtenido la siguiente calificación;

Aprobado por mayoría


Siendo las 13:00 P.M. del mismo día, se dio por concluido el acto y luego de ser leído el acta, los miembros del Jurado Evaluador procedieron a suscribirlo.


Dr. Juan Jose Palomino Ochoa
Presidente


Mg. Severino Antonio Guerra Da Silva
Miembro


CPC. Jorge Armando Palacios Valera
Miembro




Mg. Alex Davis Astohuaman Huaranga
Secretario Académico



UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

COMISION DE GRADOS Y TITULOS

"Año del Fortalecimiento de la Soberanía Nacional"

**ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE:
CONTADOR PÚBLICO**

Siendo las 12:00 PM del día Lunes 17 de Enero del 2022, en los ambientes del Salón de Grados y Títulos de la Facultad de Ciencias Económicas, Administrativas y Contables, en cumplimiento con lo señalado en los Artículos 17º y 18º del Reglamento de General de Grado Académico de Bachiller, Título Profesional y Título de segunda Especialidad Profesional, se reunió el jurado integrado por los docentes: **Dr. Juan José Palomino Ochoa (Presidente), Mg. Severino Antonio Guerra Da Silva (Miembro) y CPC. Jorge Armando Palacios Valera (Miembro)**

Se realizó la Sustentación de la Tesis Titulada: **"EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGIÓN DE UCAYALI, AÑO 2020"**, por el/la/los Bachilleres en Contabilidad: **Estefany Santa Maria Flores, EN FORMA PRESENCIAL:**

Qué; según el Artículo 21º del Reglamento General de Grado Académico de Bachiller, Título Profesional y Título de Segunda Especialidad Profesional, que a la letra dice:

"La evaluación se hará de acuerdo a la siguiente escala de calificaciones:

- e) Sobresaliente con felicitación escrita y recomendaciones de publicación
- f) Aprobado por unanimidad
- g) Aprobado por mayoría
- h) Desaprobado..."

El/la defensor(a) de la Tesis, ha obtenido la siguiente calificación;

Aprobado por mayoría

Siendo las 13:00 PM del mismo día, se dio por concluido el acto y luego de ser leído el acta, los miembros del Jurado Evaluador procedieron a suscribirlo.

.....
Dr. Juan Jose Palomino Ochoa
Presidente

.....
Mg. Severino Antonio Guerra Da Silva
Miembro

.....
CPC. Jorge Armando Palacios Valera
Miembro



.....
Mg. Alex Davis Astohuaman Huaranga
Secretario Académico

ACTA DE APROBACIÓN

La presente tesis fue aprobada por el Jurado Calificador de la Facultad de Ciencias Económicas, Administrativas y Contables de la Universidad Nacional de Ucayali, para optar el Título Profesional de Contador Público.

Dr. Juan Jose Palomino Ochoa



Presidente

Mg. Severino Antonio Guerra Da Silva



Miembro

C.P.C Jorge Armando Palacios Valera



Miembro

Dr. Migue Arévalo Ríos



Asesor

Alexis Celso Marin Ampuero



Tesista

Estefany Santa María Flores



Tesista



UNIVERSIDAD NACIONAL DE UCAYALI
VICERRECTORADO DE INVESTIGACION
DIRECCION DE PRODUCCION INTELLECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACION

SISTEMA ANTIPLAGIO URKUND

N° V/0552-2021

La Dirección de Producción Intelectual, hace constar por la presente, que el Informe Final (Tesis), Titulado:

“EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDADES DEL ÓRGANO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGIÓN DE UCAYALI, AÑO 2020”.

Autor (a) : MARIN AMPUERO. ALEXIS CELSO
SANTA MARÍA FLORES, ESTEFANY

Facultad : CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES
Escuela Profesional : CONTABILIDAD.
Asesor(a) : Dr. ARÉVALO RÍOS, MIGUES

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 0%**.

En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.

En señal de conformidad y verificación se entrega la presente constancia.

Fecha: 15/12/2021



Dr. ABRAHAM ERMITANIO HUAMAN ALMIRON
Dirección de Producción Intelectual



UNIVERSIDAD NACIONAL DE UCAYALI

OEByP - REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACION DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, ALEXIS CELSO MARIN AMPUERO

Autor(a) de la TESIS de pregrado titulada:

EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANISMO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGION DE UCAYALI / AÑO 2020.

Sustentada el año: 2022

Con la asesoría de: DR. MIGUEL ADEVALO RIOS

En la Facultad: CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

Escuela profesional: CONTABILIDAD

Autorizo la publicación:

PARCIAL Significa que se publicará en el repositorio institucional solo la carátula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar si su tesis o documento presenta material patentable, para ello deberá presentar el trámite de CATI y/o INDECOPi cuando se lo solicite la DGPI UNU.

TOTAL Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 24 / 01 / 2022

Email: alexisampuero03@gmail.com
Teléfono: 956573220

Firma: [Firma manuscrita]
DNI: 73622485



UNIVERSIDAD NACIONAL DE UCAYALI

OEByP - REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACION DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, ESTEFANY SANTA MARIA FLORES

Autor(a) de la TESIS de pregrado titulada:

EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GOBIERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANISMO DE CONTROL INTERNO EN UNA MUNICIPIALIDAD DE LA REGION DE UCAYALI, AÑO 2020

Sustentada el año: 2022

Con la asesoría de: DR. MIGUEL AREVALO REOS

En la Facultad: CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

Escuela profesional: CONTABILIDAD

Autorizo la publicación:

PARCIAL Significa que se publicará en el repositorio institucional solo la caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar si su tesis o documento presenta material patentable, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 24 / 01 / 2022

Email: estefany.santamariaflores@gmail.com
Teléfono: 962473444

Firma: 
DNI: 74370555

DEDICATORIA

A mis padres por haberme forjado como la persona que soy en la actualidad, mucho de mis logros se los debo a ustedes entre los que se incluye este. Me formaron con reglas y algunas libertades, pero al final de cuentas, me motivaron constantemente para alcanzar mis anhelos.

Alexis Celso

A Dios por que provee nuestros caminos y nos da fortaleza de levantarnos, cada vez que nos caemos y nos brinda la salud para salir adelante.

A mis padres por su tiempo, cariño y apoyo todo mi ciclo académico.

A mi familia porque también me brinda fortaleza para salir adelante y ser ejemplo futuro.

Estefany

AGRADECIMIENTO

En primer lugar, poner a Dios, por permitirnos tan buena experiencia dentro de la universidad y así convertirnos en profesional en lo que tanto nos apasiona.

Gracias a todos nuestros docentes que hicieron parte de todo este proceso integral de formación que nos dejó como producto terminado la tesis, que perdurara dentro de los conocimientos y desarrollo para las demás generaciones que están por llegar.

RESUMEN

Objetivo de la presente investigación es establecer la relación del ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020, los ciberdelitos efectúan una serie de robos cibernéticos mediante el uso de redes de las entidades en el cual suplantan identidad de los funcionarios, autoridades claves para apoderarse de los fondos públicos de manera delictiva, en ese sentido se establece la relación de los riesgos tecnológicos y la implementación de un área de control con un auditor interno antifraude de los fondos, que tenga la capacidad y la experticia en la prevención de los ciberdelitos informáticos de las municipalidades Distritales o Provinciales, por otra parte se determina la relación de los riesgos de robo de identidad de funcionarios y la prevención que deben implantarse en los sistemas informáticos de las entidades gubernamentales, asimismo se analizó la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales, la metodología es correlacional, cuantitativa, básica no es aplicada, donde los resultados conllevan a que si hay una relación del ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.

Palabras claves: Ciberdelito, Redes delictivas, Riesgos informáticos.

ABSTRACT

Objective of this research is to establish the relationship of cybercrime of criminal networks on a global scale to government entities and the responsibility of internal auditors in a municipality of the Ucayali-2020 Region, cybercrimes carry out a series of cyber thefts by using networks of entities in which they impersonate the identity of officials, key authorities to seize public funds in a criminal way, in that sense the relationship of technological risks and the implementation of a control area with an internal anti-fraud auditor is established of the funds, that has the capacity and expertise in the prevention of cybercrimes of the District or Provincial municipalities, on the other hand, the relationship of the risks of identity theft of officials and the prevention that must be implemented in the systems is determined. IT staff of government entities, the relationship of the computer risks in the diversion of funds and the obtaining of a reasonable security of the internal control of the District or Provincial municipalities, the methodology is correlational, quantitative, basic is not applied, where the results imply that if there is a relationship of cybercrime of criminal networks on a global scale to government entities and the responsibility of internal auditors in a municipality of the Ucayali Region-2020.

Keywords: Cybercrime, Criminal networks, Computer risks.

INTRODUCCIÓN

De acuerdo con la investigación realizada el problema de los robos a través de redes informáticos en el mundo se ha acentuado cada vez que ha ido mejorando los medios tecnológicos que permite que pueden realizar desde otros países, en ese sentido el estudio sobre ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.

La investigación sobre los ciberdelitos tiene una connotación en las actuales circunstancias donde se ve reflejada los robos de identidad de funcionarios claves de las entidades gubernamentales con la finalidad de que pueden realizar esta figura delictiva que causa gran daño a las entidades del estado, porque el dinero que son objeto de robo son complejos de recuperar, por tanto afecta y reduce la posibilidad de mejorar la infraestructura o servicios a los ciudadanos.

Tiene la siguiente estructura:

Capítulo I:

Se efectúan las descripciones de los problemas existentes de los ciberdelitos en las instituciones gubernamentales.

Capítulo II:

Marco teórico de la investigación que consolidan la investigación desarrollada sobre los ciberdelitos en las entidades del Estado.

Capítulo III:

Metodología de la investigación e instrumentos que se emplearon en el desarrollo del estudio, técnicas.

Capitulo IV:

Resultados de la investigación.

Las conclusiones.

Las sugerencias.

ÍNDICE

.....	vii
DEDICATORIA	viii
AGRADECIMIENTO	ix
RESUMEN	x
ABSTRACT.....	xi
INTRODUCCIÓN.....	xii
ÍNDICE	xiv
ÍNDICE DE TABLAS.....	xvi
ÍNDICE DE FIGURAS.....	xvii
CAPÍTULO I	18
1. PLANTEAMIENTO DEL PROBLEMA	18
1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA.....	18
1.2. FORMULACIÓN DEL PROBLEMA.....	21
1.2.1. PROBLEMA GENERAL	21
1.2.2. PROBLEMAS ESPECÍFICOS	21
1.3. OBJETIVO	22
1.3.1. OBJETIVO GENERAL.....	22
1.3.2. OBJETIVOS ESPECÍFICOS.....	22
1.4. HIPÓTESIS	23
1.4.1. HIPÓTESIS GENERAL.....	23
1.4.2. HIPÓTESIS ESPECÍFICAS.....	23
1.5. VARIABLES	23
1.6. JUSTIFICACIÓN E IMPORTANCIA	24
1.7. VIABILIDAD.....	25
1.8. LIMITACIONES.....	25
CAPÍTULO II	26
2. MARCO TEÓRICO	26
2.1. ANTECEDENTES.....	26
2.1.1. ANTECEDENTES INTERNACIONALES.....	26
2.1.2. ANTECEDENTES NACIONALES.....	30
2.2. BASES TEÓRICAS	34

2.2.1. CIBERDELITOS.....	34
2.2.2. RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO	37
2.3. DEFINICIONES CONCEPTUALES	41
CAPÍTULO III	46
3. MARCO METODOLÓGICO	46
3.1. TIPOS DE INVESTIGACIÓN	46
3.2. DISEÑO Y ESQUEMA DE LA INVESTIGACIÓN.....	46
3.3. POBLACIÓN Y MUESTRA	47
3.3.1. POBLACIÓN.....	47
3.3.2. MUESTRA.....	47
3.4. OPERACIONALIZACIÓN DE LAS VARIABLES.....	47
3.5. INSTRUMENTO DE RECOLECCIÓN DE DATOS	48
3.6. TÉCNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS.....	48
CAPÍTULO IV.....	49
4. RESULTADOS	49
CONCLUSIONES.....	81
SUGERENCIAS.....	82
REFERENCIAS BIBLIOGRÁFICAS.....	83

ÍNDICE DE TABLAS

Tabla 01	Riesgos tecnológicos – I_____	48
Tabla 02	Riesgos tecnológicos – II_____	50
Tabla 03	Riesgos de robo de identidad – I_____	52
Tabla 04	Riesgos de robo de identidad – II_____	54
Tabla 05	Riesgos informáticos en el desvío de fondos – I_____	56
Tabla 06	Riesgos informáticos en el desvío de fondos – II_____	58
Tabla 07	Auditor interno antifraude – I_____	60
Tabla 08	Auditor interno antifraude – II_____	62
Tabla 09	Prevención de los sistemas informáticos – I_____	64
Tabla 10	Prevención de los sistemas informáticos – II_____	66
Tabla 11	Seguridad razonable – I_____	68
Tabla 12	Seguridad razonable – II_____	70

ÍNDICE DE FIGURAS

Figura 01	Riesgos tecnológicos – I_____	48
Figura 02	Riesgos tecnológicos – II_____	50
Figura 03	Riesgos de robo de identidad – I_____	52
Figura 04	Riesgos de robo de identidad – II_____	54
Figura 05	Riesgos informáticos en el desvío de fondos – I_____	56
Figura 06	Riesgos informáticos en el desvío de fondos – II_____	58
Figura 07	Auditor interno antifraude – I_____	60
Figura 08	Auditor interno antifraude – II_____	62
Figura 09	Prevención de los sistemas informáticos – I_____	64
Figura 10	Prevención de los sistemas informáticos – II_____	66
Figura 11	Seguridad razonable – I_____	68
Figura 12	Seguridad razonable – II_____	70

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

En los últimos años la revolución de la tecnología tiene un auge a nivel global, que trae consigo una serie de avances positivos para el desarrollo socioeconómico de la sociedad en los distintos campos, sin embargo, también trae riesgos del uso indebido de la tecnología por organizaciones criminales, en el que se efectúan robo de identidad, desvío de fondos de las entidades gubernamentales que debilita el control y la seguridad en el mundo. En ese contexto los gobiernos en América Latina enfrentan retos en la seguridad de la información electrónica, que, si bien lleva a un desarrollo en la gestión gubernamental al incorporar tecnología en línea, también estas son aprovechadas para cometer los ciberdelitos, en ese sentido las entidades gubernamentales tienen ciertas carencias en la detección de los ciberdelitos, que pueden efectuar robo de identidad de funcionarios claves que tienen manejo de los fondos públicos.

