CENTRO DE ALTOS ESTUDIOS NACIONALES

ESCUELA DE POST GRADO

TESIS

EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL

PARA OPTAR EL GRADO ACADÉMICO DE DOCTOR EN DESARROLLO Y SEGURIDAD ESTRATEGICA

PRESENTADO POR: MIRIAM CHILCON SILVA

CAEN - 2019

AGRADECIMIENTO

Mi agradecimiento y reconocimiento al Centro de Altos Estudios Nacionales, a las autoridades, catedráticos, asesores temáticos y metodológico, a mi asesor personal y a todas las personas que han colaborado en el presente estudio de investigación y en forma especial a mi querida familia que constituye un impulso para ser un profesional integro.

ÍNDICE

ANEXOS

RESUMEN DE TESIS

La presente investigación titulada “EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL” tiene como objetivo principal, determinar en qué medida el cibercrimen en el Perú afecta la Seguridad Nacional.

El estudio metodológicamente es de un enfoque cuantitativo, con un alcance descriptivo explicativo y un diseño de investigación no experimental, con una población del estudio, que constituyen los directores y personal con capacidad de control del cibercrimen como las instituciones de la Policía Nacional del Perú, Ministerio Publico, y del Poder Judicial, que suman un total de 580 funcionarios, y una muestra de 231 personas, utilizándose un cuestionario tipo Likert, y el uso de la prueba Chi Cuadrado para la demostración de las Hipótesis.

Durante el desarrollo de la presente investigación se llega a la siguiente conclusión general: Que el nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional.

Como esquema final del estudio se exponen las recomendaciones a las que se ha llegado, de la cuales se desprende la propuesta de aplicación de estrategias para combatir el cibercrimen.

Las palabras claves dentro de la investigación son las siguientes: Cibercrimen y Seguridad Nacional.

ABSTRACT

This research entitled "Cybercrime in Peruvian and its impact on National Security" is like target main, determine to what extent Cybercrime in the Peru affects National Security.

The study methodologically is a quantitative approach, with a descriptive explanatory scope and design of non-experimental, with a population research study, consisting of managers and staff with ability to control cyber-crime as the institutions of the Police National of the Peru, Public Ministry, and of the judiciary, adding up to a total of 580 officials, and a sample of 231 people, using a questionnaire Likert-type, and the use of the Chi square test for demonstration of the hypothesis.

During the development of this research will reach the following general conclusion: That the level reached by affects cybercrime in the Peru significantly national security.

As the final study scheme presents the recommendations which have been reached, of which follows the proposal of implementation of strategies to combat cybercrime.

Key words within the research are the following: Cybercrime and National Security.

ABSTRATO

Esta pesquisa intitulada "Cybercrime no Peru e seu impacto na Segurança Nacional" é como alvo principal, determinar em que medida Cybercrime no Peru afeta a Segurança Nacional.

O estudo metodologicamente é uma abordagem quantitativa, com um escopo explicativo descritivo e projeto de não-experimentais, com uma pesquisa da população estudo de consistindo de gerentes e funcionários, com capacidade de controlar o delito cibernético que as instituições da Polícia nacional do Peru, Ministério público e do poder judiciário, somando um total de 580 funcionáriose uma amostra de 231 pessoas, usando um questionário do tipo Likert e o uso do teste Chi quadrado para demonstração da hipótese.

Durante o desenvolvimento desta pesquisa vai chegar à seguinte conclusão geral: Que o nível alcançado por afeta o cibercrime no Peru significativamente segurança nacional.

Como o esquema de estudo final apresenta as recomendações que foram atingidos, de que segue a proposta de implementação de estratégias para combater o cibercrime.

Palavras-chave dentro da pesquisa são os seguintes: Cybercrime e segurança nacional.

ÍNDICE DE GRAFICOS

INTRODUCCIÓN

En nuestro país en las últimos tiempos, se ha acentuado una problemática que afecta a la seguridad nacional como es el cibercrimen sobre todo en aquellos sectores que asumen una responsabilidad para prevenirla, dentro de ellas las instituciones del sector defensa, es por ello que la investigación tiene como objetivo principal, determinar en qué medida el cibercrimen en el Perú afecta la Seguridad Nacional.

El estudio metodológicamente tiene un enfoque cuantitativo, con un alcance descriptivo correlacional y un diseño de investigación no experimental, con una población del estudio, que constituyen los funcionarios con responsabilidad estratégica de la la Policía Nacional del Perú, Ministerio Publico, y del Poder Judicial, que suman un total de 580 funcionarios, y una muestra de 231 personas, utilizándose un cuestionario tipo Likert, y el uso de la prueba Chi Cuadrado para la demostración de las Hipótesis.

Es por ello que dentro del presente trabajo se han estructurado cuatro capítulos, estableciéndose, así en el primero de ellos, el planteamiento del problema con la presentación de realidad problemática, formulación y objetivos que justifican su realización.

En el segundo capítulo, se hace la diferenciación teórica del tema, abordando teorías y conceptos sobre: Cibercrimen y Seguridad Nacional, tanto en forma conceptual, como su importancia y elementos principales; asimismo se presenta el marco conceptual del estudio

En el tercer capítulo se define la metodología de la investigación con la presentación de su enfoque, alcance, diseño, población del estudio, el tamaño de la muestra representativa, las hipótesis con sus variables y se presentan las técnicas e instrumentos de recolección de datos.

En el cuarto capítulo se presenta el análisis e interpretación de resultados de la investigación de campo realizada medidas a través de la prueba de chi cuadrado en la demostración de la hipótesis general y las hipótesis específicas; con las conclusiones y recomendaciones del estudio.

Finalmente, se han seleccionado las referencias bibliográficas.

Como corolario del estudio, se presentan los anexos correspondientes.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

a) En el mundo

Se considera, según el Reporte Norton (2013):

> El costo global del cibercrimen en el mundo asciende a US$ 113 mil millones -lo suficiente para dar US$ 194.00 a cada ciudadano en América Latina-. De igual forma, se estima que existen 378 millones de víctimas anuales -casi el total de habitantes de América del Sur- y que hay 12 víctimas por cada segundo que pasa (p.7).

En tal sentido la mayor parte de todos los adultos conectados se considera que han sufrido ataques tales como malware, virus, piratería, estafas, fraudes y robo.

Esto implica que el cibercrimen es uno de los cinco delitos económicos más comunes y que preocupa a todas las empresas y organizaciones públicas a nivel mundial, dado que su incremento se ve potencializado con el desarrollo de la programación y de Internet, y donde los delitos informáticos se han vuelto más frecuentes y sofisticados.

Ver Figura Nº 1

Figura Nº 1

Fuente. Symantec (2013) Reporte Norton, 2013. USA.

b) En Latinoamérica

Según el Observatorio de la Ciberseguridad en América Latina y el Caribe (2016) se considera que es el resultado de una gestión de colaboración entre el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), la seguridad cibernética de los países de América Latina y el Caribe presentan amenazas que se ciernen sobre su operatividad y desarrollo.

> La conectividad a Internet acelera el crecimiento económico y crea oportunidades para los negocios y el comercio. La maximización del valor de la Internet y el ciberespacio debe ser una parte central de la planeación gubernamental. Sin embargo, estas oportunidades siempre traen sus riesgos. Las tecnologías de Internet aún no están maduras. Los delincuentes las pueden explotar fácilmente (p.4).

En América Latina se considera ha logrado un crecimiento económico importante, pero los gobiernos ignoran la seguridad cibernética, lo cual

es muy riesgoso. A medida que todas las sociedades se vuelvan más dependientes de las máquinas y las redes soportadas por computadores (y esto es inevitable ya que las computadoras están incrustadas en los objetos de uso cotidiano, tanto en los automóviles como en maquinaria industrial), la necesidad de adelantar acciones crecerá. En esto, el Hemisferio Occidental ha avanzado mucho, pero aún queda mucho trabajo por hacer

c) En el Perú

En nuestro país, se considera que el cibercrimen constituye una amenaza asimétrica, dado la dificultad de su rastrillaje y dar con el autor de delito.

> De acuerdo con cifras de la fiscalía, en nuestro país se han denunciado en el último año 243 casos. Los expertos en el tema calculan que la incidencia es mayor. El Reporte Norton considera que en el mundo existen 556 millones de víctimas al año y más de 2,5 millones de afectados por país, en promedio. El Perú, dada la cantidad de pobladores, se calcula que al menos se debe estar cerca del medio millón (Reporte Norton, 2013, p. 16).

En el ámbito de la seguridad nacional, el crimen cibernético es letal dado que en ciertos sectores por el nivel de confidencialidad de su información, es dable protegerla. Es el caso de la Seguridad informática en el sector público sobre todo en las instancia de seguridad y defensa, donde no se tiene una política standarizada en sus diversos sitios web, con la protección debida; la cual muchas veces viene siendo afectada por diversos ataques a sus sistema de información, esto constituye una situación crítica porque el sector público, tiene en sus redes, información delicada y secretos importantes dado su misión en el Desarrollo y la Defensa Nacional, ello implica tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información, todo lo

cual conlleva a ejecutar una política de seguridad informática estratégica, si los recursos y la información que el sector tiene en sus redes, merecen protegerse.

Se considera que al Implementar una política de seguridad de red efectiva ella significa plantear preguntas difíciles acerca de los tipos de servicios de inter redes y recursos cuyo acceso se permitirá a los usuarios, y cuales tendrán que restringirse debido a los riesgos de seguridad.

Una política de seguridad en redes es efectiva ya que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar, dado su relación con la ciberseguridad que es parte integrante de las políticas gubernamentales enfocadas a la disuasión de los ciberdelitos, por lo que el desarrollo de la tecnología de información, así como en el mejoramiento y la protección de las infraestructuras de la información críticas, es esencial para lograr la seguridad y el bienestar económico de cada país.

Por lo anterior, se debe obtener medidas de índole legal y técnico que respondan a la protección de las *tecnologías de la información y la comunicación* (TIC), como actividades destinadas a contrarrestar la integridad de las infraestructuras críticas del sector.

Los enfoques tradicionales de la seguridad deben ser sustituidos por soluciones innovadoras basadas en las nuevas tecnologías. Estas soluciones implican el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación y de control del acceso, y de filtros de software de todo tipo. Garantizar infraestructuras de información segura y fiable, no sólo exige la aplicación de diversas tecnologías, sino también su correcto despliegue y su uso efectivo. Algunas de estas tecnologías existen ya, pero a menudo los usuarios no son conscientes

de su existencia, de la manera de utilizarlas, o de las razones por las que pueden ser necesarias, esta última circunstancia está muy fuertemente arraigada en la cultura nacional, de no enfrentar esta situación con la debida anticipación, acentuando la problemática en este campo.

1.2. DELIMITACIÓN DE LA INVESTIGACIÓN

1.2.1. Delimitación espacial

La investigación se llevó a cabo desde una perspectiva amplia que incluye el ámbito del Cibercrimen en los ámbitos del ciberdelito y de los delitos informales en el país.

1.2.2. Delimitación temporal

El periodo de análisis corresponde a los años 2013 al 2015.

1.2.3. Temática y unidad de análisis

La temática de análisis corresponde al Cibercrimen en el pais en su relacion con la Seguridad Nacional.

La unidad de análisis, corresponde a la participación de los entes encargados del control del cibercrimen en nuestro país.

1.3. FORMULACIÓN DEL PROBLEMÁ

1.3.1. Problema principal

¿En qué medida el Cibercrimen en el Perú afecta a la Seguridad Nacional?

1.3.2. Problemas específicos

¿En qué medida las modalidades del Cibercrimen en el Perú afectan a la estructura informática de la Seguridad nacional?

¿En qué medida la estructura organizativa del Cibercrimen en el Perú afecta a la protección de la data de la Seguridad nacional?

¿En qué medida las técnicas del Cibercrimen en el Perú afectan a los fines de la Seguridad nacional?

1.4. JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

1.4.1. Justificación

a) Justificación Social.

- Esta investigación es necesaria para los responsables de la Seguridad informática en los sitios web de las instituciones del sector público, especialmente de la seguridad y defensa, porque la mejora de su gestión contribuye a optimizar el desarrollo nacional y de este modo lograr fortalecer el nivel del empleo de la Seguridad informática, para evitar el cibercrimen.

- Esta investigación contribuirá en lograr un iniciativa legal para mejorar la capacidad de la dirección y gestión dentro de la Seguridad informática en el país y por ende en los sitios web de las instituciones del sector público.

- Esta investigación también es necesaria para el sector público sobre todo en el sector defensa y seguridad, porque permite

el logro de los objetivos para el desarrollo de la Seguridad Informática.

b) Justificación Tecnológica – Sistémica

- Esta investigación también es consecuente para el sector público porque permitirá que cuente con un desarrollo tecnológico suficiente para permitir la Seguridad informática en los sitios web de las instituciones, asegurando entre otros la capacidad resolutiva del servicio, así mismo su proyección y prospectiva se mantendrá mediante estudios permanentes, acciones de investigación y planificación en la materia.

1.4.2. Importancia

La importancia del presente estudio, radica en la vital jerarquía del cumplimiento del principio de oportunidad y razonabilidad en el control del cibercrimen en el sector de investigación, cuestión de clara jerarquía dentro de un Estado previsor de delitos asimétricos como los delitos informáticos, por ello se este estudio se puede plasmar dentro de una iniciativa legal como elemento de relevancia para su combate.

Este control es indispensable dado que el cribercrimen es tan diverso como sus delitos; donde puede tratarse de personas naturales, terroristas o figuras del crimen organizado, estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en "paraísos informáticos" - o sea, en países que carecen de leyes o experiencia para seguirles la pista.

Otros delitos de la informática se caracterizan por sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados "gusanos" o "virus", que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro, algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes "infectados"; también es una modalidad frecuente por las redes, mayormente camuflados en mensajes electrónicos o en programas "descargados" de la red.

Además de las incursiones por las páginas particulares de la red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes o vender mercancías y servicios prohibidos, como armas, drogas, medicamentos sin receta ni regulación y pornografía.

Todo esto ha hecho que la proliferación del cibercrimen en nuestra sociedad la afecta y sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general, pero a la vez riesgosa, por lo que su control sea necesario e indispensable.

1.5. LIMITACIONES DE LA INVESTIGACION

La investigación tiene las siguientes limitaciones:

a) El estudio se llevo a cabo desde una perspectiva amplia que incluye el ámbito del cibercrimen solamente desde el ángulo del ciberdelito y de los delitos informales.

b) De orden bibliográfico, dado que existe poca bibliografía a nivel del cibercrimen en el marco de la seguridad y del sector defensa.

1.6. OBJETIVOS DE LA INVESTIGACIÓN

1.6.1. Objetivo general

Determinar en qué medida el cibercrimen en el Perú afecta la Seguridad Nacional.

1.6.2. Objetivos específicos

a) Establecer en qué medida las modalidades del Cibercrimen en el Perú afecta a la estructura informática de la Seguridad nacional.

b) Determinar en qué medida la estructura organizativa del Cibercrimen en el Perú afecta a la protección de la data de la Seguridad nacional.

c) Plantear en qué medida las técnicas del Cibercrimen en el Perú afectan a los fines de la Seguridad nacional.

CAPITULO II

MARCO TEORICO

2.1. ANTECEDENTES DE LA INVESTIGACION

2.1.1. Investigaciones internacionales

A continuación se presentan investigaciones que por su contenido y analogía sirvieron de base en nuestra investigación.

a) El estudio de Álvarez Basaldúa (2005) *Seguridad Informática.* Tesis para optar el Grado de Maestro en Ingeniería de Sistema empresariales. Universidad Iberoamericana, Méjico.

   Realizó un análisis del actual del sistema de auditoría del sistema informático en entidades gubernamentales, en la que el éxito de su gestión depende, como factor crítico de la eficiente administración de la información y la tecnología de información, en la que los sistemas de gestión han alcanzado un desarrollo notable.

   Tal concepción demanda, la participación inexcusable de la tecnología como herramienta, permitiéndole evolucionar al ritmo de las transformaciones incorporadas a la estructura del registro y del control interno y muy especialmente, para evaluar mediante auditorías a las tecnologías de información, los procedimientos de control específicos, dentro del ámbito de su soporte tecnológico, que a su vez, garantice una información objetiva sobre el grado de cumplimiento de las políticas y normativas establecidas por la organización para lograr sus objetivos.

La auditoría informática tiene como principal objetivo, evaluar el grado de efectividad de las tecnologías de información, dado que evalúa en toda su dimensión, en qué medida se garantiza la información a la organización, su grado de eficacia, eficiencia, confiabilidad e integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.

Su ámbito de acción se centra, en revisar y evaluar: los procesos de planificación; inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras.

b) Medina Iriarte, Johanna (2006) *Estándares para la seguridad de información con tecnologías de información.* Tesis para optar el título de Ingeniero en Información y Control de Gestión, Chile: Universidad de Chile

Considera que en toda organización actual, la seguridad de la información a comenzado a tomar un lugar muy importante, en cuanto a cómo se gestiona la Tecnología de Información, y se ha convertido en un elemento fundamentalmente considerado en toda estrategia de negocio con miras a lograr metas importantes, tanto como a corto, mediano y largo plazo.

En consecuencia, las organizaciones experimentan la necesidad de definir estrategias efectivas que garanticen una gestión segura de los procesos del negocio a fin de darle mayor resguardo a la información, y al mismo tiempo no obstáculos para adaptarse a los

continuos cambios de la organización como consecuencia de las exigencias del mercado.

Tal necesidad ha impulsado el énfasis en el planteamiento de nuevos paradigmas de la administración del entorno de TI basada en políticas y procedimientos. Esto ha llevado a la creación de estándares, códigos de buenas prácticas, desarrollos de políticas, etc., con motivo de resguardar uno de los activos más valiosos de las organizaciones como es la información.

Con la apertura de las empresas al mundo de Internet, se han abierto oportunidades de creación de nuevos negocios, tanto en chile como mundialmente. Por lo tanto actualmente es un tema prioritario para las empresas el resguardo de su información, ya que es un tema que abarca a las organizaciones desde las tareas más sencillas como a temas más complejos relacionados con el negocio y su supervivencia como organización.

Además, en una economía globalizada, como ocurre actualmente, donde los países y organizaciones están relacionados, también surge la necesidad de unificar criterios en cuanto a la seguridad, por lo que necesariamente surge la necesidad de certificar que las condiciones de seguridad son óptimas, tanto para las empresas como parar sus clientes.

El presente trabajo está orientado principalmente, a enumerar y desarrollar algunas políticas y estándares sobre seguridad de la información con tecnologías de información, que están presentes actualmente, sobre todo en el manejo adecuado de plataformas y de seguridad de la data recopilada.

2.1.2. Investigaciones nacionales

a) El estudio de Adrianzen Ojeda (2005) *Aspectos Penales y Tecnológicos en el Delito de Difamación cometido a través del Internet y su tratamiento en la Legislación Peruana*. Tesis para optar el Grado de Maestro en Derecho penal. Universidad Garcilaso de la Vega.

   El trabajo considera el desarrollo y masificación de las Tecnologías de la información y las Comunicaciones las cuales vienen transformando vertiginosamente a la humanidad. El derecho y sus diversas ramas no son en nada ajenas a esta *revolución digital.* La tesis se ubica en ese escenario de cambios, buscando establecer si existe o no una adecuada protección del bien jurídico honor en el Perú, tomando especialmente en cuenta la afectación del honor y la reputación de las personas en la comisión del delito de difamación mediante el uso del Internet. Las conclusiones del estudio consideran que por su novedosa temática, esta investigación puede aportar como elemento de juicio y valoración a quienes tienen bajo su responsabilidad hacer que el orden legalmente establecido mantenga permanente vigencia en el cumplimiento de su rol social, especialmente en cuanto a la cautela de los derechos fundamentales de la persona. El trabajo utilizo el método inductivo-deductivo confrontando las principales posiciones asumidas por la doctrina, la jurisprudencia y especialmente la legislación comparada

b) El estudio de Ore Céspedes (2011) *La delincuencia informática y la afectación al desarrollo económico y social.* Tesis para optar el Grado de Maestro en Administración. Universidad Nacional mayor de San Marcos.

El trabajo estudia el desarrollo de las tecnologías informáticas el cual ha abierto la puerta a conductas antisociales y delictivas, El espectacular desarrollo de la tecnología informática ha logrado nuevas posibilidades de delincuencia antes impensables. La conclusiones del estudio es que la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, y que son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

2.2. BASES TEORICAS

2.2.1. Cibercrimen

2.2.1.1. Concepto

Si se busca la definición de cibercrimen:

> Es ampliamente utilizado hoy en día para describir los delitos o daños que resultan de las oportunidades creadas por las tecnologías en red (Wall, 2008, p.16).

Por otra parte explícitamente, se considera según Kuehl (2009) es:

> El conjunto de un dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicación actuando de manera informal, no autorizada (p. 29).

En estos conceptos se incluye tanto los delitos nuevos surgidos a la luz de la creación del ciberespacio y de la aparición de diferentes intereses sociales que también pueden ser dañados o afectados por conductas realizadas en el seno de Internet, como aquellos otros delitos que tienen un referente tradicional y clásico en el espacio físico, pero que ahora también se cometen en este nuevo lugar o ámbito de intercomunicación personal configurado por el uso de las TIC, que es Internet.

Por todo ello es que el concepto de cibercrimen constituye toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, que se realiza en el entorno informático y está sancionado con una pena.

En este marco Tellez Valdez (2008) señala que los delitos informáticos son:

> Actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico) (p.187)

Esto implica que las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos, basados en internet.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de poder social, con las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configurando un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Por otra parte, el término cibercrimen permite recoger en su seno todos los delitos que hasta ahora se conocen realizados en el ciberespacio, así como los que surjan de las diferentes evoluciones de las TIC que aparezcan en el futuro. La cibercriminalidad ha ido mutando y evolucionando de manera paralela a los usuarios del ciberespacio y sus tecnologías asociadas, y lo seguirá haciendo en la medida que evolucione la tecnología y su uso

2.2.1.2. Marco legal

a) A nivel mundial

En el espectro mundial, la comunidad europea constituye uno de los principales ámbitos donde se ha puesto en la tarea y ha decidido combatir conjuntamente todas las formas de criminalidad, En tal sentido las naciones europeas se han destacado por su cohesión y su éxito en la lucha mancomunada contra toda forma de delincuencia.

El Consejo de Europa preocupado por el riesgo que implica la criminalidad cibernética, firma el Convenio suscrito el 23 de noviembre del 2.001 sobre la ciberdelincuencia también conocido como Convenio de Budapest; instrumento internacional que reconoce la necesidad de cooperación internacional en materia penal, garantizando la tipificación como delito de los actos que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de los mismos.

En éste se establecen tres aspectos fundamentales:

- Armonización de las normas penales sustantivas aplicables a las conductas delictivas que tienen como ámbito el entorno informático,
- Establecimiento de reglas procesales penales para facilitar la investigación de la criminalidad informática y
- La instrumentación de un sistema de cooperación internacional en el combate a estas conductas.

Dentro del panorama mundial existen países como China el cual tiene un sistema de regulación de niveles múltiples en malas acciones cibernéticos, con el de los instrumentos básicos y principales y sus dos enmiendas dentro de este siglo, las cuales son útiles ya que han ampliado el alcance de los delitos informáticos. La Enmienda (VII) se publicó en 2009 para cubrir la brecha que se levantó junto con la creciente popularidad de los ordenadores personales. Después de esta modificación, se estableció el enfoque de dos puntos y una dimensión. Este enfoque hace una clara distinción entre el delito informático genuina (es decir, los delitos que tienen como objetivo la seguridad del sistema de información de la computadora y los datos) y los delitos tradicionales facilitados por computadoras (es decir, delitos en virtud de las disposiciones penales tradicionales).

En EE.UU. pese a que logra penalizar las malas acciones cibernéticos no está exenta de problemas, una preocupación importante es su actitud hacia el equipo y los datos. En los delitos de piratería los legisladores eligieron una perspectiva estrecha y proteger la seguridad de la computadora; mientras que en otros delitos como el tráfico de dispositivos, las secciones relacionadas se basan en el concepto de datos e información. A partir del 2011 estos dos puntos de vista en consideración, la gente puede encontrar la legislación de los Estados Unidos sobre la ciberdelincuencia menos consistente, y esa incompatibilidad conduce a problemas en la práctica judicial.

En Inglaterra se opto por introducir nuevas disposiciones y actos que se actúe con los 'genuino ciberdelincuencia' y se basan en sus disposiciones penales existentes que se ocupan de los delitos tradicionales facilitados por computadoras. Este enfoque, como sugiere la Comisión de Derecho, se llama el enfoque 'a medio camino', lo que significa que 'rechazar la creación de completamente nuevos delitos, excepto cuando éstos son absolutamente necesarios, pero se debe estar preparado para contemplar la ampliación de los delitos generales existentes.

En el ámbito de Singapur ha sido activo en la promulgación y modificación de su Ley sobre Abusos Informáticos, el enfoque que se implementó es notable por los solapamientos y repeticiones dentro de disposiciones. En primer lugar, se aprendió de la Ley de Inglaterra sobre el mal uso de computadoras e introdujo los delitos de piratería que amenazan la seguridad de los datos, incluyendo mera piratería, la piratería de nuevos delitos, modificación de datos, y otros. Al mismo tiempo, se tomó las disposiciones equivalentes

En Canada se introdujo los delitos de piratería, el cual se centra en la capacidad de procesamiento y almacenamiento de la computadora,

como el uso de los servicios informáticos sin autorización, considera que el desarrollo de tecnología de la información y dispositivos digitales ofrece nuevas oportunidades para los delitos. El primero, facilita crímenes tradicionales como el fraude, y por el segundo, genera nuevos crímenes como la piratería. Los crímenes tradicionales facilitados por computadoras y los nuevos crímenes generados por computadoras son el llamado cibercrimen. Para combatir el cibercrimen, las jurisdicciones han desarrollado contramedidas en el campo del derecho penal tanto a nivel nacional como internacional.

b) A nivel regional

En América Latina se han implementado diversas legislaciones para combatir el cibercrimen.

Argentina

A partir de Junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos” ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia.

Brasil

La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298.

Chile

La Ley 19.223 (1993), es una ley “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. Dentro del código penal la Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos y regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.

Colombia

La Ley 1.273 (2009), de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos”. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cuál regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general “si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos”.

c) A nivel nacional

Los delitos informáticos han sido regulados en nuestra legislación peruana, mediante la Ley Nº 27309 publicada en el Diario Oficial "El Peruano" el lunes diecisiete de Julio del año dos mil, con la cual se incorpora al Título V del Libro Segundo del Código punitivo nacional,

un nuevo capítulo (Capítulo X) que comprenden las modalidades del cibercrimen en tres artículos 2O7°-A (Intrusismo informático), 207°-B (Sabotaje informático) y 207º-C (formas agravadas), lo que emerge palmariamente como un intento de actualizar nuestra legislación interna en relación a los nuevos avances de la tecnología, y sobre todo teniendo en cuenta que estamos dentro de una era informática, la cual no puede soslayarse, en sus efectos y consecuencias.

2.2.1.3. Dimensiones

Las dimensiones consideradas dentro del espectro teorico bajo el cibercrimen son las siguientes.

(a) Modalidades del cibercrimen

(1) Intrusismo informático. Esta modalidad de comisión del delito informático comprende aquellas conductas delictivas que atienden al modo operativo que se ejecuta y que pueden consistir en al apoderamiento indebido (apropiarse de la información), uso indebido (usar la información para cualquier fin) o conocimiento indebido de la información, cometidos interfiriendo, interceptando o meramente accediendo al sistema de tratamiento de datos.

> Es pues dicho comportamiento una introducción o penetración a sistemas de información o computadoras infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ella. Vemos que, aunque en ocasiones se afecten los datos computarizados o programas informáticos, ello no es determinante para la configuración del injusto, basta tan sólo el ingreso subrepticio a la información (con valor económico de empresa) para la concreción del comportamiento (Morales, 2010, p.21).

(2) Sabotaje informático. Doctrinariamente, es el acto de borrar, suprimir o modificar sin autorización, funciones o datos del sistema

informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema, considerándose que dichas conductas delictivas, están enfocadas al objeto que se afecta o atenta con la acción delictual, y que puede ser un sistema de tratamiento de la información o de sus partes componentes, el funcionamiento de un sistema de tratamiento de la información y/o de los datos contenidos en un sistema automatizado de tratamiento de información, siendo ostensible dicho atentado por medio de la destrucción, inutilización, obstaculización o modificación.

> Dentro de la doctrina penal, se nos da las pistas acerca de que se considera sabotaje informático, con el añadido que dentro de ésta modalidad delictiva también estarían englobados los llamados virus informáticos (programas secuenciales de efectos previsibles, con capacidad de reproducción en el ordenador ,y su expansión y contagio a otros sistemas informáticos, conllevando a la alteración o daño de archivos), las bombas lógicas (programa informático que tiene una fecha y hora de activaciones, luego de la cual empieza a dañar e inutilizar los componentes del ordenador), entre otras forma de sabotaje informático (Raguez, 2012, p.376).

De lo reseñado hasta aquí en este punto, es menester abordar lo que nuestra norma preconiza en su artículo, debiendo partir que en el sabotaje informático se busca el dañar el sistema informático o banco de datos, diferenciándose con ello del intrusismo, que es pues el simple acceso indebido a los sistemas de información, es decir mientras el sabotaje causa daños considerables, por así decirlo, el intrusismo o hacking es una mera intrusión o fisgoneo de los sistemas, que en algunas veces conlleva alteraciones menores, ello a la luz de los pensamientos doctrinarios dados en la materia.

En ese de orden de ideas, el sabotaje o daño informático para nuestra legislación, tiene el sujeto activo y pasivo, las mismas características mencionadas para la modalidad de intrusismo,

siendo la diferencia palmaria la referida a los actos materiales de ejecución, ello en razón a que como se ha expresado, en esta modalidad se busca el alterar, dañar o destruir el sistema informático o partes del mismo, obviamente mediante el acceso a éste. Con todo ello se puede observar, que un sabotaje informático conllevaría implícito un intrusismo informático, contrario sensu, un intrusismo informático no siempre tiene como correlato inicuo un sabotaje. Un punto saltante que se tiene de la norma sub examine, es lo correspondiente a la pena, dado a que se agrava la situación del sujeto activo al incrementarle las penas, que van desde los tres años hasta los cinco años, con el añadido de los días multa.

(3) Modalidad agravada. En cuanto a la modalidad agravada, el artículo 207-C del Código Penal, es muy diáfano en prescribir, que la pena se agrava cuando el sujeto agente quien desarrolla el tipo penal,

> Es quien tiene una vinculación o cercanía al sistema informático por razones de la función que desempeña, es decir por la facilidad que tiene el sujeto en el uso de sus funciones, de acceder a los bancos de datos o sistemas de información, lo cual lo coloca en una posición privilegiada –y manejo de información de la misma cualidad- frente a otros sujetos, siendo ésta una de las razones de la norma para sancionar con penas mucho mayores a las previstas para los delitos de intrusismo y sabotaje informático simplemente. (Raguez, 2012, p.378).

Un punto importante en este respecto, es el relativo al inciso 02 del artículo bajo análisis, en el cual el sujeto agente, puede ser cualquier persona natural, ello considerando que lo que se pone en peligro es la seguridad nacional.

(b) Estructura del cibercrimen

Para Majid Yar (2006), la ausencia de una definición específica sobre el fenómeno del cibercrimen se debe fundamentalmente a que:

> La delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tienen lugar. (p.5)

En la actualidad, las relaciones del cibercrimen más utilizada es aquella que posee el Convenio sobre Ciberdelincuencia del Consejo de Europa, firmado en Budapest, Hungría en 2001. Este define estas conductas estableciendo una clasificación de cuatro tipos de delito, a saber: 1) delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos; 2) delitos informáticos propiamente dichos; 3) delitos relacionados con contenidos ilícitos, y 4) infracciones al derecho de autor.

En relación con el primer grupo de conductas, estas incluyen el acceso, la interceptación ilícita y ataques contra la integridad de datos y sistemas y abuso de dispositivos informáticos. En cuanto a los delitos informáticos propiamente dichos, esta categoría incluye los actos ilícitos como falsificación y fraude informático; mientras que los delitos de contenido aluden básicamente a aquellos relacionados con pornografía infantil. Por último, los delitos relacionados con la propiedad intelectual refieren al mantenimiento de la validación de los derechos de autor en los medios y soportes digitales.

En cuanto a la estructura que actual contra el cibercrimen, esta se circrunscriben dentro de la norma peruana el cual condiciona y controla el cibercrimen, donde esta última serían las conductas ilícitas sancionadas por el Derecho Penal por haberse vulnerado el bien

jurídico protegido denominado Intimidad de las personas o instituciones, puesto que se utilizan elementos informáticos para vulnerar y acceder a la información contenida en los sistemas informáticos de la víctima, violando de esta forma la intimidad de la misma, de tal modo que no se sustrae la información para que forme parte del patrimonio del delincuente ya que la información se mantiene pudiendo éste hacer sólo copias.

Es necesario considerar a los sujetos que intervienen, los cuales son el delincuente informático y la víctima, así como algunos coautores que ayudan al primer sujeto a cometer el delito, siendo necesario que estos sean trabajadores de la empresa o centro de trabajo de la víctima.
Es necesario señalar que la comisión de estos delitos informáticos acarrean la criminalidad informática, debiéndose entender a ésta como los actos que vulneran la ley vigente, es decir que se tipifique el delito en el Código Penal Peruano, señalándose las sanciones imponibles de acuerdo a la gravedad de la comisión, pero en el Perú esta criminalidad no podría darse por no estar tipificado el delito y no estar regulado por ley alguna.