La (Interpol, 2020), señala respecto a los ciberdelitos que, con el uso de las nuevas tecnologías para cometer ataques cibernéticos contra gobiernos, negocios e individuos, palabras y frases que hace una década apenas existían, forman ahora parte de nuestro vocabulario diario. Estos delitos no conocen fronteras, ni físicas ni virtuales, causan importantes daños y suponen un peligro muy real para las víctimas de todo el mundo. La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. Los

ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca vista hasta ahora. Las redes delictivas operan a escala planetaria, coordinando ataques complejos contra sus objetivos en cuestión de minutos.

La auditoría en el ciberdelito cumple un rol fundamental a fin de detectar las posibles debilidades o riesgos de áreas críticas como el área de tesorería, caja, fondos de cuentas corrientes, en ese sentido el control debe ser de manera permanente a fin de salvaguardar los riesgos por robos informáticos, se debe evaluar las competencias del profesional o personal que labora en estas áreas, conociendo cuáles son sus aptitudes, los actos éticos y morales.

En nuestro país el ciberdelito se acentuado de manera sistemática con mayor incidencia en las municipalidades y otros entes gubernamentales, quienes han sufrido la transferencia de fondos destinados para obras públicas o adquisiciones de bienes o prestación de servicios, donde se ha incrementado de manera exponencial en el año 2020, periodo en el cual se incorporó el uso obligatorio las operaciones digitales como consecuencia de la pandemia del Covid_19, donde la virtualidad es una necesidad prioritaria, de ahí que los trabajos para grupos vulnerables se efectúan de manera remota.

Tal como manifiesta (Flores Vidal, 2020) que, el coronavirus también ha tenido un impacto negativo en términos de ciberseguridad en el país. Según las cifras más recientes, los delitos cibernéticos aumentaron un 59% en el primer semestre, respecto al mismo periodo del año pasado, debido a que la pandemia

impulsó el uso de las operaciones digitales y sumado a la necesidad de quedarse en casa y hacer un mayor uso de las tecnologías exponiendo nuestros datos personales debido al uso de aplicaciones, redes sociales, internet de las cosas y mucho más, lo que está siendo aprovechado por los ciberdelincuentes. Malware, estafas, robo de datos, etc., son muchas las variantes criminales, lo que puede convertir el uso de internet en un auténtico peligro si no se toman ciertos recaudos.

El problema principal de los ciberdelitos esta acentuado en las municipalidades, tal como ocurre en Ucayali, en el que Municipalidades como de Manantay, Padre Abad sufrieron el desfalco de fondos utilizando estos medios electrónicos, en el que se apropian mediante el fraude informático, uso de redes delictivas que operan a nivel global, el uso de phishing que consiste en captar contraseñas o números de tarjetas de crédito, cuentas bancarias, imitando correos electrónicos de los municipios, tal como ha sucedido en la Municipalidad Provincial de Padre Abad, en el que transfirieron fondo de capital del municipio a distintas cuentas bancarias de empresas constructoras del país por un monto significativo de 10 millones de soles de manera sistemática.

Las causas de los ciberdelitos es la falta de experticia en el manejo de la tecnología por parte de los funcionarios y servidores públicos, en la Municipalidad Provincial de Padre Abad, así como en el restos de las entidades públicas, que no tienen una preparación en el campo informático, adolecen de conocimientos básicos en seguridad de ciberdelitos, por otro parte la falta de valores éticos y morales que conducen a ser parte de los ciberdelitos, por otra

parte es la falta de evaluación al personal en el manejo de las tecnologías de información, a fin de evitar los riesgos de fraude informático de los fondos del estado.

Las consecuencias de la falta de manejo en seguridad informática conlleva a desfalco de fondos del Estado, como lo ocurrido en la Municipalidad Provincial de Padre Abad, en el que se sustrajeron 10 millones de soles, haciendo uso de transferencias a varias cuentas de empresas que retiraron esos fondos complicando la situación financiera de la municipalidad, y haciendo improbable la recuperación de los fondos transferidos, la modalidad del robo informático de las cuentas de la entidad es por la excesiva confianza del uso de claves, o participación de personal clave de la entidad, por la falta de valores éticos y morales que están propensos a cometer actos de corrupción.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿Cuál es la relación del ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020?

1.2.2. PROBLEMAS ESPECÍFICOS

- ¿Cuál es la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales?

- ¿Cuál es la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales?
- ¿Cuál es la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales?

1.3. OBJETIVO

1.3.1. OBJETIVO GENERAL

Establecer la relación del ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020

1.3.2. OBJETIVOS ESPECÍFICOS

- Establecer la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.
- Determinar la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales.
- Analizar la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

1.4. HIPÓTESIS

1.4.1. HIPÓTESIS GENERAL

Existe grado de relación entre el ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.

1.4.2. HIPÓTESIS ESPECÍFICAS

- Establecer la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.
- Determinar la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales.
- Analizar la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

1.5. VARIABLES

Variable independiente

Ciberdelito

Indicadores:

- a. Riesgos Tecnológicos
- b. Riesgos de robo de identidad
- c. Riesgos informáticos en el desvío de fondos

Variable dependiente

Responsabilidad de auditor interno

Indicadores:

- a. Auditor interno antifraude
- b. Prevención de los sistemas informáticos
- c. Seguridad razonable

1.6. JUSTIFICACIÓN E IMPORTANCIA

El ciberdelito en la actualidad opera a nivel mundial con redes delictivas organizadas que atacan a las instituciones gubernamentales, de ahí que la investigación se justifica porque las municipalidades Distritales y Provinciales en la Región de Ucayali, son acechadas por estas organizaciones que efectúan robos de identidad de funcionarios, correos electrónicos, a fin de obtener claves con la complicidad de funcionarios a fin de desviar los fondos a otras empresas de otras regiones y efectuar el desfalco de millones de soles del presupuesto público asignado a los gobiernos locales. En este contexto la labor del órgano de control interno es fundamental a fin de detectar los riesgos de los ciberdelitos en sus distintas modalidades, para ello se debe contar con un profesional contable a fin de prevenir posibles riesgos de fraude informático, detectar en el tiempo oportuno, investigar y comprobar los riesgos tecnológicos, ataques cibernéticos, redes delictivas.

Por tanto, la importancia de la investigación es que busca establecer grado de relación entre los riesgos existentes de los ciberdelitos y la responsabilidad del Órgano de Control Interno para la obtención de una seguridad razonable, que

garantice las operaciones de cuentas bancarias de los gobiernos locales en la región de Ucayali.

1.7. VIABILIDAD

La investigación por su diseño no experimental y transversal es viable en la toma de muestra que permite el desarrollo de acuerdo a lo planificado, por ser de enfoque cuantitativo en el que se miden las variables de estudio.

1.8. LIMITACIONES

De acuerdo con el contexto mundial, los escenarios han cambiado por efectos de la pandemia Covid-19, que no permite hacer el recojo de información de manera rápida, que se tiene que contar con una serie de protocolos los cuales limitan haciendo uso de mayor tiempo en el recojo de información mediante los instrumentos.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1. ANTECEDENTES INTERNACIONALES

(Quevedo Gonzáles, 2017), en su tesis “Investigación y prueba del Cibercrimen”, concluye que:

Se examina en este trabajo la tendencia que tiene el uso de internet en la aparición de nuevos delitos y de nuevas formas de comisión de los ilícitos tradicionales. A todos ellos se denomina cibercrimen, cuya investigación y prueba exigen la adopción de especiales precauciones para evitar que se frustre la labor investigadora o se vulneren derechos fundamentales. Para ello, se estudian cuestiones básicas que suscitan los cibercrimen como la competencia para conocer de los mismos, los conflictos de jurisdicción entre Estados, la cooperación internacional y los sujetos especializados en la investigación, así como las obligaciones a las que vienen sujetas las empresas proveedoras de internet. Se analiza la regulación legal de las medidas de investigación tecnológica necesarias para la investigación del cibercrimen, en concreto: la obtención de una IP, la identificación de terminales, de datos desvinculados de los procesos de comunicación, la orden de conservación de datos, la cesión de datos de tráfico, la interceptación de las comunicaciones

telefónicas y telemáticas, el registro de dispositivos informáticos de almacenamiento masivo, el registro remoto de equipos, el agente encubierto informático y qué sucede con los hallazgos casuales descubiertos tras estas medidas.

(Acuña Lopez & Villa Motato, 2018), en su tesis “Estado actual del Cibercrimen en Colombia con respecto a Latinoamérica”, concluye que:

Para un país la información y los datos, así como la tecnología que la soporta, representa uno de los activos más valiosos, por lo tanto, debe ser protegida preservada y respetada, esto se logra por medio de la legislación, generación de normatividad y leyes. En el estudio a continuación se realiza una comparación entre la legislación sobre Delitos Informáticos de distintitos países latinoamericanos, europeos y americanos con el fin de compararlos con Colombia que es el foco de estudio, e identificar las fortalezas, debilidades, falencias y sugerencias que se pueden aplicar para posteriores estudios de actualización, mejoras que se puedan presentar más adelante, desde nuevos proyectos de ley que permitan la creación de nuevos artículos o modificación que fortalezcan la Constitución Nacional. Actualmente la información de las empresas y las personas tiende a ser almacenada en bases de datos electrónicas, lo cual ha desencadenado la aparición de diferentes formas de delitos informáticos derivados de la utilización de la información con

fines lucrativos o maliciosos, o la alteración de la misma. Para tratar esos delitos se han desarrollado diferentes normativas gubernamentales, como la ley orgánica de protección de datos personales en España, o la ley 1581 de 2012 sobre protección de datos personales en Colombia. Se puede concluir que existe interés en el tema de la legislación informática en cuanto a la privacidad de los datos personales, a pesar de que un gran porcentaje de las normativas generadas en el continente derivan de leyes y normas expedidas en países como España, Alemania, Estados Unidos de donde se adaptaron a las necesidades actuales del país, cada país tiene una visión diferente de que topología, tipificación clasificación y penalizaciones requeridas, pero es una necesidad que a fin de minimizar los vacíos jurídicos que pueden permitir a los ciberdelincuentes actuar sin temor al castigo, es implementar una estandarización legislativa más adecuada a los diferentes tipos de delito informático.

(Granados Ramírez & Parra Rojas, 2014), en su tesis “El delito de hurto por medios informáticos que tipifica el artículo 2691 de la Ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cúcuta en el periodo 2012-2014”, concluye que:

La revolución informática surgida desde mediados del siglo XX hasta la actualidad, ha traído consigo un sinnúmero de beneficios, especialmente relacionados con la facilidad para el

intercambio de información y comunicación a nivel mundial; sin embargo, así como esta ha evolucionado y tiene importantes ventajas, también ésta tiene sus desventajas, y es que a la par con ella han surgido los delincuentes informáticos, quienes han venido perfeccionando sus modus operandi en los delitos informáticos, siendo uno de los más frecuentes el delito de hurto por medios informáticos, consagrado en la Ley 1273 de 2009 (Artículo 269I). La ocurrencia del delito de hurto por medios informáticos, se relaciona directamente con todas aquellas operaciones que los clientes bancarios y en especial los tarjetahabientes realizan a través de sus computadores, tablets, equipos celulares, y todos aquellos dispositivos que por su capacidad pueden almacenar o copiar información digital, como son las tarjetas débito o crédito, los cajeros electrónicos, datafonos, entre otros; pues es a través de estos medios que los delincuentes informáticos acceden a las cuentas de los clientes bancarios, y realizan operaciones sin su autorización o consentimiento, las cuales se constituyen en hurtos por medios informáticos. Antes de la expedición de la Ley 1273 de 2009 que regula lo concerniente a los delitos informáticos, el delito en estudio, era solo catalogado como un delito de hurto de acuerdo al Código Penal (Ley 599 de 2000, Artículo 239), sin embargo, con la entrada en vigencia de esta nueva ley, el tratamiento penal

es el de hurto calificado, consagrado en el artículo 240 de la Ley 599 de 2000, y tendrá una pena de prisión de seis (6) a catorce (14) años, de acuerdo a las circunstancias de tiempo, modo y lugar. Por todo lo anterior, se desarrolla esta investigación la cual busca analizar la aplicabilidad que ha tenido el artículo 269I de la Ley 1273 de 2009 que tipifica el delito de hurto por medios informáticos en el Distrito Judicial de Cúcuta en el período 2012 – 2014.

2.1.2. ANTECEDENTES NACIONALES

(Pardo Vargas, 2018), en su tesis “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018”, concluye que:

El tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todos los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio. Asimismo, el tratamiento jurídico de los delitos informáticos contra el patrimonio en su modalidad de hurto es deficiente, en la medida que en la legislación peruana no se regula en forma expresa el delito informático contra el patrimonio, y al ser este tipo penal muy abierto y ambiguo no

permite la efectiva sanción de los delitos informáticos contra el patrimonio.

(Alarcon Ariza & Barrera Barón, 2017), en su tesis “Uso de internet y delito informático en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016” concluye que:

Los resultados obtenidos de la investigación establecieron el grado de correlación de las variables uso del internet y los delitos informativos a través de la prueba estadística por chi-cuadrado y normalidad demostrando que existe una relación positiva y significativa con un valor $p \leq 0.0001$, menor que 0.005, permitió determinar los rangos de relación del uso del internet en $r=0.980$ y delitos informativos en $r=0.975$, lo que significa que la hipótesis alterna se acepta. Lo que indica que el uso del internet mediante las competencias informacionales por habilidad, acceso a la información y aspectos sociales se relacionan con los delitos informáticos de derecho de autor, uso legal de la información y el uso correcto de las redes sociales, es decir que las ocurrencias de los delitos informáticos dependen del desarrollo de las competencias informacionales en el uso del internet.

(Vilca Aira, 2018), en su tesis “Los hackers: delito informático frente al código penal peruano” concluye que:

La falta de una información adecuada sobre los límites de la tecnología informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones. Al hacer un análisis comparativo de legislación con otros países, se determinó que Perú es un país que ciertamente regula los delitos informáticos, sin embargo, lo hace de una forma deficiente ya que es de forma generalizada, lo que propicia algunos vacíos legales que imposibilitan una investigación forense en materia informática. Además, la comisión de delitos emergentes en la internet es un problema que afecta a la sociedad mundialmente, tanto niños como adultos, no importando la edad, ni género, se ven vulnerables a caer en las redes de algún delito o crimen cibernético, por lo que es necesaria la capacidad del perito o investigador en la escena del crimen y el correcto procedimiento en la misma para lograr la resolución óptima del caso.

(Blossiers Mazzini, 2018) en su tesis “El delito informático y su incidencia en la empresa bancaria” concluye que:

Conforme a lo recabado, como en las encuestas, se ha identificado que los delitos informáticos, surten un impacto económico y social en las empresas bancarias, asimismo surte

un impacto en su estabilidad jurídica. Primero, surte un impacto económico, respecto de las pérdidas que estas generan a la empresa, así como las pérdidas que se generan a los clientes de estas empresas, consecuencia de ello, es el impacto social que se tiene, pues los clientes asumen una desconfianza en las empresas bancarias, lo cual a largo plazo podría generar pérdidas a la empresa bancaria. Las inestabilidades jurídicas que podría generarse, se basa en los procesos civiles y penales que se podrían generar, ello ante el agravio de los clientes, quienes desconfiados podrían iniciar algún tipo de proceso a las empresas bancarias; lo cual en suma podría generar grandes pérdidas para las empresas, sobre todo en sus activos; si bien es cierto, las empresas pueden contar con seguros, estas no necesariamente serán suficientes para reparar los daños cometidos.

2.2. BASES TEÓRICAS

2.2.1. CIBERDELITOS

Ley N° 30096 (22 de octubre 2013). Diario Oficial El Peruano, 22 octubre 2013 establece sobre la Ley de Delitos informáticos, lo siguiente:

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

(Serrano Buitrago, 2014), sostiene que:

Resulta oportuno relacionar los daños asociados a delitos informáticos, estos perjuicios se pueden agrupar en dos métodos, el primero hace referencia a los daños y destrozos físicos en los ordenadores, computadores o sistemas de seguridad y vigilancia, donde la característica de este método es

el deterioro y no tiene ánimo de lucro, su pretensión es la de sabotear o neutralizar los sistemas como por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, son una serie de conductas destinadas a la destrucción física del hardware y el software de un sistema.

El otro método está dirigido a causar daños lógicos, son todas aquellas conductas que producen, como resultado, la destrucción, inutilización, o alteración de datos, programas, bases de datos información, documentos electrónicos, contenidos en cualquier soporte lógico, sistemas informáticos o telemáticos que permitan la intrusión del delincuente quien busca acceder a las bases de datos, la suplantación de identidad, el hurto de activos, o con la pretensión de causar destrozos irreversibles de la información empresarial, destrucción de los sistemas de protección informática, hurto de secreto comercial.

(UNODC, 2013), señala que:

El acceso a los sistemas de control de servicios en red, como el correo electrónico, los servicios bancarios en línea o de servidores, suele requerir una contraseña. Por lo tanto, la obtención de contraseñas para acceder a servicios en línea se

ha convertido en una prioridad para la comisión de delitos relacionados con la identidad. Conseguir información sobre las cuentas, además de permitir al delincuente hacer uso del servicio correspondiente y realizar transacciones en línea, enviar correos electrónicos o vender bienes en una plataforma de subastas, le puede dar acceso a otros servicios.

(UNODC, 2013), señala que:

Como se ha señalado, la información relacionada con la identidad cumple un importante papel en la vida social. La mayoría de las disposiciones penales tradicionales que podrían aplicarse para el enjuiciamiento en relación con determinados aspectos de delitos como el fraude y la falsificación de la identidad no fueron concebidas para proteger la información relativa a la identidad, sino que tienen en cuenta otros valores fundamentales, como la confianza del mercado en la fiabilidad de los documentos. Si el legislador dispusiera de un criterio específico para tipificar el hurto de identidad podría responder al creciente interés que promueve la información relativa a la identidad, mediante la adopción de una disposición penal que la proteja jurídicamente.

(Montoya Vivanco, 2013), señala que:

Los delitos de corrupción socavan gravemente la legitimidad del Estado y con ello su fundamento democrático. Por esto, es

legítimo y se constituye en imperativo sancionar los actos de corrupción. En este ámbito no se debe tolerar la impunidad como efecto de la prescripción de la acción penal de estos delitos. Los procesos por corrupción deben terminar con una sentencia que declare la responsabilidad o inocencia de los acusados. Por ello, es necesaria una reforma legislativa orientada a evitar la impunidad por prescripción, que entre otras medidas amplíe los plazos de prescripción de todos los delitos de corrupción. Sin embargo, la imprescriptibilidad no es una solución adecuada al problema de la impunidad de estos delitos, tampoco necesaria. Esta medida constituye únicamente una solución aparente, pero, además y esto es lo grave trae consigo consecuencias contraproducentes para la propia lucha contra la impunidad de los delitos de corrupción.

2.2.2. RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO

(Henaó Feria, 2017) señala que:

A través de los años se ha logrado comprobar que sin importar el tamaño de una organización o su razón de ser, el ejercer un adecuado control sobre esta resulta fundamental, siempre y cuando lo que se quiera sea garantizar su éxito y progreso, al igual que la generación de confianza en cada actividad o proceso realizado, sin embargo, el control interno, más que una medida que garantiza un adecuado funcionamiento empresarial, es una

herramienta que permite identificar riesgos o debilidades a las cuales se enfrenta diariamente las compañías, así como también se convierten en un aliado estratégico de los procesos contables o financieros llevados a cabo en dichas entidades.

(Contraloría General de la República, 2020), sostiene que:

El Órgano de Control Institucional es la unidad orgánica especializada responsable de llevar a cabo el control gubernamental en una institución o entidad pública, de conformidad con lo señalado en los artículos 7 y 17 de la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.

(Contraloría General de la República, 2020), señala que:

Su finalidad es promover la correcta y transparente gestión de los recursos y bienes de la entidad, cautelando la legalidad y eficiencia de sus actos y operaciones, así como el logro de sus resultados, mediante la ejecución de labores de control.

Es el conjunto de acciones, actividades, planes, políticas, normas, registros, procedimientos y métodos, incluido el entorno y actitudes que desarrollan autoridades y su personal a cargo, con el objetivo de prevenir posibles riesgos que afectan a una entidad pública. Se fundamenta en una estructura basada en cinco componentes funcionales:

1. Ambiente de control
2. Evaluación de riesgos
3. Actividades de control gerencial
4. Información y comunicación
5. Supervisión

¿Cuál es el beneficio de contar con un sistema de control interno?

Seguridad razonable de:

- Reducir los riesgos de corrupción
 - Lograr los objetivos y metas establecidos
 - Promover el desarrollo organizacional
 - Lograr mayor eficiencia, eficacia y transparencia en las operaciones
 - Asegurar el cumplimiento del marco normativo
 - Proteger los recursos y bienes del Estado, y el adecuado uso de los mismos
 - Contar con información confiable y oportuna
 - Fomentar la práctica de valores
 - Promover la rendición de cuentas de los funcionarios por la misión y objetivos encargados y el uso de los bienes y recursos asignados
- Implementación del sistema de control interno.

Se deben cumplir las tres fases siguientes:

Planificación

Se inicia con el compromiso formal de la Alta Dirección y la constitución de un Comité responsable de conducir el proceso. Comprende además las acciones orientadas a la formulación de un diagnóstico de la situación en que se encuentra el sistema de control interno de la entidad con respecto a las normas de control interno establecidas por la CGR, que servirá de base para la elaboración de un plan de trabajo que asegure su implementación y garantice la eficacia de su funcionamiento.

Ejecución

Comprende el desarrollo de las acciones previstas en el plan de trabajo. Se da en dos niveles secuenciales: a nivel de entidad y a nivel de procesos. En el primer nivel se establecen las políticas y normativa de control necesarias para la salvaguarda de los objetivos institucionales bajo el marco de las normas de control interno y componentes que éstas establecen; mientras que en el segundo, sobre la base de los procesos críticos de la entidad, previa identificación de los objetivos y de los riesgos que amenazan su cumplimiento, se procede a evaluar los controles existentes a efectos de que éstos aseguren la obtención de la respuesta a los riesgos que la administración ha adoptado.

Evaluación

Fase que comprende las acciones orientadas al logro de un apropiado proceso de implementación del sistema de control interno y de su eficaz funcionamiento, a través de su mejora continua.

Importante

El sistema de control interno está a cargo de la propia entidad pública. Su implementación y funcionamiento es responsabilidad de sus autoridades, funcionarios y servidores. ¿Cuál es el rol de la Contraloría? La CGR es responsable de la evaluación del sistema de control interno de las entidades del Estado. Sus resultados contribuyen a fortalecer la institución, a través de las recomendaciones que hace de conocimiento de la administración para las acciones conducentes a superar las debilidades e ineficiencias encontradas.

2.3. DEFINICIONES CONCEPTUALES

- **Adware.** – Para infectar un sistema operativo el Adware usualmente se instala junto a otro software que lo introduce en su instalador, y generalmente se puede eliminar si se desinstala el programa. (Gaviria, 2016)
- **Ataque cibernético.** – Evento que se inicia a través del internet contra un objetivo con la intención de negar, interrumpir, destruir o explotar un entorno operativo habilitado para la computadora. Muchos ataques cibernéticos están destinados a comprometerse con fines de explotación o destruir la

integridad de datos específicos, robar datos o manipular datos con fines nefastos. (Hudson Analytix, 2017)

- **Auditor.** – Los auditores están encargados de revisar las operaciones de la empresa, en tal sentido, tienen por misión mantener la transparencia del dinero que ingresa y egresa de la compañía u organización. (Guevara Arce, 2018)
- **Ciberdelitos.** - Desde el punto de vista jurídico, el primer problema a la hora de afrontar el análisis de los Ciberdelitos es intentar describir su contenido. En la actualidad hay una amplia gama de adjetivos usados para describir los delitos cometidos por internet o haciendo uso de nuevas tecnologías, sean delitos informáticos, Ciberdelitos, delitos telemáticos, cibernéticos, en línea u online, digital, en red, de alta tecnología, relacionados con internet, relacionados con informática, relacionados con telecomunicaciones, asistidos por ordenador, electrónicos, etc. (Quevedo Gonzales, 2017).
- **Control interno.** – Es un procedimiento que se enmarca en el control de recursos y activos de una empresa, y sirve para llevar un registro sobre su actividad y trazabilidad. (Villegas Cotrina, 2020)
- **Delito.** – Es una conducta, recogida en la legislación penal asociada a una sanción penal, que lesiona o pone en peligro un bien jurídico y atenta gravemente contra las concepciones ético – sociales, jurídicas, políticas y económicas esenciales de una sociedad. (Álvarez Carpentier, 1996)

- **Desvío de fondos.** – Hace referencia a una actuación de alguien que ha traspasado fondos de una entidad legítima propietaria de una suma de dinero a otra que no es la legítima titular de ese dinero.
- **Droppers.** – Bajo una apariencia de programa legítimo, los Droppers instalan y ejecutan otros programas y archivos maliciosos en el equipo del usuario atacado. La diferencia de los Droppers con los troyanos comunes es que éstos están destinados para alojar información o paquetes de datos concretos en el equipo infectado, y no suponen un fin en sí mismos, sino que son una herramienta más para conseguir un fin. (Microsoft Press, 2005)
- **DDoS.** – Los ataques DDoS (Distributed Denial of Service) son una forma relativamente sencilla y efectiva de hacer caer a una web. (Microsoft Press, 2005)
- **Entidades gubernamentales.** – Son instituciones estatales cuya administración está a cargo del gobierno de turno. Su finalidad es brindar un servicio público que resulta necesario para la ciudadanía. (Quiroz Quezada, 2015)
- **Organización criminal.** – Es aquella agrupación que cuenta con tres miembros o más, entre quienes se reparten tareas o funciones, cualquiera sea su estructura y ámbito de acción que tenga carácter estable o tiempo indefinido, funcione de manera coordinada y tenga el propósito de cometer delitos. (Cuba Ninamango, 2020)

- **Prevención.** – Está relacionada con la planificación de medidas de protección que busquen minimizar cualquier evento futuro, que pueda ocasionar daños. (Gomero Oré, 2017)
- **Redes.** – Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, recursos y servicios. (Microsoft Press, 2005)
- **Responsabilidad.** – Es el cumplimiento de las obligaciones o cuidado al hacer o decidir algo, o bien una forma de responder, que implica el claro conocimiento de que los resultados de cumplir o no las obligaciones, recaen sobre uno mismo. (Revista Alva Journal, 1990)
- **Riesgos informáticos.** – Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, a fin de determinar los controles adecuados para disminuir, trascurrir o evitar la ocurrencia del riesgo. (Gamarra Pineda, 2010)
- **Seguridad Informática.** – Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático, implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. (Taminchi Santillan, 2014)
- **Sistema informático.** – Es aquel sistema que aúna por un lado la parte física de la informática y por otra, la parte digital o no tangible de la informática. (Alfaro Soto, 2019)

- **Spam.** – Correo electrónico no solicitado o “basura”, normalmente enviado de forma masiva a destinatarios en todo el mundo y que suele relacionarse con productos farmacéuticos y pornografía. (Microsoft Press, 2005)
- **Tecnología.** – Es el conjunto de conocimientos y técnicas que se aplican de manera ordenada para alcanzar un determinado objetivo o resolver un problema. (Microsoft Press, 2005)

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. TIPOS DE INVESTIGACIÓN

El tipo de investigación es básica, relacional de enfoque cuantitativo, que busca medir el grado de relación entre el ciberdelito y la responsabilidad del órgano de control interno. En ese sentido, respecto al alcance correlacional en el que se pretende medir el grado de asociación entre las variables de estudio, (Hernández Sampieri & Mendoza Torres, 2018), señala que:

Este tipo de estudios tienen como finalidad conocer la relación o grado de asociación que existe entre dos o más conceptos, categorías o variables en un contexto en particular. (p.109).

3.2. DISEÑO Y ESQUEMA DE LA INVESTIGACIÓN

Los estudios en el ámbito de las ciencias sociales, están básicamente contextualizadas en el estudio de diseño no experimental, tal como se efectúa la investigación sobre los ciberdelitos y la responsabilidad del órgano de control interno de municipalidades en la Región de Ucayali, tal como (Palomino Ochoa & et.al, 2021), sostiene que:

El diseño de investigación es el orden a alcanzar en el que se ejecute un dominio, para lograr la confiabilidad del estudio y su dependencia con la aproximación de las hipótesis planteadas. (p.110).