La última disposición en materia de delito informático es la ley Nº 30096 del 2014, con el consiguiente tenor:

CAPÍTULO I FINALIDAD Y OBJETO DE LA LEY
Artículo 1. Objeto de la Ley 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.

CAPÍTULO II DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito 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.

Artículo 3. Atentado contra la integridad de datos informáticos El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 4. Atentado contra la integridad de sistemas informáticos El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

CAPÍTULO III DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1,

2 y 4 del artículo 36 del Código Penal.

CAPÍTULO IV DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6. Tráfico ilegal de datos El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. Artículo 7. Interceptación de datos informáticos El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

CAPÍTULO V DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de

libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

CAPÍTULO VI DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

CAPÍTULO VII DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Artículo 11. Agravantes El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando: 1. El agente comete el delito en calidad de integrante de una organización criminal. 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia. 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Codificación de la pornografía infantil La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y

supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada. La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA. Agente encubierto en delitos informáticos El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público La Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.

CUARTA. Cooperación operativa Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de

cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley.

QUINTA. Capacitación Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA. Buenas prácticas El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, de Budapest (2001): a. Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. b. Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que

un sistema informático ejecute una función.

DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957. El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957. El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

c) Técnicas avanzadas de cibercrimen

Hoy en día todos dependemos de la información que radica y generamos en nuestras computadoras; estos objetos ya no se encuentran aislados como en los 90´s y principios de los 2000´s; si no por el contrario, hoy dependemos de una conexión física para podernos comunicar, el avance que se ha tenido con las redes nos ha

permitido solucionar problemas y hacer provecho de sistemas que nos ayudan a manipular la información.

Empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los Hackers, los cuales se vuelven ataques a un sistema operativo, cuestión donde se debe tomar una serie de precauciones para evitar que alguien no deseado busque en la información y no ser presa fácil de extorsiones, fraudes y pérdidas irreparables.

- **Tipos de ataques** (Maitwald, 2009)

Ataques de intromisión: Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en una computadora hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa (p.74).

Ataque de espionaje en líneas: Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información. (p.74).

Ataque de intercepción: Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder

revisar archivos, información y contenidos de cualquier flujo en una red. (p.75).

Ataque de modificación: Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad de los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.). (p.75).

Ataque de denegación de servicio: Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. (p.75).

Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

Ataque de suplantación: Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los “nuevos ladrones” ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son

vaciadas. (p.76).

Es importante mencionar, que así como se llevan estos tipos de ataques en medios electrónicos, muchas veces se llevan a cabo en archivos físicos (expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días (como teléfonos convencionales, celulares, cajeros automáticos, etc.); inclusive los ataques a computadoras, muchas veces, comienzan precisamente con información obtenida de una fuente física (papeles, basura, intervención de correo, cartas, estados de cuenta que llegan a los domicilios; o simplemente de alguien que vigila lo que hacemos).

- **Los hackers** (Tanembaum, 2010)

> Constituye un pirata informático y/o Hacker, que realiza ataques a la seguridad de la información, con la intrusión, pérdida, alteración, inserción, bloqueo de información en sistemas, bloqueo de sistemas operativos y de dispositivos.(p.68)

Lo que motiva a un pirata informático y/o Hacker a realizar los ataques son: los retos, ya que ellos trabajan en generar códigos que pueden burlar la seguridad, infiltrarse en redes y sistemas para extraer o alterar la información sintiéndose así superiores; codicia, unos de los motivos más antiguos por lo que las personas delinquen, tratado de hacer “dinero fácil” y un propósito mal intencionado o también definido como vandalismo o terrorismo.

Los métodos tradicionales de los Hackers son: buscar comparticiones abiertas, contraseñas deficientes, fallas y vulnerabilidades en programación, desbordamiento de buffer y denegaciones de servicios. Los Métodos más avanzados son: Rastreo de redes conmutadas (transmisión de paquetes entre nodos o redes); métodos de

falseamiento y enmascaramientos de IP; códigos malintencionados y virus.

En el ámbito de Ingeniería social, con este tipo de práctica, el intruso puede obtener horarios de trabajo, claves de acceso, nombres de empleados e infiltrarse indirectamente en la organización, empresa y/o inclusive en nuestras casas. Puede obtener información con una simple plática, siendo amigables y mintiendo con alguien que trabaja en la empresa y/o organización. También a través de una llama telefónica haciéndose pasar por un empleado que pide soporte técnico a la empresa que le proporciona dicho servicio, o también haciéndose pasar por algún agente bancario y/o de seguros que trata de vender o prestar su servicio y todo esto hecho vía telefónica. Es también común recibir un correo electrónico informado que se ha ganado un premio y se requieren algunos datos para enviar el supuesto premio a al domicilio.

2.2.2. Seguridad Nacional

2.2.2.1. Concepto

Podemos indicar que la Seguridad Nacional puede entenderse en un sentido objetivo como:

> La ausencia de amenazas o terror, la capacidad del Estado para garantizar su supervivencia, manteniendo su soberanía e independencia material y espiritual, preservando su forma de vida y posibilitando el logro de sus objetivos fundamentales, adquiriendo el carácter de disciplina del orden social, de la paz de la guerra o sea del derecho, de la política interna, de la política externa y de la estrategia militar (Sánchez Palomares, 2005, p.11)

Por otra parte según Osorio (2003) dice del concepto de seguridad:

> Como una exención de peligro o daño, este concepto demasiado restrictivo y limitado, no da mayor amplitud del término, otros doctrinarios dicen de la seguridad, que consiste en contrarrestar el peligro mediante un equilibrio entre fiabilidad y riesgo aceptable (p.77).

La seguridad en tal sentido es la base principal para el desarrollo de los pueblos, sociedades y naciones, la nueva concepción del neoliberalismo con su teoría estrella, la globalización, ha sido acompañado con un crecimiento de una cultura del delito, siendo uno de ellos el informático.

2.2.2.2. Fines de la Seguridad Nacional

Podemos considerar que la seguridad nacional implica las nociones de garantía, protección y tranquilidad, de las personas, frente a amenazas o presiones que atenten contra su existencia, sus bienes, al ejercicio de sus derechos, etc.

En tal sentido los fines de la seguridad de acuerdo al Caen (2013)

> La seguridad es un fin, pero además es un medio que permite, propicia y garantiza alcanza el bienestar de la población, por tanto en este segundo caso tiene por finalidad garantizar el logro del bienestar general, en un ambiente de paz interna y externa (p. 45)

Esto se correlaciona con la defensa el cual según el Caen (2013)

> Es el conjunto de previsiones, decisiones y acciones que el gobierno genera y ejecuta permanentemente para lograr la Seguridad Nacional y alcanzar sus objetivos, incluyendo su integridad, unidad, bienestar y la facultad de actuar con autonomía en el ámbito interno, y libre de toda subordinación en el ámbito externo (p. 49)

Si se tiene en cuenta que los fines esenciales del Estado son el bienestar general, y la seguridad integral, lo deseable es que éste bienestar se logre fundamentalmente en un ambiente de paz; por consiguiente, la Defensa Nacional adopta medidas para alcanzar y preservar ese ambiente de paz necesario para que el país desarrolle sus actividades sin temor, con progreso y sin interferencias extrañas.

En cuanto a la seguridad informática su concepto es la siguiente:

> Son las medidas que permiten evitar la realización de acciones no autorizadas que afecten de alguna manera la confidencialidad, autenticidad o integridad de la información y que de la misma forma garanticen el funcionamiento correcto del equipo y la disponibilidad de éste para los usuarios legítimos (Gomez Vieitiez, 2006, p. 4)

Es lamentable decir que la información nunca va a estar libre de riesgo, así la seguridad no trata sobre cómo estar libre de peligro, más bien se refiere a una buena administración del riesgo. Así fundamentalmente la seguridad es la mejor manera para llevar a cabo la administración de la pérdida o riesgo.

Por lo tanto, la definición de seguridad informática puede ser la administración de la pérdida o riesgo en la información y del costo que resulte de esa pérdida.

En cuanto los objetivos primordiales de la seguridad informática son:

> Mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información, para poner en funcionamiento distintas medidas de seguridad, mundialmente reconocido como la tríada de la seguridad: confidencialidad, integridad y disponibilidad (Aldegani, 2005, p. 25)

La influencia de las Tecnologías de la seguridad informática en el entorno que rodea a las Organizaciones tiene implicancias significativas en el ejercicio de la gestión. De hecho los usos que se le daban a esta tecnología no tienen cabida actualmente y difícilmente serán apropiadas en el futuro, lo que implica la necesidad de contar con la capacidad de adaptación a los avances.

Al hablar de gestión:

> Estamos refiriéndonos a la acción y efecto de administrar, es decir emplear recursos escasos y asignarlos de la mejor manera posible para conseguir los fines organizaciones planteados (Mitzberg, 2003, p.19)

Lo que implica que al asignarlos de alguna manera afectamos a varias áreas y/o personas que de alguna manera interactúan ente ellas, por lo que debemos entonces también considerar la coordinación de esas actividades para que las acciones derivadas de la asignación sean coherentes y contribuyan con un objetivo común. Por lo que podemos afirmar que la gestión implica asignar y coordinar tal asignación.

Pero ¿ Cómo podemos asignar tales recursos de la seguridad informática si no sabemos el estado de estos y quizás tampoco la manera cómo afecta a cada agente involucrado en su asignación?. De aquí se genera el importante rol que cumple la seguridad informática dentro de la gestión.

Mediante un adecuado control del Sistema de Información, diferentes entes pueden compartir información referente al estado actual y posibles proyecciones útiles para un tomador de decisiones, es decir se genera transparencia entre el estado y las acciones de los afectaran.

2.2.2.2. Dimensiones

a) Estructura informática

Las políticas de uso de Internet y correo electrónico se incluyen con frecuencia en la política más general del uso de las computadoras. Sin embargo, en ocasiones se plantea en una política aparte, debido a la naturaleza específica del uso de Internet. Las organizaciones conceden conectividad a Internet a sus empleados para que éstos puedan realizar sus labores con mayor eficacia y de este modo beneficia a las organizaciones. Desgraciadamente, Internet proporciona un mecanismo para que los empleados hagan uso de los recursos de cómputo.

Las políticas de respaldo y normalización de actividades después de un desastre tienen que ser muy bien especificadas para que en un lapso muy corto de tiempo, la empresa u organización regrese a sus actividades y las pérdidas económicas sean mínimas o nulas.

La seguridad lógica: Cada organización debe de desarrollar un procedimiento para identificar la vulnerabilidad en sus sistemas de cómputo; normalmente las exploraciones son realizadas por el departamento de seguridad y los ajustes son realizados por los administradores del sistema canalizándolos a los programadores y/o proveedores del sistema. Existen algunas herramientas para realizar estas pruebas, también se puede recurrir a pruebas de desempeño y análisis de código, pero también se puede recurrir a la experiencia de uso de los usuarios.

Seguridad técnica: Las medidas técnicas de seguridad se ocupan de la implementación de los controles de seguridad sobre los sistemas de cómputo y de red. Estos controles son manifestaciones de las políticas

y los procedimientos de la organización.

En las entidades, empresas, como en los domicilios personales ya se cuenta con conexiones permanentes a las redes o a Internet y estas deben de estar protegidas mediante muros de fuego que actúan de manera que su homónimo arquitectónico entre dos habitaciones de un edificio. Puede ser físico (equipo) ó lógico (software).

Las conexiones de acceso remoto pueden ser intervenidas para obtener acceso no autorizado hacia las organizaciones y, por consiguiente, deben de estar protegidas. Este tipo de conexiones pueden ser por marcación telefónica o atreves de Internet.

Puesto que estas conexiones entran a la red de la organización o a la computadora tiene que tener un sistema de autentificación como los módems de retroalimentación (que contienen en si mecanismos de autentificación); las contraseñas dinámicas son apropiadas para utilizarse como un mecanismo de autentificación mientras las contraseña dinámica sea combinada con algo conocido por el usuario; también existen programas y dispositivos de encriptación para asegurar que la información no es altera desde su creación hasta su lectura por el receptor.

El monitoreo en redes debe de llevarse a cabo para detectar diversos tipos de actividades inesperadas de virus, códigos maliciosos o uso inapropiado de esta, existen programas como los sniffers para ver el tráfico o todo aquello que pasa por la red, también existen equipos como los IDS´s (Intrusión Detection System) que cuentan con mecanismos para hacer análisis de paquetes y errores en las redes.

La seguridad física: La seguridad física debe ser empleada junto con la seguridad administrativa y técnica para brindar una protección

completa. Ninguna cantidad de seguridad técnica puede proteger la información confidencial si no se controla el acceso físico a los servidores, equipos y computadoras. Igualmente, las condiciones climáticas y de suministro de energía pueden afectar la disponibilidad de los sistemas de información.

El acceso físico es importante, todos los equipos delicados deben de estar protegidos del acceso no autorizado; normalmente esto se consigue concentrando los sistemas en un centro de datos. Este centro está controlado de diferentes maneras, se puede limitar el acceso con dispositivos, o instalar cerraduras de combinación para restringir los accesos a empleados y personas ajenas a las instalaciones.

Los sistemas de cómputo son sensibles a las altas temperaturas. Los equipos de cómputo también generan cantidades significativas de calor.

Las unidades de control de clima para los centros de cómputo o de datos deben de ser capaces de mantener una temperatura y humedad constante.

Los sistemas de extinción de incendios para los equipos deben ser los apropiados, estos no tienen que tener base de agua para que no dañen los equipos.

Para evitar pérdidas y daños físicos a equipos y computadoras hay que contar con una instalación eléctrica adecuada, no hay que saturar las tomas de corriente (que es muy común), se recomienda utilizar fuentes reguladas como no-breaks y reguladores para la protección de equipos. Si existen instalaciones específicas para los equipos y computadoras se recomienda utilizar fuentes redundantes y una planta de energía auxiliar.

b) Protección de la data

La protección de la data son prácticas y que no son otra cosa que una cultura y educación que debemos adquirir para evitar problemas futuros en usos de equipos y sistemas. Hoy en día es tan común que usemos computadoras, cajeros automáticos, tecnologías de comunicaciones, redes e Internet, que no caemos en la cuenta de toda la que la información que manejamos, nuestra propia información, correos electrónicos, información a través de chat, datos bancarios, archivos de interés y todo nuestro trabajo cotidiano se encuentra precisamente manejado por computadoras y equipo que son vulnerables y que en un abrir y cerrar de ojos pueden sufrir de una ataque, alteraciones o descomposturas.

La seguridad en un equipo, nodo o computadora: Uno de los primero puntos a cubrir son las claves de acceso, no se deben usar claves que en su constitución son muy comunes, como es el caso de las iniciales del nombre propio y la fecha de nacimiento, apodos o sobrenombres que todo mundo conoce, o constituirlas de solo letras o solo números; estos tipos de claves son en las que los intrusos, Hackers y ladrones buscan de primera mano; hay que hacer combinaciones de letras mayúsculas, minúsculas y números alternadamente.

No hay que compartir las claves, es común que cuando alguien más necesita usar nuestros equipos, computadoras y sistemas les damos las claves de uso y muchas veces hasta en voz alta, enfrente de muchas personas que no son parte de la empresa las damos a conocer. Hay que cambiar periódicamente las claves de acceso, los equipos o computadoras que se encuentran más expuestos, tienen que tener un cambio más recurrente.

En cada nodo y servidor hay que usar antivirus, actualizarlo o configurarlo para que automáticamente integre las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados.

Si los equipos, computadoras o servidores tienen niveles de permisos de uso de archivos y de recursos, hay que configurarlos de acuerdo a los requerimientos de la empresa o usuario, y no usar la configuración predeterminada que viene de fábrica, así como nombres y usuarios. Los intrusos, ladrones y Hackers conocen muy bien las configuraciones predeterminadas y son las que usan al momento de realizar un ataque.

En computadoras que utilicen sistemas operativos de Microsoft, hay que realizar actualizaciones periódicamente, ya que constantemente los Hacker y creadores de virus encuentran vulnerabilidades en dichos sistemas operativos. También, hay que utilizar programas que detecten y remuevan “spywares” (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento), existen diferente softwares que realizan esta tarea, algunos son gratuitos y trabajan muy bien; así la recomendación es contar con uno de ellos y realizar un escaneo periódico del equipo o computadora.

La seguridad administrativa: Esta se basa en políticas y normas que se deben de implantar y seguir. Las políticas proporcionan las reglas que gobiernan el cómo deberían ser configurados los sistemas y cómo deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Define lo que debería de ser la seguridad dentro de la organización y pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos.

Toda política debe de tener un propósito y procedimiento bien específico que articule claramente por qué fueron creados tales políticas o procedimientos y qué beneficios se espera la organización derivada de las mismas.

Cada política y procedimiento debe tener una sección que defina su aplicabilidad. Por ejemplo: una política de seguridad debe aplicarse a todos los sistemas de cómputo y redes. Una política de información, puede aplicarse a todos los empleados.

La sección de responsabilidad de una política o procedimiento, define quién se hará responsable por la implementación apropiada del documento. Quienquiera que sea designado como el responsable de aplicar una política o procedimiento de ser capacitado de manera adecuada y estar consciente de los requerimientos del documento.

Las políticas de información definen qué información es confidencial y cual es de dominio público dentro de la organización, y cómo debe estar protegida esta misma. Esta política está construida para cubrir toda la información de la organización.

Las políticas de seguridad definen los requerimientos técnicos para la seguridad en un sistema de cómputo y de redes. Define la manera en que un administrador de redes o sistema debe de configurar un sistema respecto a la seguridad que requiere la empresa o el momento. Esta configuración también afecta a los usuarios y alguno de los requerimiento establecidos en la política y debe de comunicarse a la comunidad de usuarios en general de una forma pronta, oportuna y explícita.

Las políticas de uso de las computadoras extienden la ley en lo que respecta a quién puede utilizar los sistemas de cómputo y cómo

pueden ser utilizados. Gran parte de la información en esta política parece de simple sentido común, pero si las organizaciones no las establecen específicamente, toda la organización queda expuesta a demandas legales por parte de los empleados.

2.2.4. La seguridad informática a nivel comparativo

Argentina: (http://www.arcert.gov.ar/)

Con la irrupción de las TICs en las últimas décadas, el gobierno de Argentina, mediante Decreto 378/2005 del 27 de abril de 2005 y con el objetivo de optimizar la gestión pública y los servicios, garantizar la transparencia de los actos de gobierno, facilitar trámites y reducir sus costos, apoyando la integración y el desarrollo de los distintos sectores, puso en marcha el Plan Nacional de Gobierno Electrónico y los Planes Sectoriales para el uso intensivo de las TICs en los organismos de la Administración Pública Nacional.

Posteriormente y para la implementación de dicho Plan, en el seno de la Oficina Nacional de Tecnologías de Información (ONTI), adscrita a la Subsecretaría de Tecnologías de Gestión Pública de la Secretaría de Gabinete y Gestión Pública de la Jefatura de Gabinete de Ministros, se conformó un grupo de trabajo por especialistas en seguridad de la información del sector público, quienes intercambiaron opiniones con respecto a las estrategias de seguridad informática en la APN. Como resultado, y conforme a las facultades conferidas a la Oficina Nacional de Tecnologías de Información (ONTI) por la Decisión Administrativa 669/200410 y por la Resolución SGP 45/200511, el 3 de agosto de ese mismo año mediante la Disposición 6/2005 se aprobó el Modelo de Política de Seguridad de la Información para Organismos de la APN (Modelo de Política).

Las características generales de la Política de Seguridad de la Información para organismos del sector público, son las siguientes:

- Instrumento gubernamental de vigencia permanente y con carácter obligatorio para todo organismo del sector público, que tiene por objeto proteger los recursos de información del organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

- Establece el deber para el titular de cada organismo público de dictar o adecuar su Política de Seguridad de la Información al *Modelo de Política*, además de integrar un *Comité de Seguridad de la Información* (integrado por los Directores Nacionales o Generales de las áreas sustantivas del organismo de que se trate, destinado a garantizar el apoyo a las iniciativas de seguridad) y designar un *Responsable de Seguridad Informática* (supervisor del cumplimiento de la política y asesor en la materia a los integrantes del organismo que así lo requieran), así como establecer las responsabilidades en la materia de los funcionarios públicos.

Canadá: (http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp)

Si bien el ciberespacio ofrece múltiples beneficios en el desarrollo de un país, también la creciente dependencia de las tecnologías vulneran las infraestructuras críticas, debilitando a la seguridad nacional y a la propia prosperidad económica y calidad de vida. Frente a ello, el gobierno canadiense ha adoptado una política de seguridad cibernética, conformada por diversas medidas de protección, entre las que se incluyen:

- El lanzamiento de la Estrategia de Ciberseguridad de Canadá, cuya objetivo primordial es prevenir, reducir y tratar los impactos de las amenazas informáticas y los incidentes.
- La creación del Centro Canadiense de Respuesta a Incidentes Informáticos (CCIRC), encargado de controlar las amenazas cibernéticas y la coordinación de la respuesta federal a incidentes cibernéticos.
- Las reformas al Código Penal, consistentes en perfeccionar la tipificación de los delitos cibernéticos, a fin de aumentar la capacidad de las autoridades responsables para su investigación y persecución.
- La colaboración con la industria y otros gobiernos, resguardando las infraestructuras críticas para la salud, la seguridad y el bienestar económico de los canadienses, a fin de combatir los incidentes cibernéticos y proteger los activos críticos y la información.

Con respecto a la Estrategia de Ciberseguridad de Canadá, fue emitida el 3 de octubre de 2010 por las provincias de ese país, bajo el mandato de su Majestad La Reina, producto de la contribución de dependencias y entidades gubernamentales, así como del apoyo de socios provinciales y territoriales, que conjuntamente son responsables de la protección de gran parte de la infraestructura crítica en Canadá. En ella se encomienda al gobierno el compromiso de fortalecer los sistemas informáticos y los sectores de las infraestructuras críticas, a través de la colaboración con las provincias, territorios y el sector privado.

Esta Estrategia de Ciberseguridad se basa en tres pilares:

a. La protección de los sistemas de Gobierno: El gobierno es responsable de establecer las estructuras necesarias, las herramientas y el personal para cumplir con sus obligaciones en seguridad cibernética. Con ello, actuará para defender la ciber-soberanía, además de proteger la seguridad nacional y los intereses económicos.

b. La asociación para asegurar los sistemas cibernéticos vitales fuera del gobierno federal: La prosperidad económica y la seguridad de los canadienses dependen del buen funcionamiento de los sistemas fuera del Gobierno. En cooperación con los gobiernos provinciales, territoriales y el sector privado, el gobierno debe apoyar las iniciativas encaminadas al fortalecimiento de las medidas de ciberresistencia y a la protección de las infraestructuras críticas.

c. La ayuda a los canadienses para estar seguros en línea: El gobierno debe ayudar a la ciudadanía a obtener la información necesaria para protegerse a sí mismos y a sus familias en línea, además de fortalecer la capacidad de las fuerzas del orden para combatir el cibercrimen.

2.3. MARCO CONCEPTUAL

Amenaza

Se conoce como amenaza al peligro inminente, que surge, de un hecho o acontecimiento que aún no ha sucedido, pero que de concretarse aquello que se dijo que iba a ocurrir, dicha circunstancia o hecho perjudicará a una o varias personas en particular.(www.significados.com/amenaza)

Cibercrimen

Es el conjunto de un dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicación actuando de manera informal, no autorizada (Kuehl, 2009, p. 29).

Control

El control es una función de gestión: es la fase del proceso administrativo que mide y evalúa el desempeño y toma la acción correctiva cuando se necesita. De este modo, el control es un proceso esencialmente regulador (Chiavennato, 2014, p.156).

Defensa nacional

Es el conjunto de previsiones, decisiones y acciones que el gobierno genera y ejecuta permanentemente para lograr la Seguridad Nacional y alcanzar sus objetivos, incluyendo su integridad, unidad, bienestar y la facultad de actuar con autonomía en el ámbito interno, y libre de toda subordinación en el ámbito externo (Caen, 2013, p. 49)

Intereses nacionales.

Son aquellos aspectos que están constituidos por las necesidades y aspiraciones, amplias y duraderas que posee la Nación y se traducen en Objetivos Nacionales, que vienen a ser la expresión formal de los intereses y aspiraciones nacionales (Libro Blanco 2006, p.62)

Gestión

Es el proceso a través del cual una organización formula objetivos, está dirigida a la obtención de los mismos. Gestión es el medio, la vía para la obtención de los objetivos de una organización. Es el arte (maña) de entremezclar el análisis interno y la sabiduría utilizada por los dirigentes para crear valores de los recursos y habilidades que ellos controlan. Para diseñar una Gestión exitosa hay dos reglas claves: Hacer que lo que haga bien, y escoger a los competidores que pueden derrotar. Análisis y acción están integrados en la Gestión (Mitzberg, 2003, p.11).

Meta

La meta es el desempeño esperado por el indicador asociado al producto y/o al objetivo estratégico relacionado con el producto. Desde

esta perspectiva, permite medir el avance de los logros de sus productos y el desempeño de estos establecidos en los objetivos estratégicos (Mitzberg, 2003, p.35).

Políticas públicas

Es un proceso cíclico: definición del problema, escogencia de políticas, monitoreo o evaluación de los resultados de esas políticas y redefinición del problema. La evaluación es usualmente considerada como la etapa de post implementación, diseñada para determinar la efectividad del programa y facilitar la reorientación o terminación del mismo (Dye,1984, p.104).

Seguridad nacional

La seguridad es un medio que permite, propicia y garantiza el bienestar de la población; por tanto, en este caso tiene por finalidad garantizar el logro del bienestar general, en un ambiente de paz interna y externa (Caen, 2013, p. 45)

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ENFOQUE

El enfoque es cuantitativo ya que utiliza la recolección de datos, para probar las hipótesis, como base en la medición numérica y el análisis estadístico con el fin de establecer pautas de comportamiento y probar teorías (Hernández, 2014, p.4).

3.2. ALCANCE

El alcance de la investigación es descriptivo explicativo (Hernández, 2014, p. 92), es descriptivo debido a que busca especificar propiedades y características importantes de cualquier fenómeno que se analice y es explicativo porque pretenden establecer las causas de los sucesos o fenómenos que se estudian.

3.3. DISEÑO DE INVESTIGACIÓN

La investigación es no experimental, el cual es aquella que se realiza sin la manipulación deliberada de variables, y en los que solo se observa los fenómenos en su ambiente natural, para analizarlos (Hernández, 2014, p. 152).

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

La población del estudio lo constituyen los directores y personal con capacidad de control del cibercrimen como las instituciones de la Policía

Nacional del Perú, Ministerio Publico, y del Poder Judicial, que suman un total de 495 funcionarios.

3.4.2. Muestra

Para determinar el tamaño óptimo de la Muestra se eligió la fórmula del cálculo de una muestra simple al azar, la que se detalla a continuación: (Ayres, 2002, p.65):

$$n = \frac{(Z)^2 \ (PQN)}{(e)^2 \ (N-1) + (Z)^2 \ (PQ)}$$

Donde:

z = Desviación estándar
E = Error de muestreo 0.05 (5%)
p = Probabilidad de ocurrencia de casos 0.5 (50%)
q = 1-p (0.50) 50%
N = Tamaño del universo de la población
n = Muestra

PRINCIPALES NIVELES DE CONFIANZA Z

$1 - \alpha$	$z_{al\ 2}$
80.00%	1.2800
90.00%	1.6450
95.00%	1.9600
96.00%	2.0500
98.00%	2.3300
99.00%	2.5800

Aplicando la formula tenemos:

$$n = \frac{(Z)^2 \ (PQN)}{(e)^2 \ (N-1) + (Z)^2 \ (PQ)}$$

$$n = \frac{(1.96)^2 \ (0.5 \times 0.5) \ 580}{(0.05)^2 \ (N-1) + (1.96)^2 \ (0.5 \times 0.5)} =$$

$$n = \frac{(3.8416) \ (0.25)(580)}{(0.0025)(579) + 0.9604}$$

$$n = 231$$

3.5. HIPÓTESIS

3.5.1. Hipótesis general

El nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional.

3.5.2. Hipótesis específicas

a) El nivel alcanzado por las modalidades del Cibercrimen en el Perú afecta significativamente a la estructura informática de la Seguridad nacional

b) El nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú afecta significativamente a la protección de la data de la Seguridad nacional.

c) El nivel alcanzado por las técnicas del Cibercrimen en el Perú afecta significativamente a los fines de la Seguridad nacional.

3.6. OPERACIONALIZACIÓN DE LAS VARIABLES

3.6.1. Definición conceptual

Cibercrimen. Constituye aquella acción por los cuales se vulnera la información en si, como es la piratería, la obtención ilegal de información, accediendo sin autorización a una PC, el Cracking y Hacking de software protegido con licencias.

Seguridad Nacional. Se refiere a la noción de relativa estabilidad, calma o predictibilidad que se supone beneficiosa para el desarrollo de un país; así como a los recursos y estrategias para conseguirla, principalmente a través de la defensa nacional.

3.6.2. Definición operacional

VARIABLES	DIMENSIONES	INDICADORES
1. Variable Independiente Cibercrimen	x1: Modalidades	- % del intrusismo informático - % del sabotaje informático
	x2:Estructura organizativa	- Nº de delitos - % de responsabilidad
	x3: Técnicas	- Nº de tipos de ataques - % de Hackers

2. Variable Dependiente Seguridad Nacional	y1:Estructura informática y2: Protección de la data y3: Fines	- % de control efectivo - % de cumplimiento de los reglamentos - Nº de programas - Nº de normas legales - % de eficacia de las políticas - % cumplimiento de objetivos

3.7. TÉCNICAS E INSTRUMENTOS

3.7.1. Técnicas

La técnica utilizada en la investigación es el de Observación, el cual según Sampieri (2014):

> Es el registro sistemático, valido y confiable de comportamiento o conducta (p.309).

La técnica es directa e indirecta. A nivel de observación directa se aplicó una encuesta al personal de las instituciones del control del cibercrimen, mientras que a nivel indirecta se utilizó la revisión documentaria relativa al tema estudiado.

3.7.2. Instrumentos de recolección de datos

1. Revisión documentaria. Se utilizó como instrumento las fichas, citas y subrayados bibliográficas seleccionados provenientes de libros del Centro de Altos Estudios Nacionales, Instituto Nacional de Altos Estudios Policiales, Universidad Federico Villarreal, etc

2. Encuesta. A nivel de la encuesta se utilizó como instrumento un Cuestionario aplicada a miembros de las instituciones del sector

público encargados de su control.

Para la recolección de datos a nivel de la utilización del cuestionario se fundamentó en una serie de preguntas y que nos permita tener una visión más amplia del tema, en función a la opinión vertida por los encuestados. Las preguntas del cuestionario son cerradas y mixtas, así como de concepto a fin que sean llenadas por éstos, para lo cual se les dio un plazo adecuado para su llenado. Luego se procedió a recoger dicho cuestionario y a vaciar los resultados en la matriz que para el efecto se tuvo preparada.

Para describir los datos, valores o puntuaciones recolectadas se empleó la herramienta estadística de la Distribución de Frecuencias, la cual permite ordenar categorías de acuerdo a las puntuaciones, completando esta herramienta con frecuencias relativas o porcentajes en cada categoría y frecuencias de cada categoría.

Para la contrastación de las Hipótesis se utilizaron los datos de la muestra los cuales se formularon y calcularon con coeficientes de validez específicos como la prueba de chi cuadrada.

El cuestionario estructurado empleado en la presente investigación tiene una revisión por tres jueces expertos, para su **validación,** donde se analizaron el contenido del instrumento y la concordancia con los objetivos del estudio, donde se cumplieron los siguientes criterios:

a) El instrumento tiene claridad.
b) Las preguntas tiene objetividad.
c) El instrumento es actual
d) El instrumento tiene un constructo organizado
e) El instrumento es suficiente en dimensiones

f) El instrumento valora la teoría del trabajo.
g) El instrumento es consistente
h) El instrumento tiene coherencia
i) El instrumento tiene concordancia metodológica.
j) El instrumento es pertinente para la ciencia.

Antes de preparar el cuestionario, esta fue sometida a la prueba de validación a cargo de 3 expertos, los que emitieron su informe respectivo, el cual está compuesto por el Dr. José Toledo Valdivia, Dr. Oswaldo García Bedoya, y Dr. Edwin Cruz Aspajo, para su validación, donde analizaron el contenido del instrumento y la concordancia con los objetivos del estudio, donde se cumplieron los siguientes criterios:

a) El instrumento tiene claridad.
b) Las preguntas tiene objetividad.
c) El instrumento es actual
d) El instrumento tiene un constructo organizado
e) El instrumento es suficiente en dimensiones
f) El instrumento valora la teoría del trabajo.
g) El instrumento es consistente
h) El instrumento tiene coherencia
i) El instrumento tiene concordancia metodológica.
j) El instrumento es pertinente para la ciencia.

A continuación se presenta un cuadro resumen de los resultados de la validación:

Si = 1 No = 2

Cuadro Nº 2

Resultados de la validación del contenido del Cuestionario

ÁREA	CALIFICACIÓN			Resultado
	1	2	3	
a	1	1	1	100.0%
b	1	1	1	100.0%
c	1	1	1	100.0%
d	1	1	1	100.0%
e	1	1	1	100.0%
f	1	1	1	100.0%
g	1	1	1	100.0%
h	1	1	1	100.0%
I	1	1	2	66.6%
j	1	1	2	66.6%

Fuente: propia

Se concluye en que hubo concordancia de los jueces al 93.32%. Por lo tanto, el instrumento tiene validez de contenido.