Formula Estadísticas

Margen: 10%

Nivel de confianza: 99%

Población: 186

Tamaño de muestra: 88

Ecuacion Estadistica para Proporciones poblacionales

n= Tamaño de la muestra

Z= Nivel de confianza deseado

p= Proporción de la población con la característica deseada (éxito)

q= Proporción de la población sin la característica deseada (fracaso)

e= Nivel de error dispuesto a cometer

N= Tamaño de la población

$$n = \frac{z^2(p \cdot q)}{e^2 + \frac{z^2(p \cdot q)}{N}}$$

3.3. POBLACIÓN Y MUESTRA

3.3.1. POBLACIÓN

Para el presente estudio se cuenta con una población de estudio de 186 servidores públicos de la Municipalidad Provincial de Padre Abad.

3.3.2. MUESTRA

La muestra representativa de la presente investigación es de 88 servidores públicos de la Municipalidad Provincial de Padre Abad, a los cuales se sometieron la encuesta.

3.4. OPERACIONALIZACIÓN DE LAS VARIABLES

VARIABLE	DEFINICIÓN	DIMENSIONES
VARIABLE INDEPENDIENTE CIBERDELITO	(Serrano Buitrago, 2014), sostiene que: Resulta oportuno relacionar los daños asociados a delitos informáticos, estos perjuicios se pueden agrupar en dos métodos, el primero hace referencia a los daños y destrozos físicos en los ordenadores, computadores o sistemas de seguridad y vigilancia, donde la característica de este método es el deterioro y no tiene ánimo de lucro, su pretensión es la de sabotear o neutralizar los sistemas	Riesgos tecnológicos Riesgos de robo de identidad Riesgos informáticos en el desvío de fondos
VARIABLE DEPENDIENTE RESPONSABILIDAD DE AUDITOR INTERNO	(Henaó Fera, 2017) señala que: A través de los años se ha logrado comprobar que sin importar el tamaño de una organización o su razón de ser, el ejercer un adecuado control sobre esta resulta fundamental, siempre y cuando lo que se quiera sea garantizar su éxito y progreso, al igual que la generación de confianza en cada actividad o proceso realizado,	Auditor interno antifraude Prevención de los sistemas informáticos Seguridad razonable

3.5. INSTRUMENTO DE RECOLECCIÓN DE DATOS

Los instrumentos que se empleó en la investigación es el uso de instrumentos como la encuesta de 18 preguntas de 09 de cada variable de estudio.

Según, (Arroyo Morales, 2020), señala que:

En la etapa de ejecución del proceso de investigación científica la recolección de datos es una de las actividades desarrolladas de fundamental importancia.

Actividades realizadas a través de instrumentos de recolección que materializan las técnicas utilizadas para la extracción de datos e información tienen como objetivo acumular datos e información significativos y libres de errores es decir información valida, confiable y relacionada con el hecho o aspecto problemático. (p.259)

3.6. TÉCNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS

La encuesta, esta técnica se trasunta en un formato que aplicado a la muestra de informantes sirve a los propósitos de recolección de datos a través del instrumento denominado "cuestionario".

El cuestionario comprende un conjunto o batería de preguntas sobre cada uno de los indicadores de los ítems identificados en la "operacionalización o itemnización de variables"; es decir, ítems e indicadores de las variables de la investigación presentes en la hipótesis o en los objetivos según sea el caso, (Arroyo Morales, 2020).

CAPÍTULO IV

4. RESULTADOS

4.1. Dimensión: Riesgos tecnológicos

Está usted de acuerdo que los riesgos tecnológicos deben ser prevenidos con la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

Tabla 1.

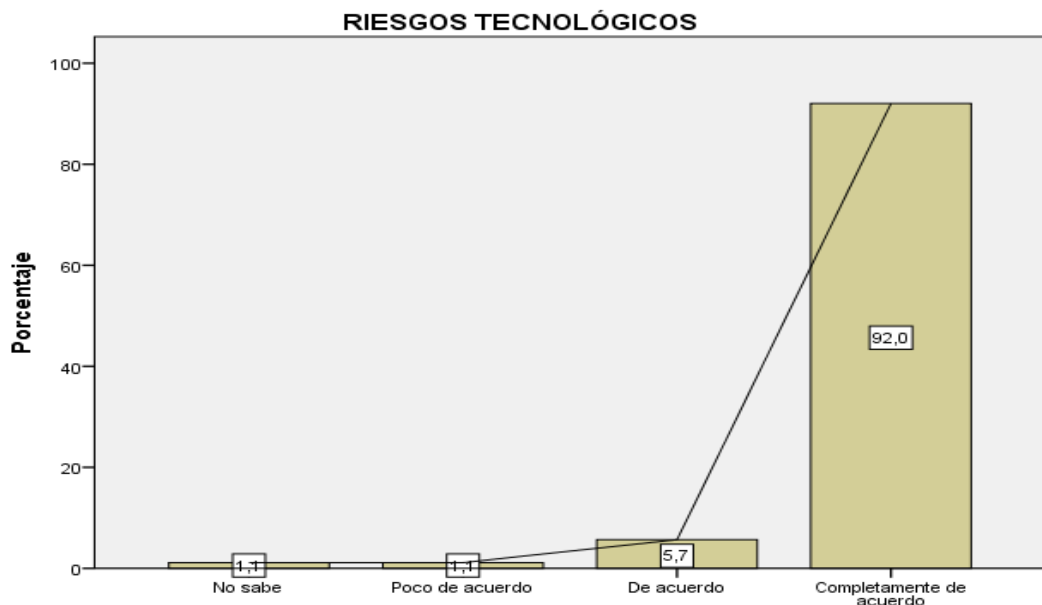
Riesgos tecnológicos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	1	1,1	1,1	1,1
Poco de acuerdo	1	1,1	1,1	2,3
Válidos De acuerdo	5	5,7	5,7	8,0
Completamente de acuerdo	81	92,0	92,0	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable ciberdelito.

Fuente: Elaboración propia

Figura 1



P1

Análisis:

Con respecto a los resultados se tomó una muestra de 88 servidores públicos de la Municipalidad Provincial de Padre Abad, quienes contestaron lo siguiente:

Para la primera pregunta el 92.0% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que los riesgos tecnológicos deben ser prevenidos con la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 5.7% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que los riesgos tecnológicos deben ser prevenidos con la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

Al mismo tiempo el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que los riesgos tecnológicos deben ser prevenidos con la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

Por último, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que no saben si los riesgos tecnológicos deben ser prevenidos con la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

4.2. Dimensión: Riesgos tecnológicos

Está usted de acuerdo que ciberdelito de redes delictivas a escala global a las entidades gubernamentales genera responsabilidad de los auditores internos por la falta de prevención en una municipalidad de la Región de Ucayali-2020.

Tabla 2.

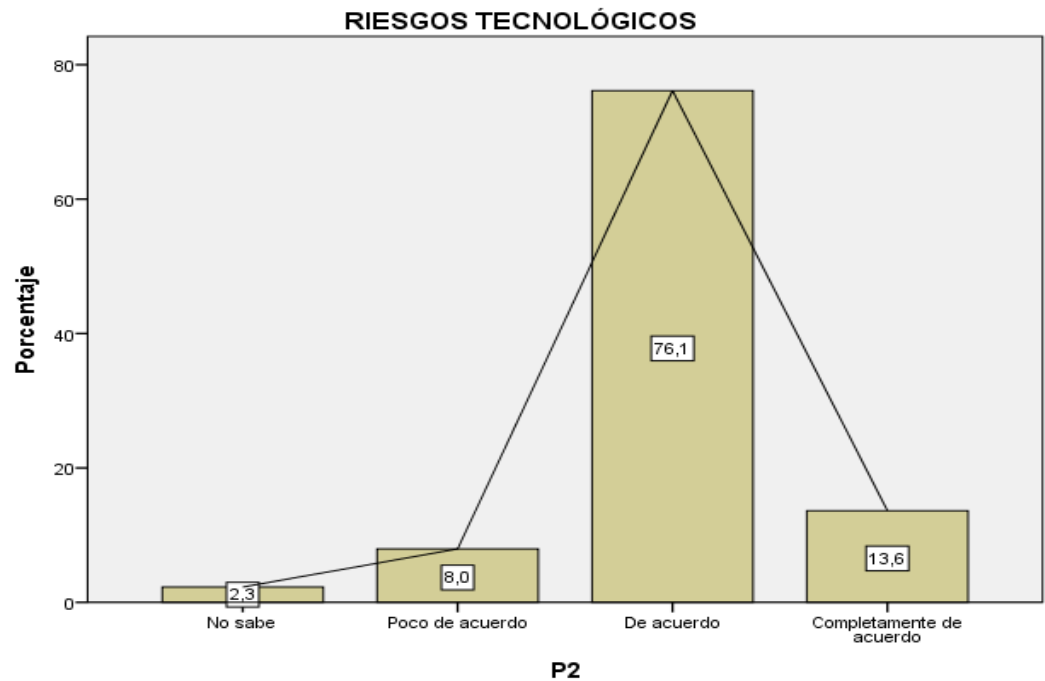
Riesgos tecnológicos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	2	2,3	2,3	2,3
Poco de acuerdo	7	8,0	8,0	10,2
De acuerdo	67	76,1	76,1	86,4
Completamente de acuerdo	12	13,6	13,6	100,0
Válidos				
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable ciberdelito.

Fuente: Elaboración propia

Figura 2



Análisis:

Para la primera pregunta el 13.6% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que ciberdelito de redes delictivas a escala global a las entidades gubernamentales genera responsabilidad de los auditores internos por la falta de prevención en una municipalidad de la Región de Ucayali-2020.

El siguiente resultado se observó que el 76.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que ciberdelito de redes delictivas a escala global a las entidades gubernamentales genera responsabilidad de los auditores internos por la falta de prevención en una municipalidad de la Región de Ucayali-2020.

Al mismo tiempo el 8.0% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que ciberdelito de redes delictivas a escala global a las entidades gubernamentales genera responsabilidad de los auditores internos por la falta de prevención en una municipalidad de la Región de Ucayali-2020.

Por último, el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que no saben si ciberdelito de redes delictivas a escala global a las entidades gubernamentales genera responsabilidad de los auditores internos por la falta de prevención en una municipalidad de la Región de Ucayali-2020.

4.3. Dimensión: Riesgos de robo de identidad

Está de acuerdo que los riesgos de robo de identidad de funcionarios son por la falta de prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Tabla 3.

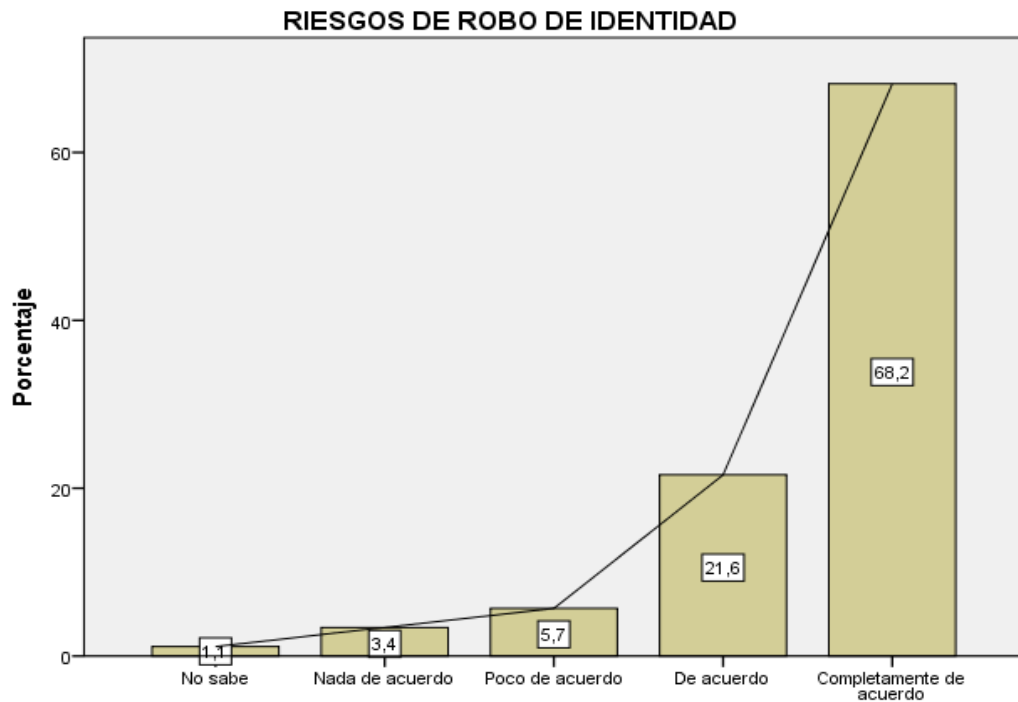
Riesgos de robo de identidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	1	1,1	1,1	1,1
Nada de acuerdo	3	3,4	3,4	4,5
Poco de acuerdo	5	5,7	5,7	10,2
De acuerdo	19	21,6	21,6	31,8
Completamente de acuerdo	60	68,2	68,2	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable ciberdelito.

Fuente: Elaboración propia

Figura 3



P3

Análisis:

Para la primera pregunta el 68.2% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que los riesgos de robo de identidad de funcionarios son por la falta de prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

El siguiente resultado se observó que el 21.6% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que los riesgos de robo de identidad de funcionarios son por la falta de prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Al mismo tiempo el 5.7% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que los riesgos de robo de identidad de funcionarios son por la falta de prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

En el caso del siguiente resultado, el 3.4% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que los riesgos de robo de identidad de funcionarios son por la falta de prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Por último, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, respondieron no saber.

4.4. Dimensión: Riesgos de robo de identidad

Está de acuerdo que el órgano de control interno debe prevenir los riesgos de robo de identidad de funcionarios asegurando los sistemas informáticos de las municipalidades Distritales o Provinciales.

Tabla 4.