La confiabilidad del instrumento de confiabilidad, medido por el Alfa de Cronbach, alcanzo un 0.902.

Estadístico de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N° de elementos
0,902	0,902	8

Fuente: propia

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. PRESENTACIÓN DE RESULTADOS

A continuación se presenta la ejecución de resultados

TABLA N° 1: Percepción sobre existencia de un alto nivel alcanzado por el intrusismo informático dentro de las modalidades del cibercrimen en el país

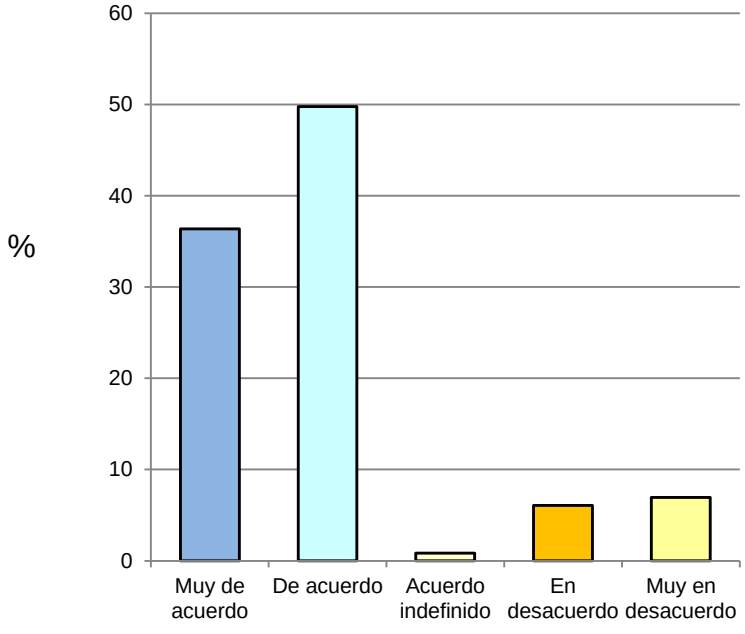
Xi	Ni	%
Muy de acuerdo	84	36.36
De acuerdo	115	49.78
Indefinido	2	0.86
En desacuerdo	14	6.06
Muy en desacuerdo	16	6.94
Total	**231**	**100.00**

Los resultados de este cuadro nos indican en que existe un alto nivel de percepción sobre la existencia de un alto nivel alcanzado por el intrusismo informático dentro de las modalidades del cibercrimen en el país, donde un 86.14%, de los encuestados percibe dicha influencia. Un 6.06% interpreta que es débil este marco, con la afirmación en desacuerdo, y un 6.94% está muy en desacuerdo.

Esto significa que el intrusismo informático dentro de las modalidades del cibercrimen en el país constituye una de las principales amenazas a la seguridad nacional.

Gráfico Nº 1

Percepción sobre existencia de un alto nivel alcanzado por el intrusismo informático dentro de las modalidades del cibercrimen en el país



CUADRO N° 2: Percepción sobre existencia de un alto nivel alcanzado por el sabotaje informático dentro de las modalidades del cibercrimen en el país

Xi	Ni	%
Muy de acuerdo	68	29.44
De acuerdo	73	31.60
Indefinido	35	15.15
En desacuerdo	33	14.29
Muy en desacuerdo	22	9.52
Total	**231**	**100.00**

Dentro de los efectos de este cuadro, se puede inferir en un 61.04% de la muestra perciben la existencia de un alto nivel alcanzado por el sabotaje informático dentro de las modalidades del cibercrimen en el país.

Un nivel del 14.29% de la muestra se encuentra muy en desacuerdo y un 9.52% en desacuerdo con esta influencia.

Esto indica que los encuestados son conscientes de una fuerte relación del sabotaje informático como una de las principales modalidades del cibercrimen en el país.

Gráfico Nº 2

Percepción sobre existencia de un alto nivel alcanzado por el sabotaje informático dentro de las modalidades del cibercrimen en el país

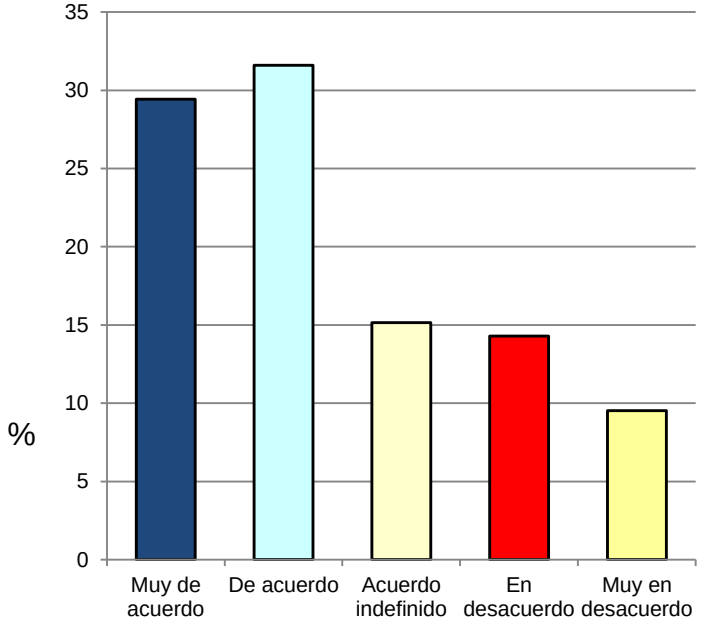


TABLA N° 3: Percepción sobre la existencia de un alto nivel alcanzado por los delitos informáticos dentro de la estructura del cibercrimen en el país

Xi	Ni	%
Muy de acuerdo	89	38.54
De acuerdo	97	41.99
Indefinido	8	3.46
En desacuerdo	22	9.52
Muy en desacuerdo	15	6.49
Total	**231**	**100.00**

Dentro de la condición básica sobre la existencia de un alto nivel alcanzado por los delitos informáticos dentro de la estructura del cibercrimen en el país, se percibe que un 80.53% de los mismos perciben dicha actividad delictiva.

Un 9.52% está en desacuerdo y un 6.49% muy en desacuerdo con que los encuestados aceptan la existencia de este marco.

Esto nos indica que dentro de la estructura del cibercrimen en el país, los delitos informáticos alcanza ribetes de amenaza para la sociedad.

.

.

Gráfico Nº 3

Percepción sobre existencia de un alto nivel alcanzado por los delitos informáticos dentro de la estructura del cibercrimen en el país

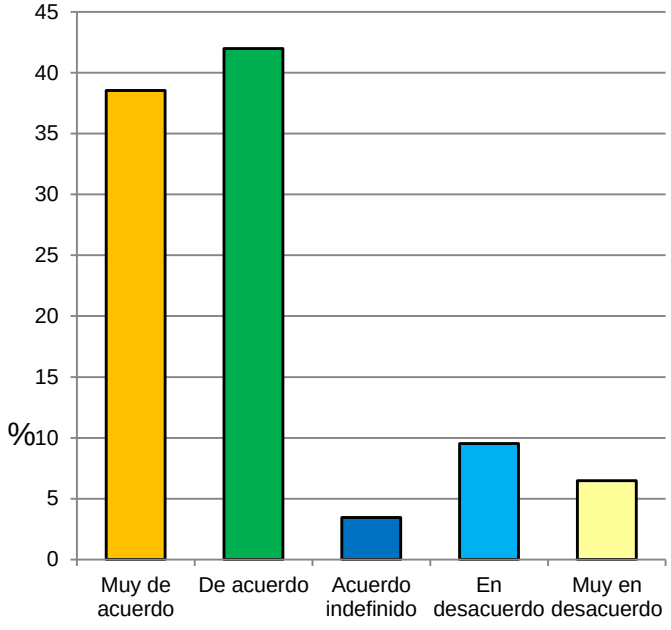


TABLA N° 4: Percepción sobre la existencia de un alto nivel alcanzado por la irresponsabilidad funcional de los encargados informáticos dentro de la estructura del cibercrimen en el país

Xi	Ni	%
Muy de acuerdo	73	31.60
De acuerdo	67	29.00
Indefinido	7	3.03
En desacuerdo	48	20.78
Muy en desacuerdo	21	15.59
Total	**216**	**100.00**

Los resultados de éste cuadro, nos indican según los encuestados, que existe una tendencia a un alto nivel en la existencia de un alto nivel alcanzado por la irresponsabilidad funcional de los encargados informáticos dentro de la estructura del cibercrimen en el país, el cual llega a un 60.60%, de la muestra. Solo un 20.78% está en desacuerdo con que existe esta relación y un 15.59% muy de acuerdo.

Esto significa que existe una falta de una mayor diligencia de los encargados informáticos dentro de la estructura del cibercrimen en el país.

Gráfico Nº 4

Percepción sobre existencia de un alto nivel alcanzado por la irresponsabilidad funcional de los encargados informáticos dentro de la estructura del cibercrimen en el país

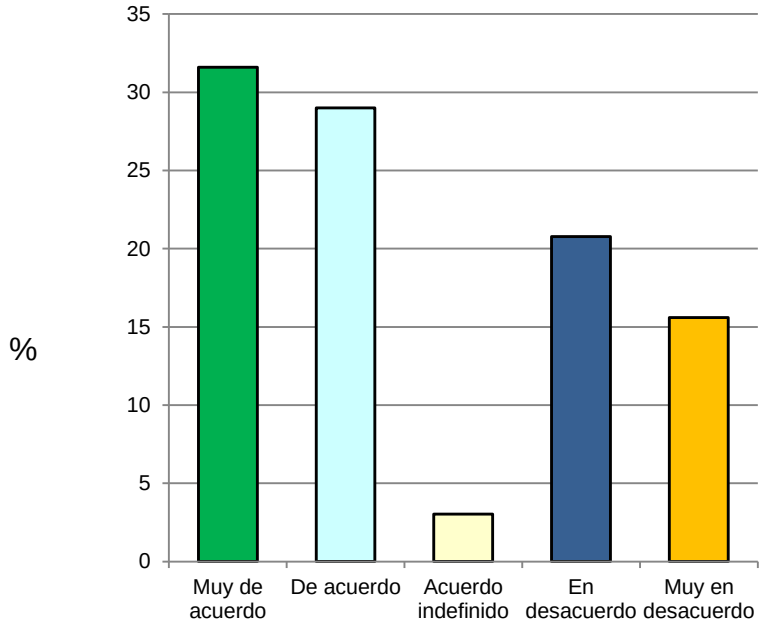


TABLA N° 5: Percepción sobre la existencia de un alto nivel alcanzado por la frecuencia de ataques informáticos dentro de las técnicas del cibercrimen en el país

Xi	Ni	%
Muy de acuerdo	86	37.23
De acuerdo	91	39.39
Indefinido	4	1.73
En desacuerdo	20	8.66
Muy en desacuerdo	30	12.99
Total	**231**	**100.00**

Los resultados de este cuadro nos indican que existe un alto nivel alcanzado por la frecuencia de ataques informáticos dentro de las técnicas del cibercrimen en el país, donde un 76.62%, de los encuestados, perciben dicha influencia. Un total del 8.66% de la muestra no perciben esta influencia y un 12.99% está en desacuerdo.

Esto significa que existe frecuencia de ataques informáticos dentro de las técnicas del cibercrimen en el país que afecta a la seguridad nacional.

Gráfico Nº 5

Percepción sobre la existencia de un alto nivel alcanzado por la frecuencia de ataques informáticos dentro de las técnicas del cibercrimen en el país

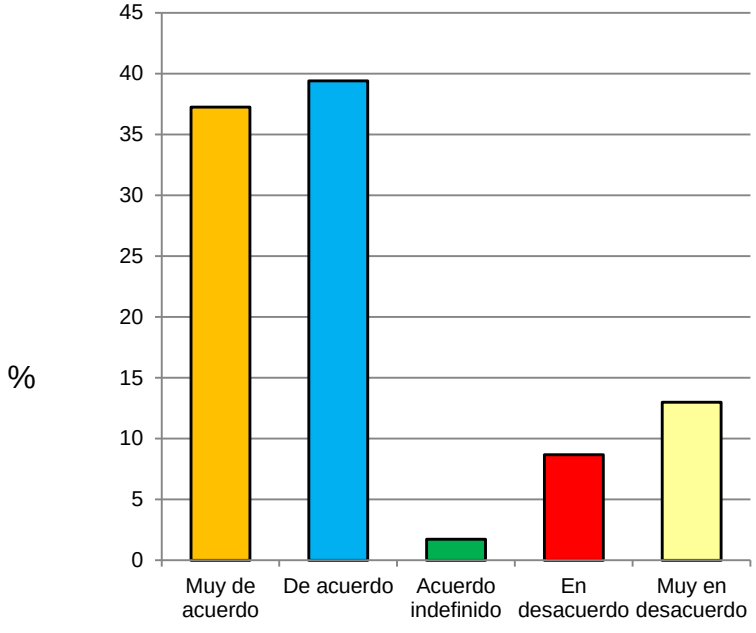


TABLA N° 6: Percepción sobre existencia de un alto nivel alcanzado por la presencia de hackers dentro de las técnicas del cibercrimen en el país

Xi	Ni	%
Muy de acuerdo	61	26.41
De acuerdo	64	27.70
Indefinido	26	11.26
En desacuerdo	43	18.61
Muy en desacuerdo	37	16.02
Total	**231**	**100.00**

Los resultados de éste cuadro nos indican que un 54.11% de los encuestados perciben que existe una percepción alta sobre la existencia de un alto nivel alcanzado por la presencia de hackers dentro de las técnicas del cibercrimen en el país. Asimismo un 34.63% de los encuestados manifestaron no percibir dicha existencia.

Esto significa que para los encuestados existe cierta influencia de los hackers dentro de las técnicas del cibercrimen en el país.

Gráfico Nº 6

Percepción sobre existencia de un alto nivel alcanzado por la presencia de hackers dentro de las técnicas del cibercrimen en el país

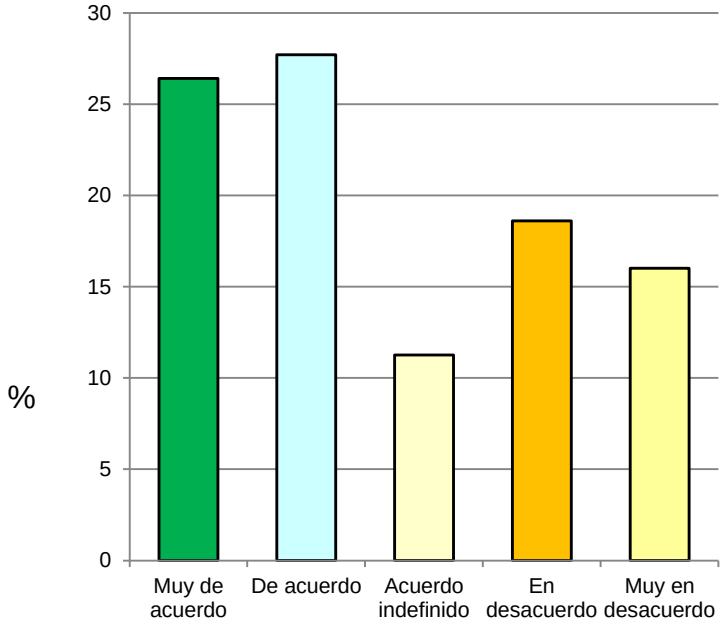


TABLA N° 7: Percepción sobre existencia del control efectivo de la estructura informática dentro de la Seguridad Nacional

Xi	Ni	%
Muy de acuerdo	32	13.85
De acuerdo	34	14.72
Indefinido	32	13.85
En desacuerdo	72	31.17
Muy en desacuerdo	61	26.41
Total	**231**	**100.00**

Dentro de la muestra analizada, los encuestados mencionan que perciben una baja existencia de control efectivo de la estructura informática dentro de la Seguridad Nacional, así un 57.58% en la muestra no percibe este precepto del control; un 14.72% está de acuerdo que exista esta suficiencia, mientras que un 13.85% está muy de acuerdo.

Estos resultados son importantes dentro de la parte estructural debido a que la existencia de un bajo control efectivo afecta a la estructura informática dentro de la Seguridad Nacional.

.