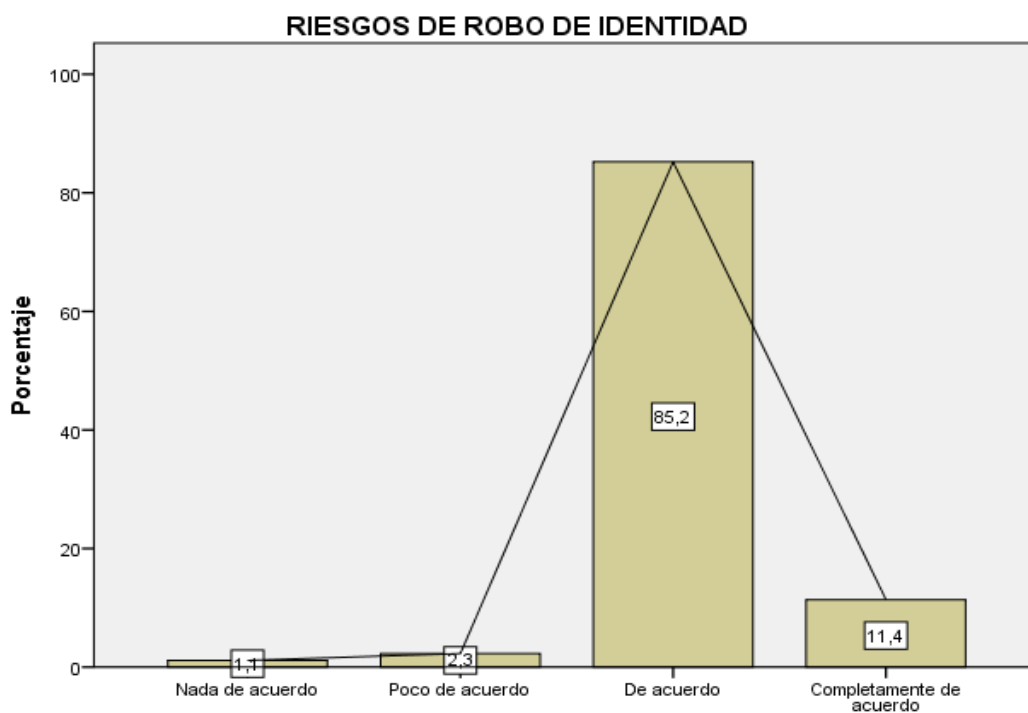
Riesgos de robo de identidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Nada de acuerdo	1	1,1	1,1	1,1
Poco de acuerdo	2	2,3	2,3	3,4
De acuerdo	75	85,2	85,2	88,6
Completamente de acuerdo	10	11,4	11,4	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable ciberdelito.

Fuente: Elaboración propia

Figura 4



P4

Análisis:

Para la primera pregunta el 11.4% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que el órgano de control interno debe prevenir los riesgos de robo de identidad de funcionarios asegurando los sistemas informáticos de las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 85.2% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que el órgano de control interno debe prevenir los riesgos de robo de identidad de funcionarios asegurando los sistemas informáticos de las municipalidades Distritales o Provinciales.

Al mismo tiempo el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que el órgano de control interno debe prevenir los riesgos de robo de identidad de funcionarios asegurando los sistemas informáticos de las municipalidades Distritales o Provinciales.

En el caso del siguiente resultado, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que el órgano de control interno debe prevenir los riesgos de robo de identidad de funcionarios asegurando los sistemas informáticos de las municipalidades Distritales o Provinciales.

4.5. Dimensión: Riesgos informáticos en el desvío de fondos

Está usted de acuerdo que los riesgos informáticos en el desvío de fondos es por la falta de seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

Tabla 5.

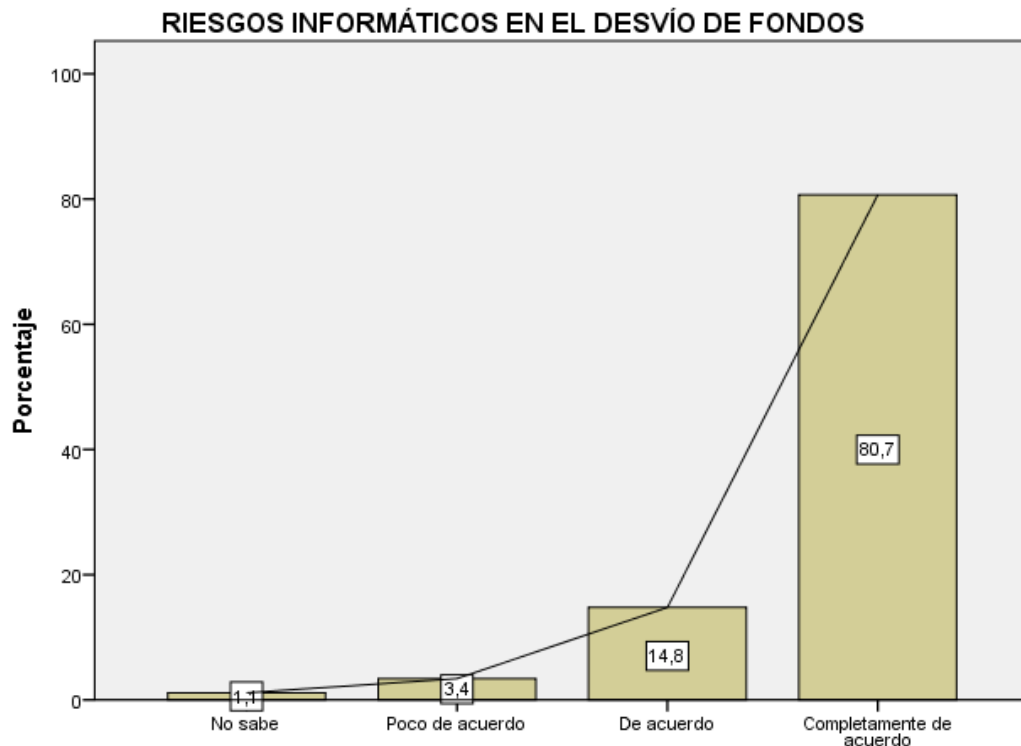
Riesgos informáticos en el desvío de fondos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	1	1,1	1,1	1,1
Poco de acuerdo	3	3,4	3,4	4,5
Válidos De acuerdo	13	14,8	14,8	19,3
Completamente de acuerdo	71	80,7	80,7	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable ciberdelito.

Fuente: Elaboración propia

Figura 5



Análisis:

Para la primera pregunta el 80.7% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que los riesgos informáticos en el desvío de fondos es por la falta de seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 14.8% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que los riesgos informáticos en el desvío de fondos es por la falta de seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

Al mismo tiempo el 3.4% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que los riesgos informáticos en el desvío de fondos es por la falta de seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

Por último, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, respondieron no saber.

4.6. Dimensión: Riesgos informáticos en el desvío de fondos

Está usted de acuerdo que los riesgos informáticos en el desvío de fondos deben tener un aseguramiento de calidad por parte del control interno de las municipalidades Distritales o Provinciales.

Tabla 6.

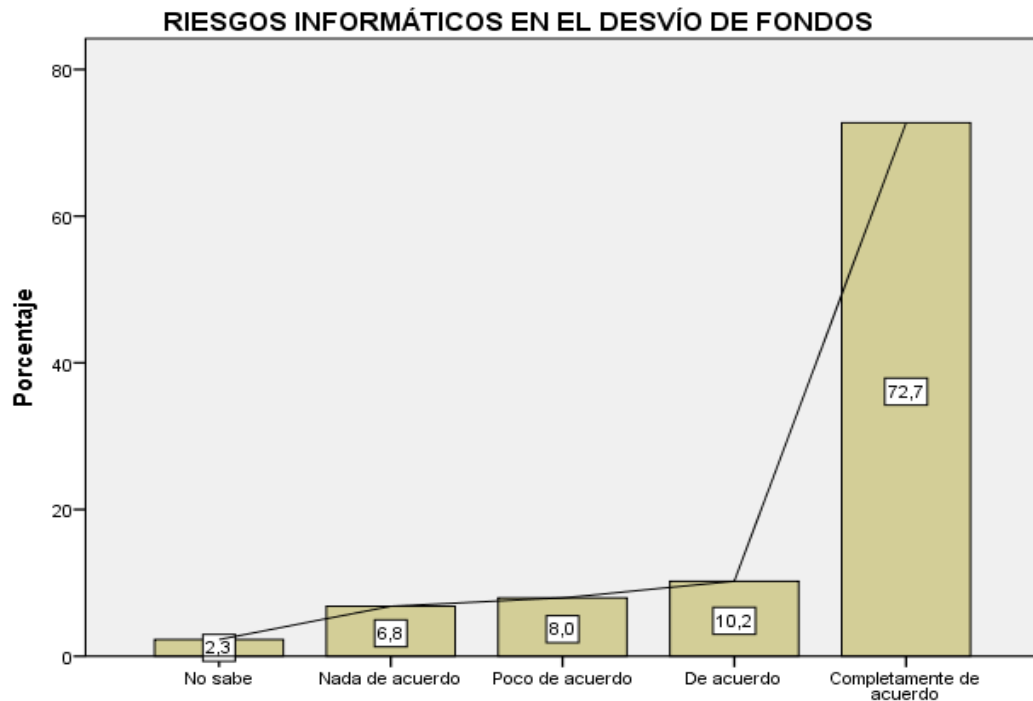
Riesgos informáticos en el desvío de fondos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	2	2,3	2,3	2,3
Nada de acuerdo	6	6,8	6,8	9,1
Poco de acuerdo	7	8,0	8,0	17,0
De acuerdo	9	10,2	10,2	27,3
Completamente de acuerdo	64	72,7	72,7	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable ciberdelito.

Fuente: Elaboración propia

Figura 6



Análisis:

Para la primera pregunta el 72.7% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que los riesgos informáticos en el desvío de fondos deben tener un aseguramiento de calidad por parte del control interno de las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 10.2% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que los riesgos informáticos en el desvío de fondos deben tener un aseguramiento de calidad por parte del control interno de las municipalidades Distritales o Provinciales.

Al mismo tiempo el 8.0% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que los riesgos informáticos en el desvío de fondos deben tener un aseguramiento de calidad por parte del control interno de las municipalidades Distritales o Provinciales.

En el caso del siguiente resultado, el 6.8% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que los riesgos informáticos en el desvío de fondos deben tener un aseguramiento de calidad por parte del control interno de las municipalidades Distritales o Provinciales.

Por último, el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, respondieron no saber.

4.7. Dimensión: Auditor interno antifraude

Está usted de acuerdo que la implementación de estrategias de antifraude para la protección de fondos debe estar evidenciado por el auditor interno de las municipalidades Distritales o Provinciales.

Tabla 7.

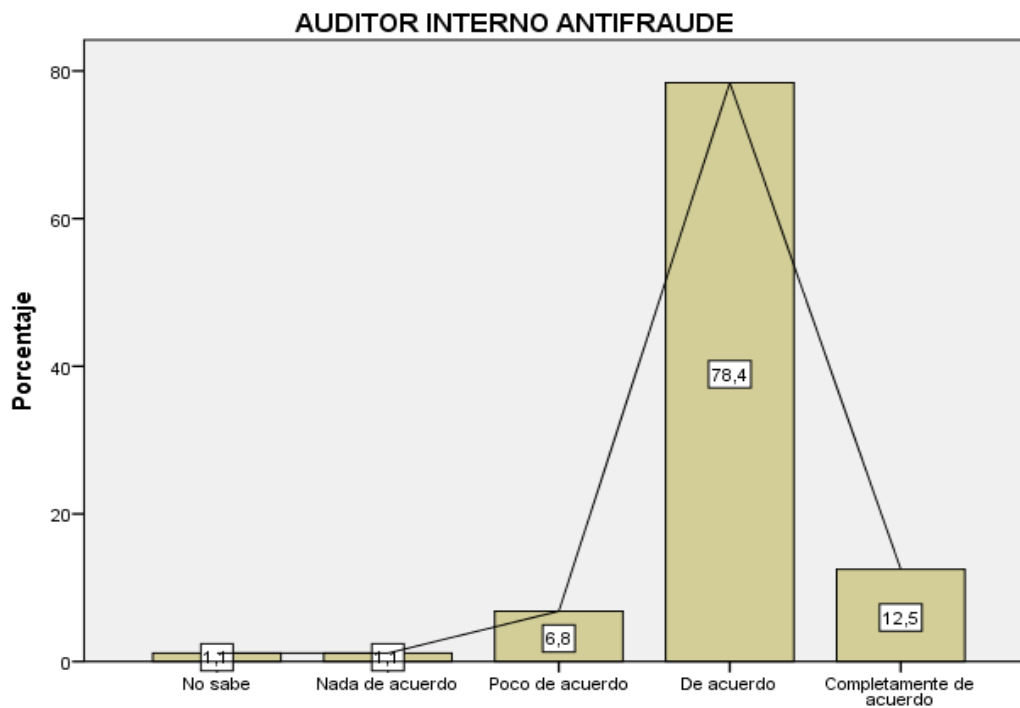
Auditor interno antifraude

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	1	1,1	1,1	1,1
Nada de acuerdo	1	1,1	1,1	2,3
Poco de acuerdo	6	6,8	6,8	9,1
De acuerdo	69	78,4	78,4	87,5
Completamente de acuerdo	11	12,5	12,5	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable responsabilidad de auditor interno.

Fuente: Elaboración propia

Figura 7



P7

Análisis:

Para la primera pregunta el 12.5% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que la implementación de estrategias de antifraude para la protección de fondos debe estar evidenciado por el auditor interno de las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 78.4% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que la implementación de estrategias de antifraude para la protección de fondos debe estar evidenciado por el auditor interno de las municipalidades Distritales o Provinciales.

Al mismo tiempo el 6.8% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que la implementación de estrategias de antifraude para la protección de fondos debe estar evidenciado por el auditor interno de las municipalidades Distritales o Provinciales.

En el caso del siguiente resultado, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que la implementación de estrategias de antifraude para la protección de fondos debe estar evidenciado por el auditor interno de las municipalidades Distritales o Provinciales.

Por último, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, respondieron no saber.

4.8. Dimensión: Auditor interno antifraude

Está usted de acuerdo que las medidas antifraude para la protección de fondos por los riesgos tecnológicos existentes en las municipalidades Distritales o Provinciales.

Tabla 8.

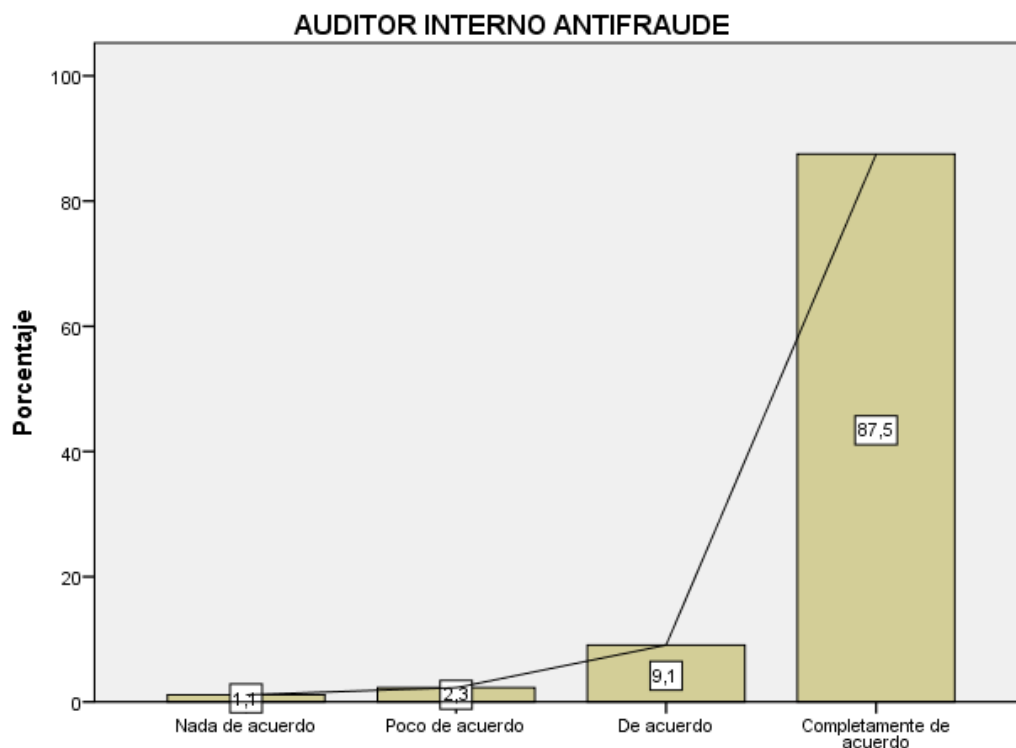
Auditor interno antifraude

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Nada de acuerdo	1	1,1	1,1	1,1
Poco de acuerdo	2	2,3	2,3	3,4
Válidos De acuerdo	8	9,1	9,1	12,5
Completamente de acuerdo	77	87,5	87,5	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable responsabilidad de auditor interno.

Fuente: Elaboración propia

Figura 8



Análisis:

Para la primera pregunta el 87.5% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que las medidas antifraude para la protección de fondos por los riesgos tecnológicos existentes en las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 9.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que las medidas antifraude para la protección de fondos por los riesgos tecnológicos existentes en las municipalidades Distritales o Provinciales.

Al mismo tiempo el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que las medidas antifraude para la protección de fondos por los riesgos tecnológicos existentes en las municipalidades Distritales o Provinciales.

En el caso del siguiente resultado, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que las medidas antifraude para la protección de fondos por los riesgos tecnológicos existentes en las municipalidades Distritales o Provinciales.

4.9. Dimensión: Prevención de los sistemas informáticos

Está usted de acuerdo que la falta de prevención de los sistemas informáticos evidencia la falencia en el control interno de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Tabla 9.

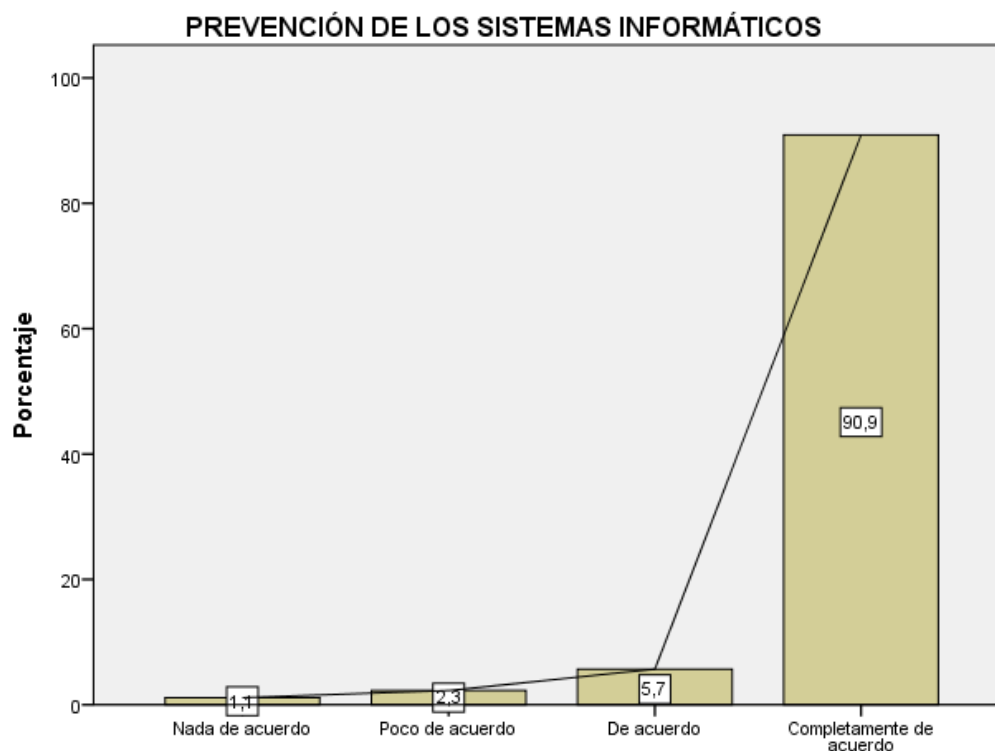
Prevención de los sistemas informáticos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Nada de acuerdo	1	1,1	1,1	1,1
Poco de acuerdo	2	2,3	2,3	3,4
Válidos De acuerdo	5	5,7	5,7	9,1
Completamente de acuerdo	80	90,9	90,9	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable responsabilidad de auditor interno.

Fuente: Elaboración propia

Figura 9



Análisis:

Para la primera pregunta el 90.9% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que la falta de prevención de los sistemas informáticos evidencia la falencia en el control interno de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

El siguiente resultado se observó que el 5.7% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que la falta de prevención de los sistemas informáticos evidencia la falencia en el control interno de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Al mismo tiempo el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que la falta de prevención de los sistemas informáticos evidencia la falencia en el control interno de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

En el caso del siguiente resultado, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que la falta de prevención de los sistemas informáticos evidencia la falencia en el control interno de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

4.10. Dimensión: Prevención de los sistemas informáticos

Está usted de acuerdo que la prevención de los sistemas informáticos se debe implementar con las áreas críticas de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Tabla 10.

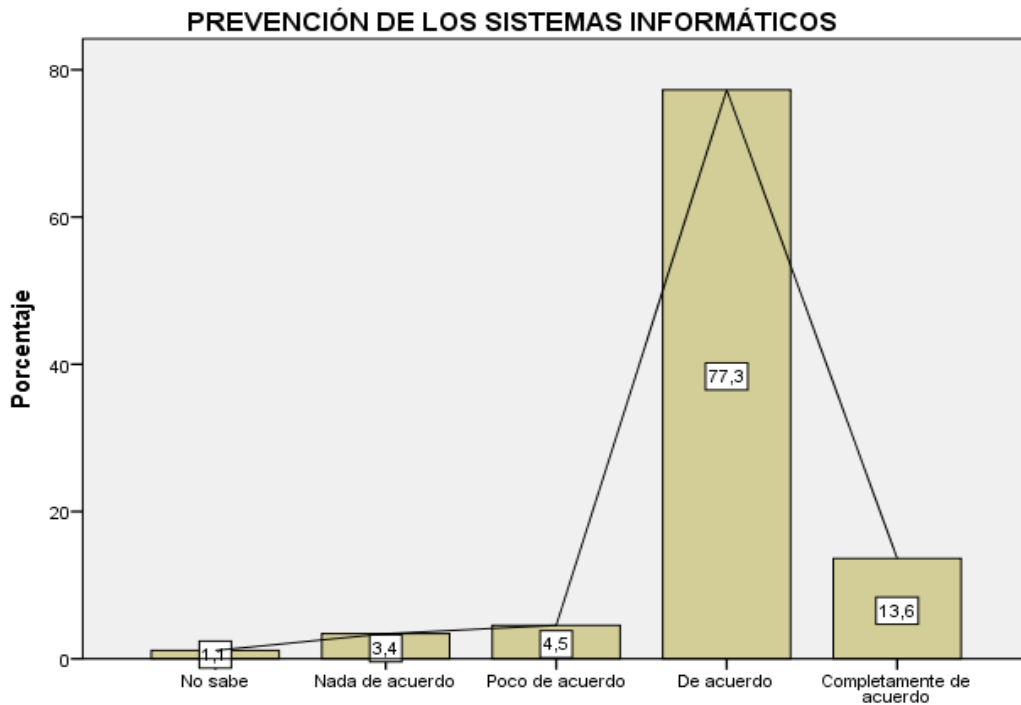
Prevención de los sistemas informáticos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	1	1,1	1,1	1,1
Nada de acuerdo	3	3,4	3,4	4,5
Poco de acuerdo	4	4,5	4,5	9,1
Válidos De acuerdo	68	77,3	77,3	86,4
Completamente de acuerdo	12	13,6	13,6	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable responsabilidad de auditor interno.

Fuente: Elaboración propia

Figura 10



P10

Análisis:

Para la primera pregunta el 13.6% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que la prevención de los sistemas informáticos se debe implementar con las áreas críticas de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

El siguiente resultado se observó que el 77.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que la prevención de los sistemas informáticos se debe implementar con las áreas críticas de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Al mismo tiempo el 4.5% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que la prevención de los sistemas informáticos se debe implementar con las áreas críticas de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

En el caso del siguiente resultado, el 3.4% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están nada de acuerdo que la prevención de los sistemas informáticos se debe implementar con las áreas críticas de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.

Por último, el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, respondieron no saber.

4.11. Dimensión: Seguridad razonable

Está usted de acuerdo que el desvío de fondos es por la falta de seguridad razonable por el control interno de las municipalidades Distritales o Provinciales.

Tabla 11.

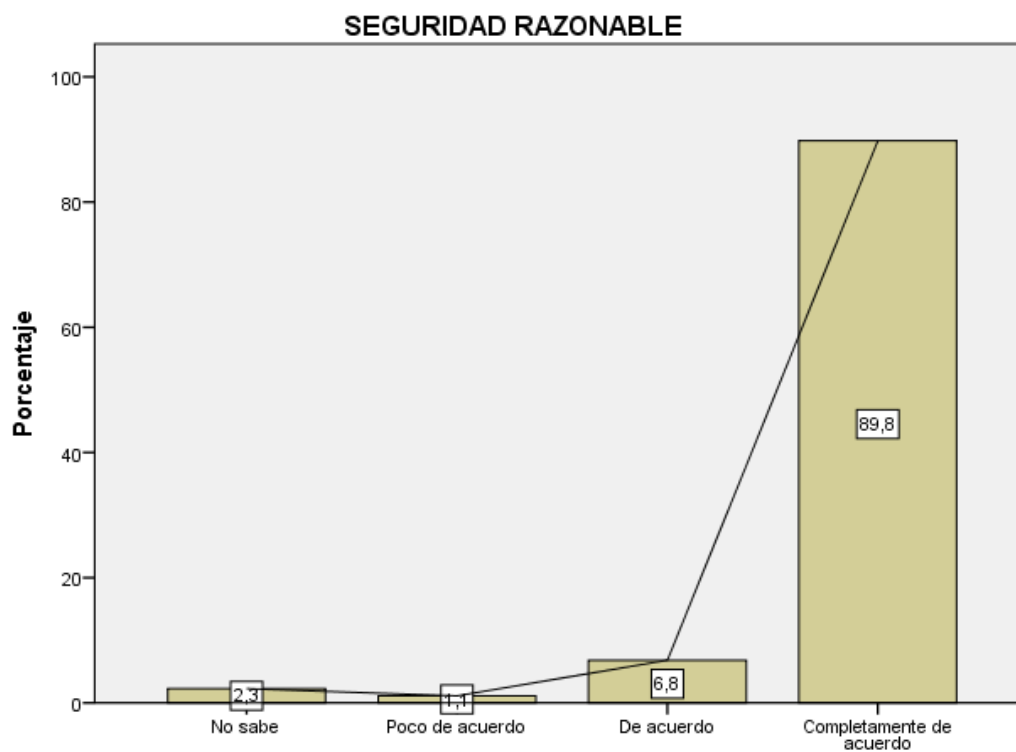
Seguridad razonable

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No sabe	2	2,3	2,3	2,3
Poco de acuerdo	1	1,1	1,1	3,4
Válidos De acuerdo	6	6,8	6,8	10,2
Completamente de acuerdo	79	89,8	89,8	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable responsabilidad de auditor interno.

Fuente: Elaboración propia

Figura 11



Análisis:

Para la primera pregunta el 89.8% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que el desvío de fondos es por la falta de seguridad razonable por el control interno de las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 6.8% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que el desvío de fondos es por la falta de seguridad razonable por el control interno de las municipalidades Distritales o Provinciales.

Al mismo tiempo el 1.1% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que el desvío de fondos es por la falta de seguridad razonable por el control interno de las municipalidades Distritales o Provinciales.

Por último, el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, respondieron no saber.

4.12. Dimensión: Seguridad razonable

Está usted de acuerdo que la carencia en estrategias de control electrónico genera el desvío de fondos en las municipalidades Distritales o Provinciales.

Tabla 12.