Gráfico Nº 7

Percepción sobre existencia del control efectivo de la estructura informática dentro de la Seguridad Nacional

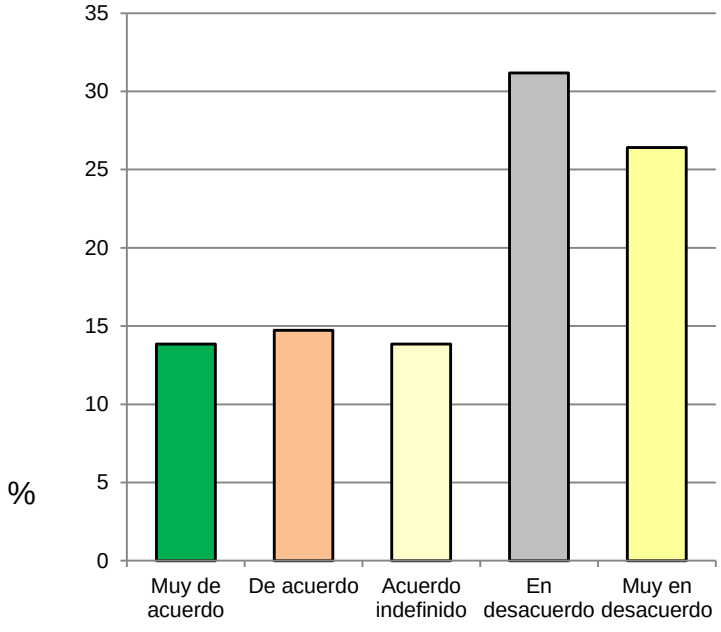


TABLA N° 8: Percepción sobre existencia de cumplimiento de los reglamentos de la estructura informática dentro de la Seguridad Nacional

Xi	Ni	%
Muy de acuerdo	41	17.75
De acuerdo	49	21.21
Indefinido	20	8.66
En desacuerdo	63	27.27
Muy en desacuerdo	58	25.11
Total	**231**	**100.00**

Lo que se deduce de éste cuadro, es que los encuestados no perciben la existencia de cumplimiento de los reglamentos de la estructura informática dentro de la Seguridad Nacional, considerando que existe un 52.38% de la muestra que no perciben este precepto.

Un 21.21% de la muestra considera que existe una normal relación de cumplimiento legal y un 17.75% muy de acuerdo. Estos indicadores señalan que existe incumplimiento de los reglamentos de la estructura informática dentro de la Seguridad Nacional

Gráfico Nº 8

Percepción sobre existencia de cumplimiento de los reglamentos de la estructura informática dentro de la Seguridad Nacional

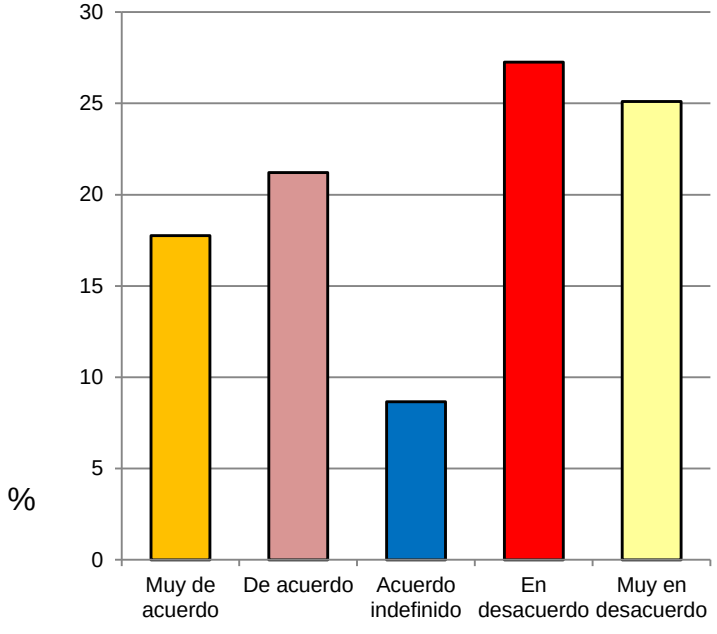


TABLA N° 9: Percepción sobre existencia de optimización del control de los programas en la protección de la data dentro de la Seguridad Nacional

Xi	Ni	%
Muy de acuerdo	27	11.69
De acuerdo	43	18.62
Indefinido	7	3.03
En desacuerdo	78	33.76
Muy en desacuerdo	76	32.90
Total	**231**	**100.00**

Dentro de la condición básica sobre la necesidad de optimización del control de los programas en la protección de la data dentro de la Seguridad Nacional, se percibe que un 66.66% de los mismos perciben que no se encuentra mayor énfasis.

Un 18.62% está de acuerdo y un 11.69% muy de acuerdo con que los encuestados aceptan la existencia de este marco.

Esto nos indica que los actuales encuestados opinan que no existe mayor optimización del control de los programas en la protección de la data dentro de la Seguridad Nacional

.

Gráfico Nº 9

Percepción sobre existencia de optimización del control de los programas en la protección de la data dentro de la Seguridad Nacional

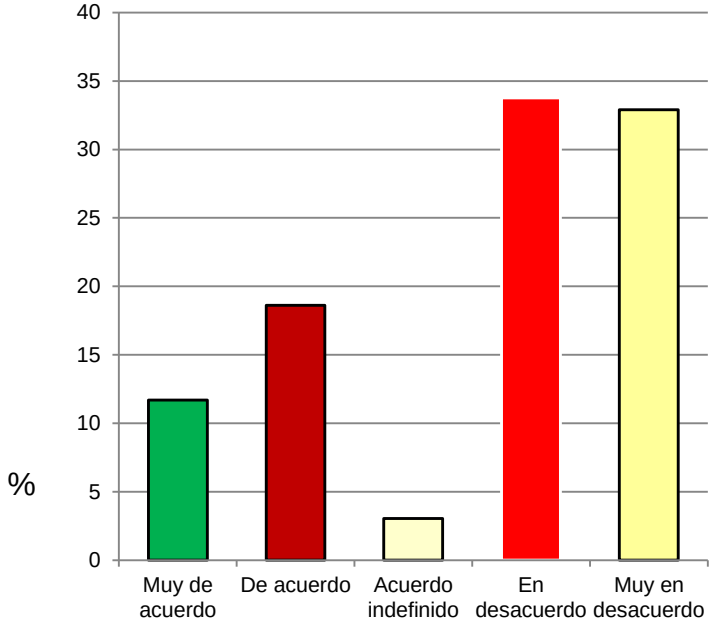


TABLA N° 10: Percepción sobre existencia de optimización de las normas legales para la protección de la data dentro de la Seguridad Nacional

Xi	Ni	%
Muy de acuerdo	23	9.96
De acuerdo	25	10.82
Indefinido	9	3.90
En desacuerdo	97	41.99
Muy en desacuerdo	77	33.33
Total	**231**	**100.00**

Los resultados de éste cuadro, nos indican según los encuestados, que existe una tendencia a un bajo nivel en la existencia de optimización de las normas legales para la protección de la data dentro de la Seguridad Nacional, el cual llega a un 75.32%, de la muestra. Solo un 10.82% está de acuerdo con que existe efectividad de las normas legales y un 9.96% muy de acuerdo.

Esto significa que existe baja existencia de optimización de las normas legales para la protección de la data dentro de la Seguridad Nacional y que es generado por la falta de integración del control administrativo legal en la materia.

Gráfico Nº 10

Percepción sobre existencia de optimización de las normas legales para la protección de la data dentro de la Seguridad Nacional

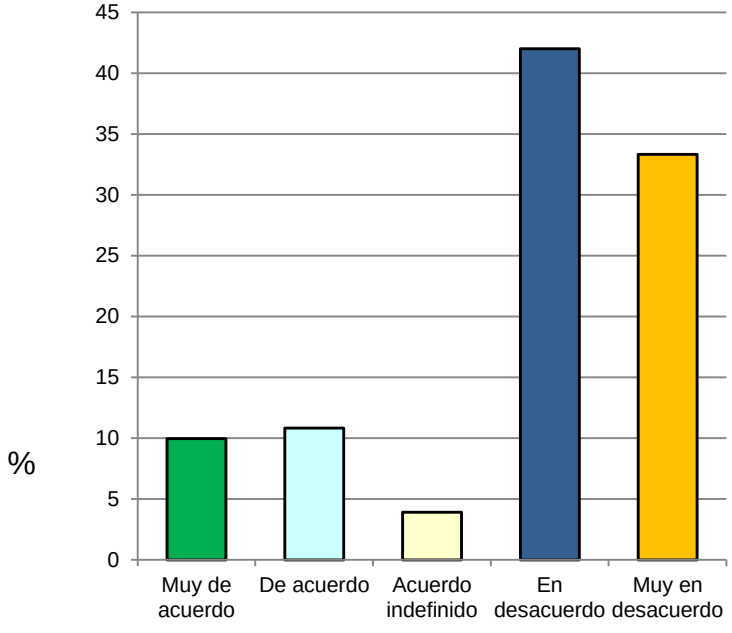


TABLA N° 11: Percepción sobre existencia de eficacia de las políticas a nivel informático en los fines de la Seguridad Nacional

Xi	Ni	%
Muy de acuerdo	26	11.25
De acuerdo	33	14.28
Indefinido	12	5.19
En desacuerdo	82	35.50
Muy en desacuerdo	78	33.78
Total	**231**	**100.00**

Los resultados de éste cuadro, nos indican según los encuestados, que existe una tendencia a un bajo nivel de existencia de eficacia de las políticas a nivel informático en los fines de la Seguridad Nacional, el cual llega a un 69.28%, de la muestra. Solo un 14.28% está de acuerdo con que existe este dominio y un 11.25% muy de acuerdo.

Esto significa que existe poca efectividad de las políticas a nivel informático en los fines de la Seguridad Nacional.

Gráfico Nº 11

Percepción sobre existencia de eficacia de las políticas a nivel informático en los fines de la Seguridad Nacional

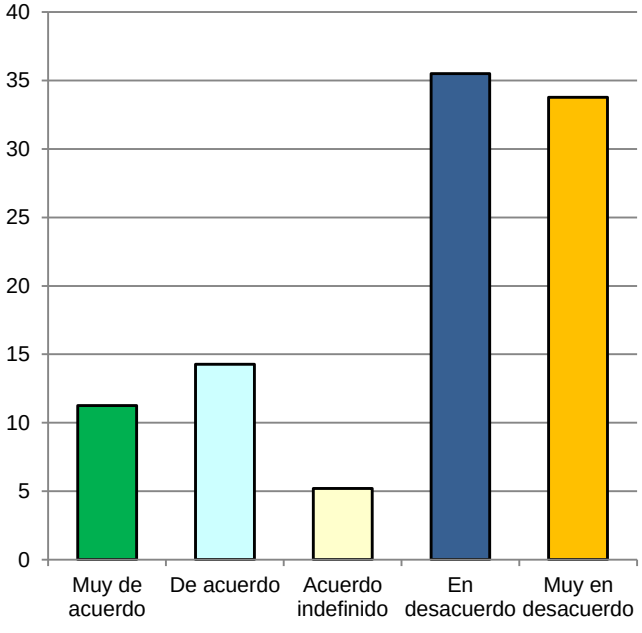


TABLA N° 12: Percepción sobre existencia de cumplimiento de objetivos a nivel informático en los fines de la Seguridad Nacional

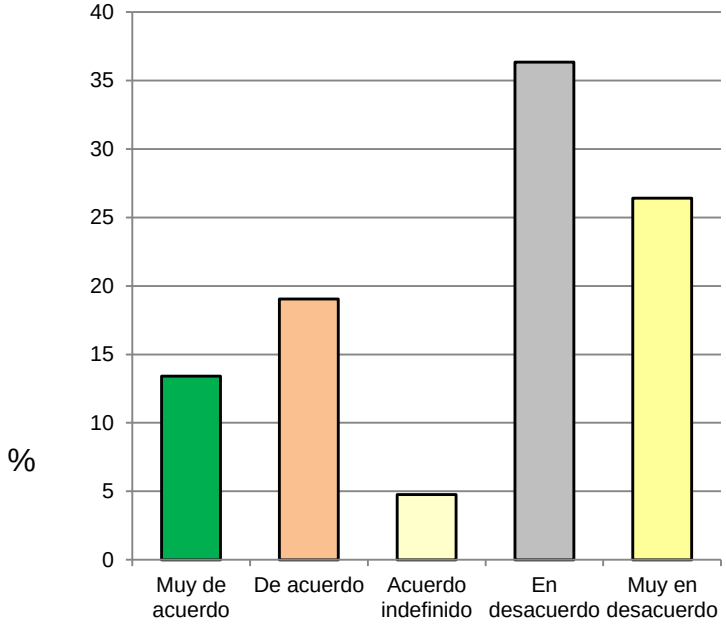
Xi	Ni	%
Muy de acuerdo	31	13.42
De acuerdo	44	19.05
Indefinido	11	4.76
En desacuerdo	84	36.36
Muy en desacuerdo	61	26.41
Total	**231**	**100.00**

Dentro de la muestra analizada, los encuestados mencionan que perciben una baja eficacia del cumplimiento de objetivos a nivel informático en los fines de la Seguridad Nacional, así un 62.77% en la muestra no percibe este precepto; un 19.05% está de acuerdo que exista este precepto, mientras que un 13.42% está muy de acuerdo.

Estos resultados son importantes dentro de la parte estructural debido a que los fines de la Seguridad Nacional no se efectivizan por el incumplimiento de objetivos a nivel informático.

Gráfico Nº 12

Percepción sobre existencia de cumplimiento de objetivos a nivel informático en los fines de la Seguridad Nacional



4.2. PRESENTACIÓN DE RESULTADOS

4.2.1. CONTRASTACION DE LA HIPÓTESIS GENERAL

Considerando que una hipótesis constituye un valioso instrumento de la investigación, pues permite desarrollar la teoría con la observación y viceversa, y que cuando se prueba esta, existen dos posibles resultados:

Ho (hipótesis nula): “El nivel alcanzado por el Cibercrimen en el Perú no afecta significativamente a la Seguridad nacional”.

H1 (hipótesis alternativa): “El nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional”.

Para realizar la contrastación de Hipótesis se hizo uso de la técnica Estadística de la Prueba Chi-Cuadrada cruzada, toda vez que se trata de demostrar la contribución o no de las variables: Cibercrimen en el Perú y la Seguridad nacional, habiéndose aplicado sobre las tablas N° 3 y 11 respectivamente, el cual representa a un amplio conjunto de observaciones sobre un acontecimiento o variable. Para ello se ha realizado la siguiente secuencia de actividades de demostración:

1. Se empleó como estadístico de prueba, la chi–cuadrada.

2. Se buscó en la tabla estadística con un α = 0.01 y 8 grados de libertad, y se obtuvó un valor de 20.09.

3. Se combinó los datos de las tablas N° 3 y Nº 11, dándonos los siguientes resultados de la frecuencia observada.

Escala	Nivel		
	Tbla 3	Tbla 11	Total
Muy de acuerdo	89	26	115
De acuerdo	97	33	130
Acuerdo indefinido	8	12	20
En desacuerdo	22	82	104
Muy en desacuerdo	15	78	93
Total	231	231	462

4. Se utilizó la siguiente fórmula para la determinación de la frecuencia esperada de las tablas N° 3 y Nº 11:

Eij= (Nai x Nbj) /N

Dándonos los siguientes resultados:

E11= (115 x 231) /462 = 57.50
E12= (115 x 231) /462 = 57.50
E21= (130 x 231) /462 = 65.00
E22= (130 x 231) /462 = 65.00
E31= (20 x 231) /462 = 10.00
E32= (20 x 231) /462 = 10.00
E41= (104 x 231) /462 = 52.00
E42= (104 x 231) /462 = 52.00
E51= (93 x 231) /462 = 46.50
E52= (93 x 231) /462 = 46.50

5. Se utilizó la formula la determinación del chi cuadrado y se halló:

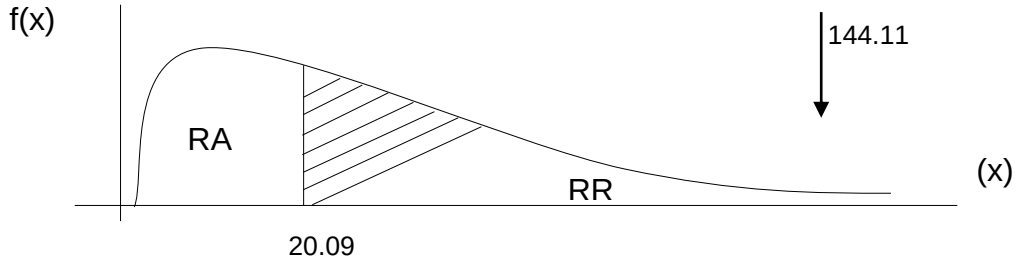
$$\chi^2 = \frac{\Sigma\,(fo - fe)^2}{fe}$$

$$\frac{(89-57.50)^2}{57.50} + \frac{(26-57.50)^2}{57.50} + \frac{(97-65.00)^2}{65.00} + \frac{(33-65.00)^2}{65.00} + \frac{(8-10.00)^2}{10.00} +$$

$$\frac{(12-10.00)^2}{10.00} + \frac{(22-52.00)^2}{52.00} + \frac{(82-52.00)^2}{52.00} + \frac{(15-46.50)^2}{46.50} + \frac{(78-46.50)^2}{46.50} =$$

$\chi^2 = 144.1132$

6. Identificamos la Región de Aceptación (RA) Región de Rechazo (RR) de la Hipótesis Nula.



Como el valor de χ^2 pertenece a la Región de rechazo por lo tanto no aceptamos la Hipótesis Nula (Ho) y aceptamos la Hipótesis alternativa (H1), por tanto se demuestra que el nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional.