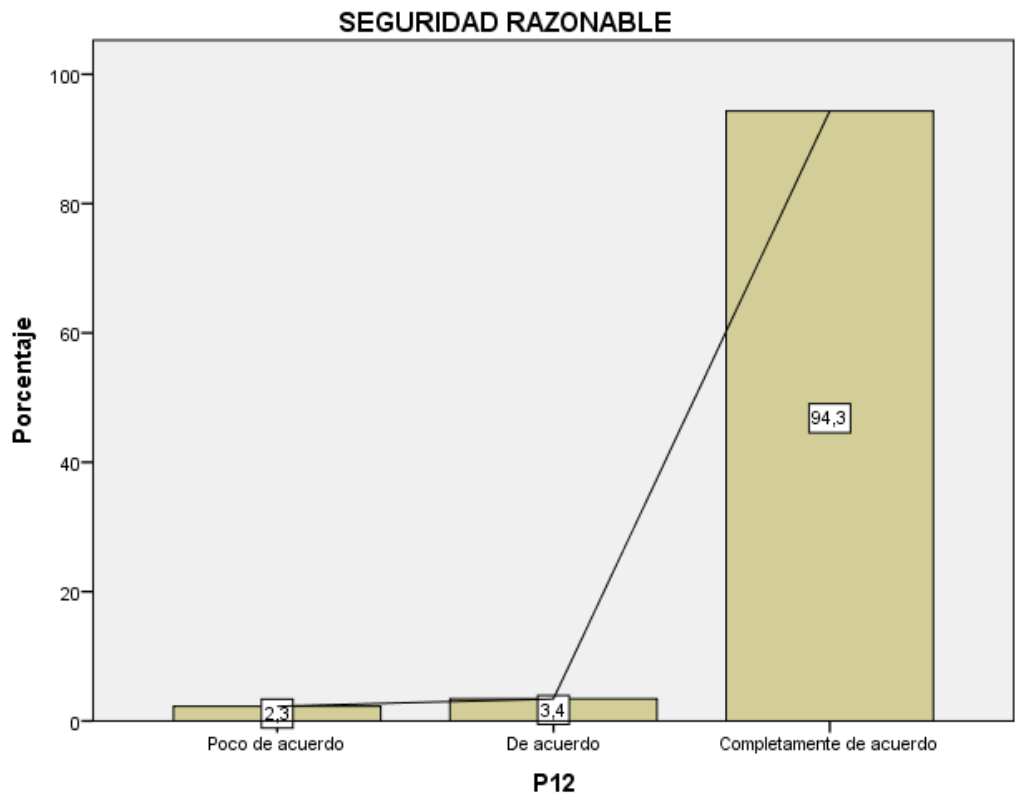
Seguridad razonable

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Poco de acuerdo	2	2,3	2,3	2,3
De acuerdo	3	3,4	3,4	5,7
Completamente de acuerdo	83	94,3	94,3	100,0
Total	88	100,0	100,0	

Nota: Dimensión correspondiente a la variable responsabilidad de auditor interno.

Fuente: Elaboración propia

Figura 12



Análisis:

Para la primera pregunta el 94.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están completamente de acuerdo que la carencia en estrategias de control electrónico genera el desvío de fondos en las municipalidades Distritales o Provinciales.

El siguiente resultado se observó que el 3.4% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están de acuerdo que la carencia en estrategias de control electrónico genera el desvío de fondos en las municipalidades Distritales o Provinciales.

Al mismo tiempo el 2.3% de los servidores públicos de la Municipalidad Provincial de Padre Abad, contestaron que están poco de acuerdo que la carencia en estrategias de control electrónico genera el desvío de fondos en las municipalidades Distritales o Provinciales.

ANÁLISIS INFERENCIAL

PRUEBA DE HIPÓTESIS GENERAL

H1: Existe grado de relación entre el ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.

H0: No existe grado de relación entre el ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.

Tabla de contingencia CIBERDELITO * RESPONSABILIDAD DE AUDITOR INTERNO

			RESPONSABILIDAD DE AUDITOR INTERNO		Total
			De acuerdo	Completamente de acuerdo	
CIBERDELITO	De acuerdo	Recuento	6	29	35
		Frecuencia esperada	10,3	24,7	35,0
		% del total	6,8%	33,0%	39,8%
O	Completamente de acuerdo	Recuento	20	33	53
		Frecuencia esperada	15,7	37,3	53,0
		% del total	22,7%	37,5%	60,2%
Total		Recuento	26	62	88
		Frecuencia esperada	26,0	62,0	88,0
		% del total	29,5%	70,5%	100,0%

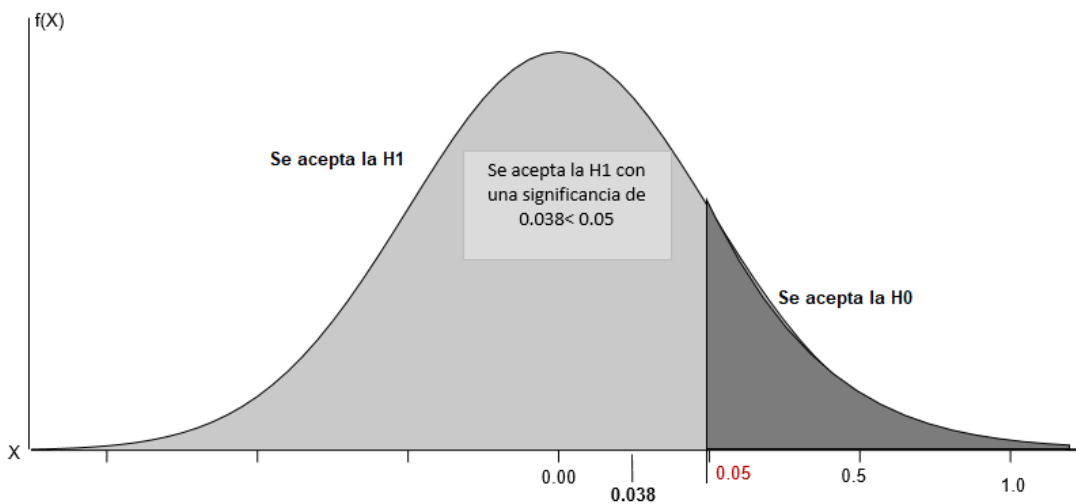
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	4,294 ^a	1	,038		
Corrección por continuidad ^b	3,362	1	,067		
Razón de verosimilitudes	4,503	1	,034		
Estadístico exacto de Fisher				,056	,032
Asociación lineal por lineal	4,246	1	,039		
N de casos válidos	88				

INTERPRETACIÓN

Para el análisis se utilizó la prueba de Chi-cuadrada donde se determinó que el grado de significancia es de $0.038 < 0.05$, de modo que se acepta la hipótesis alternativa, es decir que existe grado de relación entre el ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.

GRÁFICA DEL NIVEL DE SIGNIFICANCIA



HIPÓTESIS ESPECÍFICA I

H1: Establecer la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

H0: No existe relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

Tabla de contingencia RIESGOS TECNOLÓGICOS * AUDITOR INTERNO ANTIFRAUDE

			AUDITOR INTERNO ANTIFRAUDE			Total
			Poco de acuerdo	De acuerdo	Completamente de acuerdo	
RIESGOS TECNOLÓGICOS	Poco de acuerdo	Recuento	2	0	1	3
		Frecuencia esperada	,1	,5	2,4	3,0
		% del total	2,3%	0,0%	1,1%	3,4%
	De acuerdo	Recuento	0	2	12	14
		Frecuencia esperada	,6	2,4	11,0	14,0
		% del total	0,0%	2,3%	13,6%	15,9%
	Completamente de acuerdo	Recuento	2	13	56	71
		Frecuencia esperada	3,2	12,1	55,7	71,0
		% del total	2,3%	14,8%	63,6%	80,7%
Total	Recuento	4	15	69	88	
	Frecuencia esperada	4,0	15,0	69,0	88,0	
	% del total	4,5%	17,0%	78,4%	100,0%	

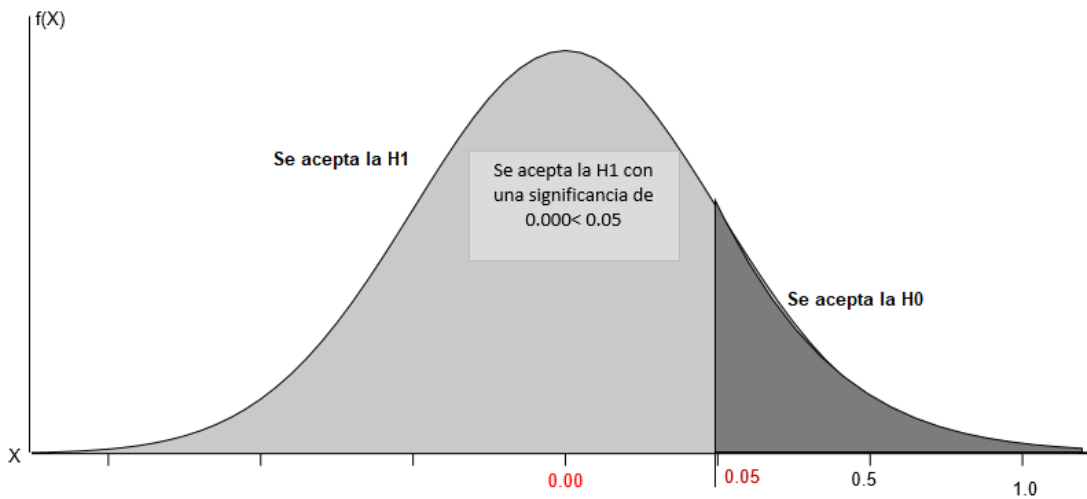
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	28,088 ^a	4	,000
Razón de verosimilitudes	11,070	4	,026
Asociación lineal por lineal	3,696	1	,055
N de casos válidos	88		

INTERPRETACIÓN

Para el análisis se utilizó la prueba de Chi-cuadrada donde se determinó que el grado de significancia es de $0.000 < 0.05$, de modo que se acepta la hipótesis alternativa, es decir que se establece una relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales.

GRÁFICA DEL NIVEL DE SIGNIFICANCIA



HIPÓTESIS ESPECÍFICA II

H1: Determinar la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales.

H0: No existe una relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales.

Tabla de contingencia RIESGOS DE ROBO DE IDENTIDAD * PREVENCIÓN DE LOS SISTEMAS INFORMÁTICOS

			PREVENCIÓN DE LOS SISTEMAS INFORMÁTICOS			Total
			Poco de acuerdo	De acuerdo	Completamente de acuerdo	
RIESGOS DE ROBO DE IDENTIDAD	Poco de acuerdo	Recuento	1	0	2	3
		Frecuencia esperada	,0	,9	2,1	3,0
		% del total	1,1%	0,0%	2,3%	3,4%
	De acuerdo	Recuento	0	9	19	28
		Frecuencia esperada	,3	8,3	19,4	28,0
		% del total	0,0%	10,2%	21,6%	31,8%
	Completamente de acuerdo	Recuento	0	17	40	57
		Frecuencia esperada	,6	16,8	39,5	57,0
		% del total	0,0%	19,3%	45,5%	64,8%
Total	Recuento	1	26	61	88	
	Frecuencia esperada	1,0	26,0	61,0	88,0	
	% del total	1,1%	29,5%	69,3%	100,0%	

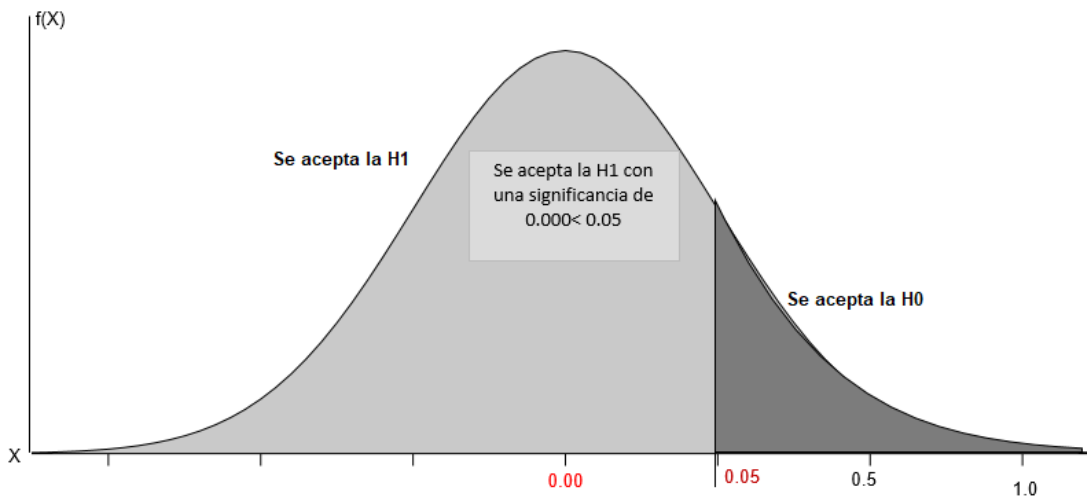
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	29,303 ^a	4	,000
Razón de verosimilitudes	8,612	4	,072
Asociación lineal por lineal	,731	1	,393
N de casos válidos	88		

INTERPRETACIÓN

Para el análisis se utilizó la prueba de Chi-cuadrada donde se determinó que el grado de significancia es de $0.000 < 0.05$, de modo que se acepta la hipótesis alternativa, es decir que se determina una relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales.

GRÁFICA DEL NIVEL DE SIGNIFICANCIA



HIPÓTESIS ESPECÍFICA III

H1: Analizar la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

H0: No existe una relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

Tabla de contingencia RIESGOS INFORMÁTICOS EN EL DESVÍO DE FONDOS * SEGURIDAD RAZONABLE

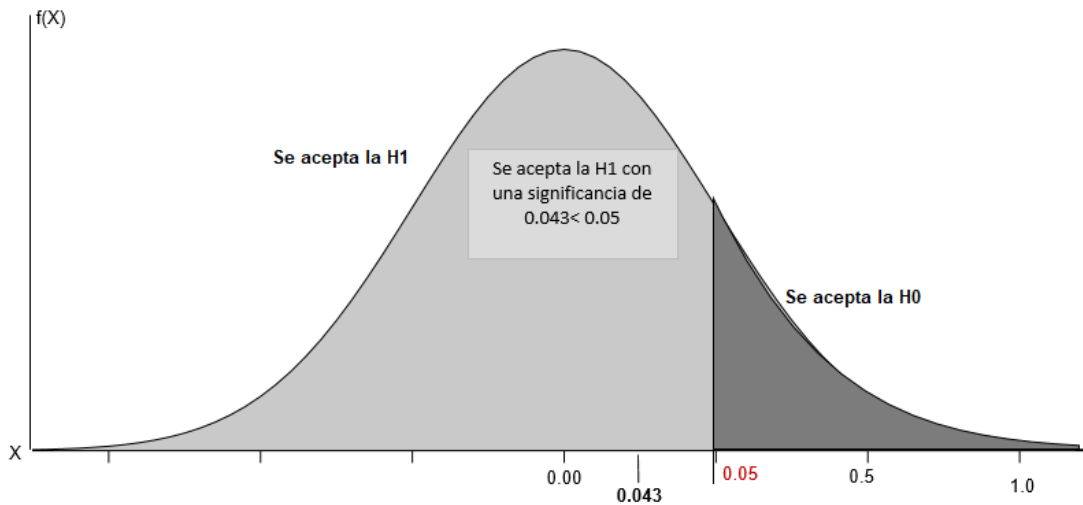
			SEGURIDAD RAZONABLE			Total
			Poco de acuerdo	De acuerdo	Completamente de acuerdo	
RIESGOS INFORMÁTICOS EN EL DESVÍO DE FONDOS	Poco de acuerdo	Recuento	0	0	3	3
		Frecuencia esperada	,0	,3	2,7	3,0
		% del total	0,0%	0,0%	3,4%	3,4%
	De acuerdo	Recuento	0	5	13	18
		Frecuencia esperada	,2	1,6	16,2	18,0
		% del total	0,0%	5,7%	14,8%	20,5%
	Completamente de acuerdo	Recuento	1	3	63	67
		Frecuencia esperada	,8	6,1	60,1	67,0
		% del total	1,1%	3,4%	71,6%	76,1%
Total	Recuento	1	8	79	88	
	Frecuencia esperada	1,0	8,0	79,0	88,0	
	% del total	1,1%	9,1%	89,8%	100,0%	

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	9,857 ^a	4	,043
Razón de verosimilitudes	8,295	4	,081
Asociación lineal por lineal	1,764	1	,184
N de casos válidos	88		

INTERPRETACIÓN

Para el análisis se utilizó la prueba de Chi-cuadrada donde se determinó que el grado de significancia es de $0.043 < 0.05$, de modo que se acepta la hipótesis alternativa, es decir que existe una relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

GRÁFICA DEL NIVEL DE SIGNIFICANCIA

CONCLUSIONES

- Se concluye que hay una estrecha relación entre los riesgos tecnológicos y la implementación de un área de prevención con un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales. De los resultados obtenidos el 92,00% esta completamente de acuerdo que los riesgos tecnológicos tiene relación la implementación de un área de prevención con un auditor interno antifraude de los fondos, el 1,10% no sabe al respecto.
- Se concluye que hay una estrecha relación entre los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales. De los resultados obtenidos el 68,20% está completamente de acuerdo los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos, el 1,10% no sabe al respecto.
- Se concluye que hay una estrecha relación entre los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales. De los resultados obtenidos el 89,70% está completamente de acuerdo que los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno, el 1,10% no sabe al respecto.

SUGERENCIAS

- Ante los riesgos tecnológicos es necesario que las entidades gubernamentales tomen acciones o estrategias, implementando un área de prevención con un auditor interno antifraude de los fondos que tenga la experticia y la capacidad para dichos controles en las municipalidades Distritales o Provinciales.
- Ante los riesgos de robo de identidad de funcionarios de áreas claves se deben crear mecanismos de control y aseguramiento de calidad con una adecuada prevención de los sistemas informáticos por personal especializado a fin de evitar estas modalidades delictivas que afectan a las municipalidades Distritales o Provinciales.
- Ante los riesgos informáticos en el desvío de fondos el personal de áreas críticas deben estar altamente capacitados para conocer sobre las modalidades de los ciberdelitos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.

REFERENCIAS BIBLIOGRÁFICAS

- Acuña Lopez, L. F., & Villa Motato, S. M. (2018). *Estado actual del cibercrimen en Colombia con respecto a Latinoamerica*. Pereira: <https://repository.unad.edu.co/bitstream/handle/10596/25619/%20%09lfacunal.pdf?sequence=1>.
- Alarcon Ariza, D. A., & Barrera Barón, J. A. (2017). *Uso de internet y delito informático en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. Escuela de Posgrado. Lima, Perú: Universidad Privada Norbert Wiener.
- Alfaro Soto, J. W. (2019). *Auditoría de Sistemas Informáticos*. Perú: Universidad José Carlos Mariátegui.
- Álvarez Carpentier, T. (1996). *La represión del delito tributario como modalidad de delito económico*. Lima, Perú: Revista PUCP - Derecho & Sociedad.
- Arroyo Morales, A. (2020). *Metodología de la investigación en las ciencias empresariales*. Cusco: <http://repositorio.unsaac.edu.pe>.
- Blossiers Mazzini, J. J. (2018). *El delito informático y su incidencia en la empresa bancaria*. Escuela Universitaria de Posgrado. Lima, Perú: Universidad Nacional Federico Villareal.
- Contraloría General de la República. (2020). *Sistema nacional de Control*. Lima: https://apps.contraloria.gob.pe/packanticorrupcion/control_interno.html.
- Cuba Ninamango, N. A. (2020). *Incongruencia en la redacción del delito de banda criminal para diferenciarlo del delito de organización criminal*. Perú: Grupo Educativo Universidad Privada de Ica.

- Flores Vidal, J. G. (2020). *Los ciberdelitos: la otra pandemia que avanzó en silencio en el Perú*. Lima: <https://pagina3.pe/2020/10/14/los-ciberdelitos-la-otra-pandemia-que-avanzo-en-silencio-en-el-peru/>.
- Gamarra Pineda, A. C. (2010). *Diseño de un modelo de evaluación de riesgos ocupacionales con soporte informático*. Perú: Universidad Nacional de Ingeniería.
- Gaviria, P. (2016). *Aplicación de metodología de malware para el análisis de la amenaza avanzada persistente (APT) "Poison Ivy"*. San Juan de Pasto: Universidad Internacional de la Rioja.
- Gomero Oré, K. (2017). *Prevención de riesgos laborales*. Perú: Universidad César Vallejo.
- Granados Ramírez, R., & Parra Rojas, A. C. (2014). *El delito de hurto por medios informáticos que tipifica el artículo 2691 de la Ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cucuta en el periodo 2012-2014*. Cucuta Colombia: <https://repository.unilibre.edu.co/bitstream/handle/10901/9310/trabajodegrado.pdf?sequence=1&isAllowed=y>.
- Guevara Arce, C. (2018). *Auditoría Tributaria*. Perú: Universidad Nacional de la Amazonía Peruana.
- Henao Feria, Y. (2017). *Importancia del control interno como herramienta en la detección y prevención de riesgos empresariales*. Zarzal: <https://bibliotecadigital.univalle.edu.co/bitstream/handle/10893/11020/0567378.pdf;jsessionid=F92ADD07E82347E07EDB4686D093B1EF?sequence=1>.
- Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación*. Mexico: Mc Graw-Hill.

- Hudson Analytix. (2017). *Glosario de seguridad Cibernética para la Comisión Interamericana de Puertos Organización de los Estados Americanos*. Washington, DC, EE.UU.: HudsonAnalytix, Inc.
- Interpol. (2020). *Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad*. Estados Unidos: <https://www.interpol.int/es/Delitos/Ciberdelincuencia>.
- Microsoft Press. (2005). *Diccionario de informática e internet*. Anaya Multimedia.
- Montoya Vivanco, Y. (2013). *Estudios críticos sobre los delitos de corrupción de funcionarios en Perú*. Lima: Grafica Delvi S.R.L.
- Palomino Ochoa, J. J., & et.al. (2021). *Metodos de investigación y praxis cuantitativa*. Huancayo: Corporación Atlas.
- Pardo Vargas, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*. Escuela de Posgrado. Lima, Perú: Universidad César Vallejo.
- Quevedo Gonzales, J. (2017). *Investigación y prueba del ciberdelito*. Barcelona: Universitat de Barcelona España.
- Quevedo Gonzáles, J. (2017). *Investigación y prueba del Ciberdelito*. Barcelona España: Universitat de Barcelona.
- Quiroz Quezada, P. R. (2015). *Acciones de saneamiento contable en las entidades gubernamentales*. Perú: Revista UNALM - Ecología Aplicada.
- Revista Alva Journal. (1990). *Responsabilidad Profesional*. Perú: Revista PUCP - Themis.

- Serrano Buitrago, E. R. (2014). *La práctica de delitos informáticos en Colombia*. Bogotá:
<https://repository.unimilitar.edu.co/bitstream/handle/10654/13452/Ensayo%20%20Edison%20Serrano%20EAS.pdf?sequence=1&isAllowed=y>.
- Taminchi Santillan, J. D. (2014). *Seguridad Informática*. Perú: Universidad Nacional de la Amazonía Peruana.
- UNODC, O. y. (2013). *Manual sobre los delitos relacionados con la identidad*. Nueva York: Oficina de Naciones Unidas en Viena.
- Vilca Aira, G. L. (2018). *Los hackers: delito informático frente al código penal peruano*. Facultad de Derecho y Ciencias Políticas. Anchas, Perú: Universidad Nacional Santiago Antúnez de Mayolo.
- Villegas Cotrina, D. G. (2020). *Sistema de control interno*. Perú: Universidad de Piura.

ANEXOS

ANEXO Nº 01
MATRIZ DE CONSISTENCIA LÓGICA
TÍTULO: “EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGIÓN DE UCAYALI, AÑO 2020”.

PROBLEMA	HIPOTESIS	OBJETIVOS	OPERACIONALIZACIÓN DE VARIABLES				
			VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTO	METODOLOGÍA
<p>PROBLEMA GENERAL ¿Cuál es la relación del ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020?</p> <p>PROBLEMAS ESPECÍFICOS - ¿Cuál es la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales? - ¿Cuál es la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales? - ¿Cuál es la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales?</p>	<p>HIPOTESIS GENERAL Existe grado de relación entre el ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.</p> <p>HIPOTESIS ESPECÍFICOS - Establecer la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales. - Determinar la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales. - Analizar la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.</p>	<p>GENERAL Establecer la relación del ciberdelito de redes delictivas a escala global a las entidades gubernamentales y la responsabilidad de los auditores internos en una municipalidad de la Región de Ucayali-2020.</p> <p>OBJETIVOS ESPECÍFICOS - Establecer la relación de los riesgos tecnológicos y la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales. - Determinar la relación de los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales. - Analizar la relación de los riesgos informáticos en el desvío de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales.</p>	<p>Independiente Ciberdelito (Escala de medición mixta)</p>		<p>X1: Riesgos Tecnológicos X2: Riesgos de robo de identidad X3: Riesgos informáticos en el desvío de fondos</p>	<p>Cuestionario de pruebas objetiva y de desarrollo</p>	<p>*Población (N): 186 *Muestra (n): 88 *Tipo de Investigación Descriptivo correlacional *Diseño de Investigación: Correlación</p> 
			<p>Dependiente Responsabilidad de auditor interno (Escala de medición mixta)</p>		<p>Y1: Auditor interno antifraude Y2: Prevención de los sistemas informáticos Y3: seguridad razonable</p>	<p>Cuestionario de prueba objetiva</p>	<p>*Técnicas Para Acopio de datos: Fichas *Instrumentos de Recolección de datos: Pruebas campo *Técnicas el Para Análisis e Interpretación de Datos: Estadística descriptiva e inferencial para cada variable *Para el Informe Final: Reglamento general de Grados y Títulos de la FCEAyC de la UNU.</p>
			<p>Interviniente Contribuyentes ciudad de Pucallpa</p>		<p>Municipalidad de la Región de Ucayali, 2020</p>		



Anexo 03
UNIVERSIDAD NACIONAL DE UCAYALI
Facultad de Ciencias Económicas Administrativas
y Contables
Escuela Profesional de Contabilidad

Código de encuesta: _____

ENCUESTA - INSTRUCCIONES:

Tesis titulada “**EL CIBERDELITO DE REDES DELICTIVAS A ESCALA GLOBAL A ENTIDADES GUBERNAMENTALES Y LA RESPONSABILIDAD DEL ORGANO DE CONTROL INTERNO EN UNA MUNICIPALIDAD DE LA REGIÓN DE UCAYALI, AÑO 2020**”; marcar las alternativas que considere correctas con una (X):

Ítems	5	4	3	2	1
	Completamente de acuerdo	De acuerdo	Poco de acuerdo	Nada de acuerdo	No sabe

Ítems	5	4	3	2	1
I RIESGOS TECNOLÓGICOS					
1. Está usted de acuerdo que los riesgos tecnológicos deben ser prevenidos con la implementación de un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales					

<p>2. Está usted de acuerdo que cibercrimen de redes delictivas a escala global a las entidades gubernamentales genera responsabilidad de los auditores internos por la falta de prevención en una municipalidad de la Región de Ucayali-2020</p>					
<p>II. RIESGOS DE ROBO DE IDENTIDAD</p>					
<p>3. Está de acuerdo que los riesgos de robo de identidad de funcionarios son por la falta de prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020.</p>					
<p>4. Está de acuerdo que el órgano de control interno debe prevenir los riesgos de robo de identidad de funcionarios asegurando los sistemas informáticos de las municipalidades Distritales o Provinciales</p>					
<p>III. RIESGOS INFORMÁTICOS EN EL DESVÍO DE FONDOS</p>					

5. Está usted de acuerdo que los riesgos informáticos en el desvío de fondos es por la falta de seguridad razonable del control interno de las municipalidades Distritales o Provinciales.					
6. Está usted de acuerdo que los riesgos informáticos en el desvío de fondos deben tener un aseguramiento de calidad por parte del control interno de las municipalidades Distritales o Provinciales.					
IV. AUDITOR INTERNO ANTIFRAUDE					
7. Está usted de acuerdo que la implementación de estrategias de antifraude para la protección de fondos debe estar evidenciado por el auditor interno de las municipalidades Distritales o Provinciales.					
8. Está usted de acuerdo que las medidas antifraude para la protección de fondos por los riesgos tecnológicos existentes en las municipalidades Distritales o Provinciales.					
V. PREVENCIÓN DE LOS SISTEMAS INFORMÁTICOS					

<p>9. Está usted de acuerdo que la falta de prevención de los sistemas informáticos evidencia la falencia en el control interno de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020</p>					
<p>10. Está usted de acuerdo que la prevención de los sistemas informáticos se debe implementar con las áreas críticas de las municipalidades Distritales o Provinciales de la Región de Ucayali-2020</p>					
<p>VI. SEGURIDAD RAZONABLE</p>					
<p>11. Está usted de acuerdo el desvío de fondos es por la falta de seguridad razonable por el control interno de las municipalidades Distritales o Provinciales.</p>					
<p>12. Está usted de acuerdo que la carencia en estrategias de control electrónico genera el desvío de fondos en las municipalidades Distritales o Provinciales.</p>					