4.2.2. CONTRASTACIÓN DE LAS HIPÓTESIS ESPECÍFICAS

a) Contrastación de la hipótesis especifica 1

Considerando que una hipótesis constituye un valioso instrumento de la

investigación, pues permite desarrollar la teoría con la observación y viceversa, y que cuando se prueba esta, existen dos posibles resultados:

Ho (hipótesis nula): “El nivel alcanzado por las modalidades del Cibercrimen en el Perú no afecta significativamente a la estructura informática de la Seguridad nacional”

H1 (hipótesis alternativa): “El nivel alcanzado por las modalidades del Cibercrimen en el Perú afecta significativamente a la estructura informática de la Seguridad nacional”

Para realizar la contrastación de Hipótesis se hizo uso de la técnica Estadística de la Prueba Chi-Cuadrada cruzada, toda vez que se trata de demostrar la contribución o no de las variables: Las modalidades del Cibercrimen en el Perú y la estructura informática de la Seguridad nacional” habiéndose aplicado sobre las tablas N° 1 y 7 respectivamente, el cual representa a un amplio conjunto de observaciones sobre un acontecimiento o variable. Para ello se ha realizado la siguiente secuencia de actividades de demostración:

1. Se empleó como estadístico de prueba, la chi–cuadrada.

2. Se buscó en la tabla estadística con un α = 0.01 y 8 grados de libertad, y se obtuvó un valor de 20.09.

3. Se combinó los datos de las tablas N° 1 y Nº 7, dándonos los siguientes resultados de la frecuencia observada.

Escala	Nivel		
	Tbla 1	Tbla 7	Total
Muy de acuerdo	84	32	116
De acuerdo	115	34	149
Acuerdo indefinido	2	32	34
En desacuerdo	14	72	86
Muy en desacuerdo	16	61	77
Total	231	231	462

4. Se utilizó la siguiente fórmula para la determinación de la frecuencia esperada de las tablas N° 1 y Nº 7:

Eij= (Nai x Nbj) /N

Dándonos los siguientes resultados:

E11= (116 x 231) /462 = 58.00
E12= (116 x 231) /462 = 58.00
E21= (149 x 231) /462 = 74.50
E22= (149 x 231) /462 = 74.50
E31= (34 x 231) /462 = 17.00
E32= (34 x 231) /462 = 17.00
E41= (86 x 231) /462 = 43.00
E42= (86 x 231) /462 = 43.00
E51= (77 x 231) /462 = 38.50
E52= (77 x 231) /462 = 38.50

5. Se utilizó la formula la determinación del chi cuadrado y se halló:

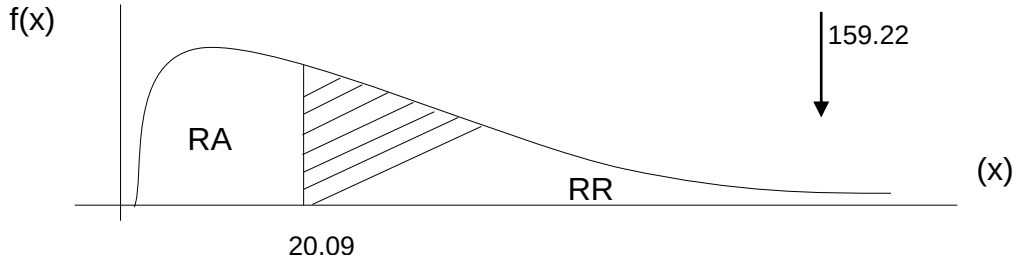
$$\chi^2 = \frac{\Sigma\,(fo - fe)^2}{fe}$$

$$\frac{(84-58.00)^2}{58.00} + \frac{(32-58.00)^2}{58.00} + \frac{(115-74.50)^2}{74.50} + \frac{(34-74.50)^2}{74.40} + \frac{(2-17.00)^2}{17.00} +$$

$$\frac{(32-17.00)^2}{17.00} + \frac{(14-43.00)^2}{43.00} + \frac{(72-43.00)^2}{43.00} + \frac{(16-38.50)^2}{38.50} + \frac{(61-38.50)^2}{38.50} =$$

$\chi^2 = 159.2288$

6. Identificamos la Región de Aceptación (RA) Región de Rechazo (RR) de la Hipótesis Nula.



Como el valor de χ^2 pertenece a la Región de rechazo por lo tanto no aceptamos la Hipótesis Nula (Ho) y aceptamos la Hipótesis alternativa (H1), por tanto se demuestra que el nivel alcanzado por las modalidades del Cibercrimen en el Perú afecta significativamente a la estructura informática de la Seguridad nacional.

b) Contrastación de la hipótesis especifica 2

Considerando que una hipótesis constituye un valioso instrumento de la investigación, pues permite desarrollar la teoría con la observación

y viceversa, y que cuando se prueba esta, existen dos posibles resultados:

Ho (hipótesis nula): ”El nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú no afecta significativamente a la protección de la data de la Seguridad nacional”.

H1 (hipótesis alternativa): ”El nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú afecta significativamente a la protección de la data de la Seguridad nacional”.

Para realizar la contrastación de Hipótesis se hizo uso de la técnica Estadística de la Prueba Chi-Cuadrada cruzada, toda vez que se trata de demostrar la contribución o no de las variables: La estructura organizativa del Cibercrimen en el Perú y la protección de la data de la Seguridad nacional, habiéndose aplicado sobre las tablas N° 4 y 9 respectivamente, el cual representa a un amplio conjunto de observaciones sobre un acontecimiento o variable. Para ello se ha realizado la siguiente secuencia de actividades de demostración:

1. Se empleó como estadístico de prueba, la chi–cuadrada.

2. Se buscó en la tabla estadística con un α = 0.01 y 8 grados de libertad, y se obtuvó un valor de 20.09.

3. Se combinó los datos de las tablas N° 4 y Nº 9, dándonos los siguientes resultados de la frecuencia observada.

Escala	Nivel		
	Tbla 4	Tbla 9	Total
Muy de acuerdo	73	27	100
De acuerdo	67	43	110
Acuerdo indefinido	7	7	14
En desacuerdo	48	78	126
Muy en desacuerdo	36	76	112
Total	231	231	462

4. Se utilizó la siguiente fórmula para la determinación de la frecuencia esperada de las tablas N° 4 y Nº 9:

Eij= (Nai x Nbj) /N

Dándonos los siguientes resultados:

E11= (100 x 231) /462 = 50.00
E12= (100 x 231) /462 = 50.00
E21= (110 x 231) /462 = 55.00
E22= (110 x 231) /462 = 55.00
E31= (14 x 231) /462 = 7.00
E32= (14 x 231) /462 = 7.00
E41= (126 x 231) /462 = 63.00
E42= (126 x 231) /462 = 63.00
E51= (112 x 231) /462 = 56.00
E52= (112 x 231) /462 = 56.00

5. Se utilizó la formula la determinación del chi cuadrado y se halló:

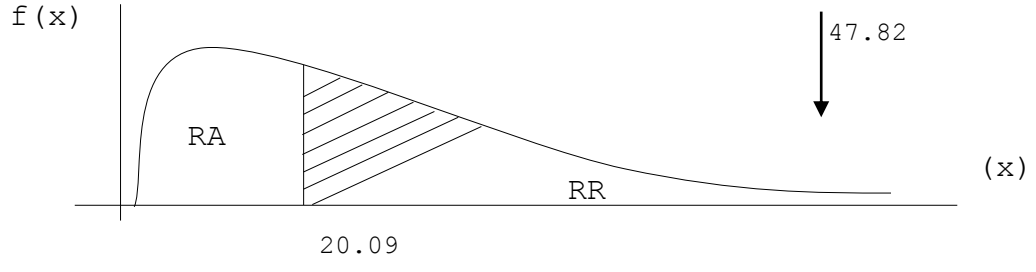
$$\chi^2 = \frac{\Sigma\,(fo - fe)^2}{fe}$$

$$\frac{(73-50.00)^2}{50.00} + \frac{(27-50.00)^2}{50.00} + \frac{(67-55.00)^2}{55.00} + \frac{(43-55.00)^2}{55.00} + \frac{(7-7.00)^2}{7.00} +$$

$$\frac{(7-7.00)^2}{7.00} + \frac{(48-63.00)^2}{63.00} + \frac{(78-63.00)^2}{63.00} + \frac{(36-56.00)^2}{56.00} + \frac{(76-56.00)^2}{56.00} =$$

$\chi^2 = 47.8246$

6. Identificamos la Región de Aceptación (RA) Región de Rechazo (RR) de la Hipótesis Nula.



Como el valor de χ^2 pertenece a la Región de rechazo por lo tanto no aceptamos la Hipótesis Nula (Ho) y aceptamos la Hipótesis alternativa (H1), por tanto se demuestra que el nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú afecta significativamente a la protección de la data de la Seguridad nacional.

c) Contrastación de la hipótesis especifica 3

Considerando que una hipótesis constituye un valioso instrumento de la investigación, pues permite desarrollar la teoría con la observación y viceversa, y que cuando se prueba esta, existen dos posibles resultados:

Ho (hipótesis nula): ““El nivel alcanzado por las técnicas del Cibercrimen en el Perú no afecta significativamente a los fines de la Seguridad nacional”

H1 (hipótesis alternativa): “El nivel alcanzado por las técnicas del Cibercrimen en el Perú afecta significativamente a los fines de la Seguridad nacional”

Para realizar la contrastación de Hipótesis se hizo uso de la técnica Estadística de la Prueba Chi-Cuadrada cruzada, toda vez que se trata de demostrar la contribución o no de las variables: Las técnicas del Cibercrimen en el Perú y los fines de la Seguridad nacional, habiéndose aplicado sobre las tablas N° 5 y 12 respectivamente, el cual representa a un amplio conjunto de observaciones sobre un acontecimiento o variable. Para ello se ha realizado la siguiente secuencia de actividades de demostración:

1. Se empleó como estadístico de prueba, la chi–cuadrada.

2. Se buscó en la tabla estadística con un α = 0.01 y 8 grados de libertad, y se obtuvó un valor de 20.09.

3. Se combinó los datos de las tablas N° 5 y Nº 12, dándonos los siguientes resultados de la frecuencia observada.

Escala	Nivel		
	Tbla 5	Tbla 12	Total
Muy de acuerdo	89	31	120
De acuerdo	97	44	141
Acuerdo indefinido	8	11	19
En desacuerdo	22	84	106
Muy en desacuerdo	15	61	76
Total	231	231	462

4. Se utilizó la siguiente fórmula para la determinación de la frecuencia esperada de las tablas N° 5 y Nº 12:

Eij= (Nai x Nbj) /N

Dándonos los siguientes resultados:

E11= (120 x 231) /462 = 60.00
E12= (120 x 231) /462 = 60.00
E21= (141 x 231) /462 = 70.50
E22= (141 x 231) /462 = 70.50
E31= (19 x 231) /462 = 9.50
E32= (19 x 231) /462 = 9.50
E41= (106 x 231) /462 = 53.00
E42= (106 x 231) /462 = 53.00
E51= (76 x 231) /462 = 38.00
E52= (76 x 231) /462 = 38.00

5. Se utilizó la formula la determinación del chi cuadrado y se halló:

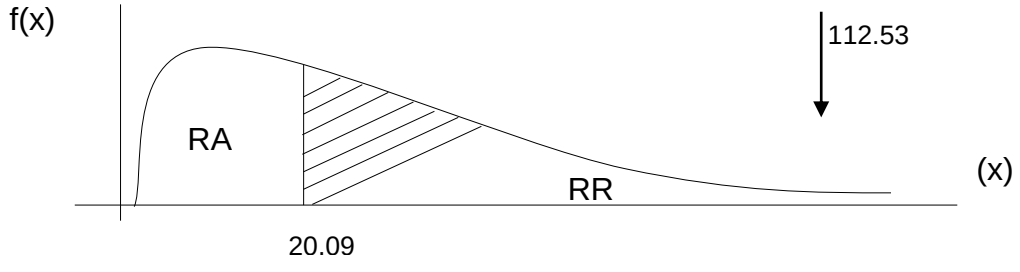
$$\chi^2 = \frac{\Sigma\,(fo - fe)^2}{fe}$$

$$\frac{(89-60.00)^2}{60.00} + \frac{(31-60.00)^2}{60.00} + \frac{(97-70.50)^2}{70.50} + \frac{(44-70.50)^2}{70.50} + \frac{(8-9.50)^2}{9.50} +$$

$$\frac{(11-9.50)^2}{9.50} + \frac{(22-53.00)^2}{53.00} + \frac{(84-53.00)^2}{53.00} + \frac{(15-38.00)^2}{38.00} + \frac{(61-38.00)^2}{38.00} =$$

$\chi^2 = 112.5346$

6. Identificamos la Región de Aceptación (RA) Región de Rechazo (RR) de la Hipótesis Nula.



Como el valor de χ^2 pertenece a la Región de rechazo por lo tanto no aceptamos la Hipótesis Nula (Ho) y aceptamos la Hipótesis alternativa (H1), por tanto se demuestra que el nivel alcanzado por las técnicas del Cibercrimen en el Perú afecta significativamente a los fines de la Seguridad nacional.

4.3. CONCLUSIONES

4.3.1. Conclusión general

Se ha determinado mediante esta investigación que el nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional.

4.3.2. Conclusiones Específicas

a) Se ha determinado mediante esta investigación que el nivel alcanzado por las modalidades del Cibercrimen en el Perú afecta significativamente a la estructura informática de la Seguridad nacional

b) Se ha determinado mediante esta investigación que el nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú afecta significativamente a la protección de la data de la Seguridad nacional.

c) Se ha determinado mediante esta investigación que el nivel alcanzado por las técnicas del Cibercrimen en el Perú afecta significativamente a los fines de la Seguridad nacional

4.4. RECOMENDACIONES

a) Considerando por los resultados obtenidos que el nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional; es necesario implementar una gestión de control de la información y que puedan ser sujetos de los ataques de las diversas modalidades basados en el cuidado de los procesos donde existan mayor intrusión, con diversas funciones prácticas y documentadas

con la finalidad de mejorar la calidad de los servicios producidos, de modo que sea posible elevar el resguardo de la datas y que sean compatibles con la necesidad de la Seguridad nacional.

b) Considerando por los resultados obtenidos que el nivel alcanzado por las modalidades del Cibercrimen en el Perú afecta significativamente a la estructura informática de la Seguridad nacional, es necesario solucionar las deficiencias actuales relacionadas a la interacción grupal y coordinación con otras instancias de control de la informacion del ámbito de la seguridad del Estado, a fin de mejorar la operatividad de las acciones de supervisión informatica.

c) Considerando por los resultados obtenidos que el nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú afecta significativamente a la protección de la data de la Seguridad nacional**,** es necesario procurar una capacitación al personal operativo para lograr una eficacia organizacional en materia de seguridad de la información.

d) Considerando por los resultados obtenidos que el nivel alcanzado por las técnicas del Cibercrimen en el Perú afecta significativamente a los fines de la Seguridad nacional; es pertinente que las estrategias se diseñen en forma altamente competitiva, para que pueda contribuir a optimizar el proceso de control de los ataques informaticos y reguardo de la data, contando para ello con un proceso de evaluación de las acciones de supervisión basadas en:

   - Lograr una plena automatización de trámites, en el aspecto informativo, en el nivel interactivo y en lo transaccional, aunque en este último campo el avance del control es urgente.

- Se deben establecer redes de coordinación y colaboración entre diferentes instituciones públicas y privadas, para la debida supervisión y resguardo de la data.

- Los principales factores de control son: el compromiso de la alta dirección institucional; el involucramiento del personal; y el rediseño de objetivos institucionales de las instancias respectivas de control.

- Propender a la certificación de calidad en los servicios, la participación de aliados estratégicos en el sector público, privado y de naturaleza internacional, la inversión tecnológica y el soporte legislativo para impulsar los cambios.

- Se deben superar los cuellos de botella que radican en los trámites administrativos que requieren de mayor seguridad, para la adquisición y contratación de servicios; disposición de locales y su implementación; soporte logístico para la tecnología avanzada; escasez de recursos humanos para atender los servicios descentralizados y el ritmo heterogéneo de trabajo de las instituciones involucradas en la protección de la data.

- Que se debe partir del reconocimiento de la existencia de soluciones ya realizadas por otras entidades públicas, que se pueden recoger vía transferencia de tecnología y capacitaciones.

- Que se debe llegar a contar con una asignación presupuestal adecuada a las exigencias de la protección de la data y su control.

- Asimismo debe alentarse una cultura tecnológica que permita acercar las nuevas tecnologías a los usuarios, creando además versiones amables y simplificadas de los sistemas para que

puedan ser usadas por personas cuyo acceso sea permitido dentro de la seguridad nacional.

- Propender al uso de expedientes electrónicos en el marco de la Ley de Firmas y Certificados Digitales, la cual regula la utilización de la firma electrónica, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otro análoga que conlleve manifestación de voluntad.

- Deberá fomentarse la cooperación interinstitucional e integración de instituciones, donde la necesaria autonomía no signifique que se establezcan islas.

- Es necesario ampliar el acceso y democratización de las TICS (Tecnologías de la Información y la Comunicación), para que llegue al mayor número de personas.

- Se debe propender a generar la certificación ISO 9000 para las mejoras en los procesos de gestión de control del cibercrimen en sus diversas modalidades.

- Es necesario perfeccionar el marco legal imperante contra los delitos informáticos tomando en cuenta los lineamientos del Convenio de Budapest y los Acuerdos Multilaterales de la Organización Mundial de Comercio, aprobados y suscritos por el Perú, los cuales están incluidos dentro del ordenamiento legal interno peruano; teniendo por ejemplo al Acuerdo TRIPS, referido a la propiedad intelectual, refiriéndose específicamente con ciertos artículos a los chips o circuitos integrados aplicados a la actividad informática.

CAPÍTULO V

REFERENCIAS BIBLIOGRÁFICAS

5.1. BIBLIOGRAFÍA

ADRIANZEN OJEDA, M (2005) *Aspectos Penales y Tecnológicos en el Delito de Difamación cometido a través del Internet y su tratamiento en la Legislación Peruana*. Tesis para optar el Grado de Maestro en Derecho penal. Universidad Garcilaso de la Vega.

ALDEGANI, Gustavo Miguel (2005). *Seguridad Informática*, Ediciones MP. Argentina.

ÁLVAREZ BASALDÚA, L (2005) *Seguridad Informática.* Tesis para optar el Grado de Maestro en Ingeniería de Sistema empresariales. Universidad Iberoamericana, Méjico.

CAEN (2012) *Planteamientos Doctrinarios y Metodológicos del Desarrollo, Seguridad y la Defensa Nacional*. Edit. CAEN, Lima, Perú.

CHIAVENATO, Idalberto (2014*) Introducción a la teoría general de la administración*. México: Mc Graw-Hill.

DYE, Thomas R. (2002). *Understanding public policy. Upper Saddle River.* New Jersey: Prentice Hall.

GÓMEZ VIEITES, Alvaro (2006). *Enciclopedia de la Seguridad Informática*, Edit Rama .España.

HERNÁNDEZ SAMPIERI (2014). *Metodología de la Investigación científica*. Edit. Mc Graw Hill. Lima

KUEHL, Dan (2009) Cyberspace & Cyberpower: Defining the Problem, Usa: Cyberpower & National Security,

MAIWALD, Eric (2009) *Fundamentos de seguridad de Redes*. Edit. Mc Graw Hill. Méjico.

Ministerio de Defensa (2006) *Libro Blanco*. Lima: Mindef

MITZBERG, Henry (2003). *Estrategias en organizaciones inteligentes.* Edit. Mc Graw Hill. Méjico.

MONROY LOPEZ, J (2009) *Análisis inicial de la anatomía de un sistema informático* .Tesis para optar el Título de Ingeniero en Computación. Universidad Nacional Autónoma de Méjico. Méjico D.F.

MORALES GARCÍA, O. (2010) *Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas.* España: Cizur Menor

ORE CÉSPEDES, B. (2011) *La delincuencia informática y la afectación al desarrollo económico y social.* Tesis para optar el Grado de Maestro en Administración. Universidad Nacional mayor de San Marcos.

PÉREZ LUÑO, Antonio Enrique (2006) *Manual de informática y derecho.* España: Ariel.

OSORIO, Manuel (2003) *Diccionario Jurídico*. Edit. Kapeluszt. España.

RAGUÉS I VALLÉS, R. (2012) *La reforma de los delitos informáticos: incriminación de los ataques a los sistemas de información.* España: Pastor Muñoz. Madrid

SÁNCHEZ PALOMARES, Zoila (2005) *Estrategia de Seguridad Regional: Hacia una Política Exterior de Cooperación*, CID, Washington DC.

SYMANTEC (2013) *Reporte Norton, 2013*. USA.

TANENBAUM, Andres (2010) *Red de computadoras*. Edit. Pearson. España.

TELLEZ VALDES, Julio (2008) *Derecho Informático*. Mejico: McGraw-Hill.

WALL, D. (2008). *Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International*. Review of Law, Computers & Technology

YAR, M. (2006) *Cybercrime and society.* London: Sage Publications

5.2. REFERENCIAS HEMEROGRÁFICAS

DE LA COLINA, J (1999). *Una aproximación al concepto de seguridad*. Instituto de Investigación sobre Seguridad y Crimen Organizado de la Subsede Buenos Aires. Gendarmería Nacional, de la Universidad Católica de Salta. Argentina.

VANDERSCHAUREN F. (2004), *Políticas de Seguridad Ciudadana en Europa y América Latina,* División de Seguridad Ciudadana, Ministerio del Interior de Chile

5.3. PAGINAS WEB

http://www.online.upaep.mx/LPC/online/apa/APAimp.pdf

http://www.arcert.gov.ar/

http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp .

http://www.significados.com/amenaza

ANEXOS

Anexo 01 CUESTIONARIO

I. INSTRUCCIONES

A. Los resultados que se obtengan de la presente encuesta serán utilizados exclusivamente para el desarrollo de la investigación: EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL.

B. La presente encuesta será aplicada a una muestra seleccionada perteneciente a oficiales y funcionarios de la Policía Nacional del Perú, Ministerio Publico y Poder Judicial.

C. La “identidad de las personas” encuestadas, así como la “confidencialidad” de sus respuestas, queda plenamente garantizadas.

II. INFORMACIÓN BÁSICA

(Encierre con un círculo, el número que contenga su respuesta)

A. Edad
   1. De 18 a 35 años.
   2. De 36 a 50 años.
   3. Más de 50 años.

B. Sexo:
   1. Masculino.
   2. Femenino.

C. Nivel de instrucción:
   1. Secundaria.
   2. Superior.

A continuación se le presenta una serie de preguntas, Ud. deberá responder una sola alternativa y marcarla con un aspa (x) al costado de los ítems.

1. ¿Cree Ud. que existe un alto nivel alcanzado por el intrusismo informático dentro de las modalidades del cibercrimen en el país?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

2. ¿Cree Ud. que existe un alto nivel alcanzado por el sabotaje informático dentro de las modalidades del cibercrimen en el país?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

3. ¿Cree Ud. que existe un alto nivel alcanzado por los delitos informáticos dentro de la estructura del cibercrimen en el país?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

4. ¿Cree Ud. que existe un alto nivel alcanzado por la irresponsabilidad funcional de los encargados informáticos dentro de la estructura del cibercrimen en el país?

Muy de acuerdo

De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

5. ¿Cree Ud. que existe un alto nivel alcanzado por la frecuencia de ataques informáticos dentro de las técnicas del cibercrimen en el país?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

6. ¿Cree Ud. que existe un alto nivel alcanzado por la presencia de hackers dentro de las técnicas del cibercrimen en el país?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

7. ¿Cree Ud. que existe control efectivo de la estructura informática dentro de la Seguridad Nacional?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

8. ¿Cree Ud. que existe cumplimiento de los reglamentos de la estructura informática dentro de la Seguridad Nacional?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

9. ¿Cree Ud. que existe optimización del control de los programas en la protección de la data dentro de la Seguridad Nacional?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

10. ¿Cree Ud. que existe optimización de las normas legales para la protección de la data dentro de la Seguridad Nacional?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

11. ¿Cree Ud. que existe eficacia de las políticas a nivel informático en los fines de la Seguridad Nacional?

Muy de acuerdo
De acuerdo

Indefinido
En desacuerdo
Muy en desacuerdo

12. ¿Cree Ud. que existe cumplimiento de objetivos a nivel informático en los fines de la Seguridad Nacional?

Muy de acuerdo
De acuerdo
Indefinido
En desacuerdo
Muy en desacuerdo

MATRIZ DE CONSISTENCIA
TEMA: **EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL**

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	INDICADORES
PROBLEMA PRINCIPAL ¿En qué medida el Cibercrimen en el Perú afecta a la Seguridad Nacional? **PROBLEMAS ESPECÍFICOS** En qué medida las modalidades del Cibercrimen en el Perú afectan a la estructura informática de la Seguridad nacional? ¿En qué medida la estructura organizativa del Cibercrimen en el Perú afecta a la protección de la data de la Seguridad nacional? ¿En qué medida las técnicas del Cibercrimen en el Perú afectan a los fines de la Seguridad nacional?	**OBJETIVO GENERAL** Determinar en qué medida el cibercrimen en el Perú afecta la Seguridad Nacional, **OBJETIVOS ESPECÍFICOS** Establecer en qué medida las modalidades del Cibercrimen en el Perú afecta a la estructura informática de la Seguridad nacional. Determinar en qué medida la estructura organizativa del Cibercrimen en el Perú afecta a la protección de la data de la Seguridad nacional. Plantear en qué medida las técnicas del Cibercrimen en el Perú afectan a los fines de la Seguridad nacional.	**HIPOTESIS GENERAL** El nivel alcanzado por el Cibercrimen en el Perú afecta significativamente a la Seguridad nacional **HIPÓTESIS ESPECÍFICAS** El nivel alcanzado por las modalidades del Cibercrimen en el Perú afecta significativamente a la estructura informática de la Seguridad nacional El nivel alcanzado por la estructura organizativa del Cibercrimen en el Perú afecta significativamente a la protección de la data de la Seguridad nacional. El nivel alcanzado por las técnicas del Cibercrimen en el Perú afecta significativamente a los fines de la Seguridad nacional	**X :** El cibercrimen en el Perú **Y :** Seguridad Nacional	**<u>1RA HIPÓTESIS</u>** **VARIABLE (X)** Las modalidades del cibercrimen **INDICADOR** - % del intrusismo informático - % del sabotaje informático **VARIABLE (Y)** Estructura informática de la Seguridad Nacional. **INDICADOR** - % de control efectivo - % de cumplimiento de los reglamentos **<u>2DA HIPÓTESIS</u>** **VARIABLE (X)** Estructura organizativa del cibercrimen **INDICADOR** - Nº de delitos - % de responsabilidad **VARIABLE (Y)** Protección de la data de la Seguridad Nacional. **INDICADOR** - Nº de programas - Nº de normas legales

				<u>3RA HIPÓTESIS</u> **VARIABLE (X)** Técnicas del cibercrimen **INDICADOR** - Nº de tipos de ataques - % de Hackers **VARIABLE (Y)** Fines de la Seguridad Nacional **INDICADOR** - % de eficacia de las políticas - % cumplimiento de objetivos

FICHAS DE VALIDACIÓN

CENTRO DE ALTOS ESTUDIOS NACIONALES
ESCUELA DE POSGRADO
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1 APELLIDOS Y NOMBRES: OSWALDO GARCIA BEDOYA
1.2 GRADO ACADÉMICO: Doctor en Administración.
1.3 INSTITUCIÓN DONDE LABORA: UNIVERSIDAD FEDERICO VILLARREAL
1.4 TÍTULO DE LA INVESTIGACIÓN: EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL
. 1.5 AUTOR DEL INSTRUMENTO: MIRIAM CHILCON SILVA
1.6 DOCTORADO: DESARROLLO Y SEGURIDAD ESTRATEGICA.
1.7 NOMBRE DEL INSTRUMENTO: Cuestionario.
1.8 CRITERIOS DE APLICABILIDAD:

a) De 01 a 09: (No válido, reformular) **b) De 10 a 12: (No válido reformular)**
c) De 12 a 15: (Válido, mejorar) **d) De 15 a 18: (Válido, precisar)**
e) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

Indicadores de evaluación del instrumento	Criterios Cualitativos Cuantitativos	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	MB (15-18)	Excelente (18-20)
		01	02	03	04	05
1. Claridad	Está formulado con lenguaje apropiado.					18
2. Objetividad	Esta expresado con conductas observables.					18
3. Actualidad	Adecuado al avance de la ciencia y tecnología.					19
4. Organización	Existe una organización y lógica.					19
5. Suficiencia	Comprende los aspectos en cantidad y calidad.					18
6. Intencionalidad	Adecuado para valorar los aspectos de estudio.					18
7. Consistencia	Basado en el aspecto teórico científico y del tema de estudio.					18
8. Coherencia	Entre las variables, dimensiones y variables.					18
9. Metodología	La estrategia responde al propósito de estudio.					18
10. Conveniencia	Genera nuevas pautas para la investigación y construcción de teorías.					18
	Sub total					182
	Total					18.20

Valoración cuantitativa: Dieciocho y veinte.
Valoración cualitativa: Excelente.
Opinión de aplicabilidad: El instrumento es válido y se puede aplicar.
Lugar y fecha: Lima 15 de octubre del 2017.

Firma y Postfirma del experto

DNI: 10001151

CENTRO DE ALTOS ESTUDIOS NACIONALES
ESCUELA DE POSGRADO
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1 APELLIDOS Y NOMBRES: JOSE TOLEDO VALDIVIA
1.2 GRADO ACADÉMICO: Doctor en Administración.
1.3 INSTITUCIÓN DONDE LABORA: CONGRESO DE LA REPUBLICA
1.4 TÍTULO DE LA INVESTIGACIÓN: EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL
. 1.5 AUTOR DEL INSTRUMENTO: MIRIAM CHILCON SILVA
1.6. DOCTORADO: DESARROLLO Y SEGURIDAD ESTRATEGICA
1.7 NOMBRE DEL INSTRUMENTO: Cuestionario.

1.8 CRITERIOS DE APLICABILIDAD:

a) De 01 a 09: (No válido, reformular) **b) De 10 a 12: (No válido reformular)**

c) De 12 a 15: (Válido, mejorar) **d) De 15 a 18: (Válido, precisar)**

e) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

Indicadores de evaluación del instrumento	Criterios Cualitativos Cuantitativos	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	MB (15-18)	Excelente (18-20)
		01	02	03	04	05
11. Claridad	Está formulado con lenguaje apropiado.					18
12. Objetividad	Esta expresado con conductas observables.					18
13. Actualidad	Adecuado al avance de la ciencia y tecnología.					18
14. Organización	Existe una organización y lógica.					18
15. Suficiencia	Comprende los aspectos en cantidad y calidad.					18
16. Intencionalidad	Adecuado para valorar los aspectos de estudio.					18
17. Consistencia	Basado en el aspecto teórico científico y del tema de estudio.					18
18. Coherencia	Entre las variables, dimensiones y variables.					18
19. Metodología	La estrategia responde al propósito de estudio.					18
20. Conveniencia	Genera nuevas pautas para la investigación y construcción de teorías.					18
Sub total						180
Total						18.00

Valoración cuantitativa: Dieciocho.
Valoración cualitativa: Excelente.
Opinión de aplicabilidad: El instrumento es válido y se puede aplicar.
Lugar y fecha: Lima 15 de octubre del 2017.

Firma y Postfirma del experto

DNI: 43347165

CENTRO DE ALTOS ESTUDIOS NACIONALES
ESCUELA DE POSGRADO
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1 APELLIDOS Y NOMBRES: EDWIN CRUZ ASPAJO
1.2 GRADO ACADÉMICO: Doctor en Administración .
1.3 INSTITUCIÓN DONDE LABORA: CAEN
1.4 TÍTULO DE LA INVESTIGACIÓN: EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL
. 1.5 AUTOR DEL INSTRUMENTO: MIRIAM CHILCON SILVA
1.6.DOCTORADO: DESARROLLO Y SEGURIDAD ESTRATEGICA
1.7 NOMBRE DEL INSTRUMENTO: Cuestionario.
1.8 CRITERIOS DE APLICABILIDAD:

a) De 01 a 09: (No válido, reformular) **b) De 10 a 12: (No válido reformular)**

c) De 12 a 15: (Válido, mejorar) **d) De 15 a 18: (Válido, precisar)**

e) De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR:

Indicadores de evaluación del instrumento	Criterios Cualitativos Cuantitativos	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	MB (15-18)	Excelente (18-20)
		01	02	03	04	05
21. Claridad	Está formulado con lenguaje apropiado.					19
22. Objetividad	Esta expresado con conductas observables.					19
23. Actualidad	Adecuado al avance de la ciencia y tecnología.					20
24. Organización	Existe una organización y lógica.					19
25. Suficiencia	Comprende los aspectos en cantidad y calidad.					19
26. Intencionalidad	Adecuado para valorar los aspectos de estudio.					19
27. Consistencia	Basado en el aspecto teórico científico y del tema de estudio.					19
28. Coherencia	Entre las variables, dimensiones y variables.					19
29. Metodología	La estrategia responde al propósito de estudio.					19
30. Conveniencia	Genera nuevas pautas para la investigación y construcción de teorías.					19
Sub total						191
Total						19.10

Valoración cuantitativa: Diecinueve y diez.
Valoración cualitativa: Excelente.
Opinión de aplicabilidad: El instrumento es válido y se puede aplicar.
Lugar y fecha: Lima 15 de octubre del 2017.

Firma y Postfirma del experto

DNI: 43750935