**UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA**

**FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN**

**DESARROLLO DE ALGORITMO DE CIFRADO PERSONALIZADO, PARA LA POLICIA NACIONAL CIVIL DE GUATEMALA.**

**HÉCTOR ROLANDO SUNÚN RAYMUNDO**

**JUTIAPA 2020**

**UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA**

**FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN**

**DESARROLLO DE ALGORITMO DE CIFRADO PERSONALIZADO, PARA LA POLICIA NACIONAL CIVIL DE GUATEMALA.**

**HECTOR ROLANDO SUNUN RAYMUNDO**

**JUTIAPA 2020**

**Introducción**

**Desde la época primitiva la humanidad ha sentido la necesidad de privacidad, tratando de evitar que la información llegue a terceros, vemos la criptografía en dos fases importantes la era clásica y la era moderna ya con el uso de computadores. A medida que va incrementando el intercambio de información por Internet surge la necesidad de proteger dicha información, en este trabajo se presenta una reseña histórica y evolución de los diferentes tipos de cifrados cómo Simétricos, Asimétricos e Híbridos así cómo una buena cantidad de algoritmos, los cuales han sido desafiados debido al incremento del poder computacional, por lo tanto la necesidad de desarrollar nuevos algoritmos para seguir reforzando la protección de datos, el cual será una tarea constante.**

**En principio la criptografía utilizada especialmente por gobiernos y militares, pero en la actualidad es un tema general, ya involucradas personas individuales así cómo distintas corporaciones. Ya no basta con cifrar información almacenada en algún disco duro sino la información que se transporta por Internet.**

Índice

[**CAPITULO I** 2](#_Toc46045429)

[**MARCO CONCEPTUAL** 2](#_Toc46045430)

[1.1 Antecedentes 2](#_Toc46045431)

[1.2 Justificación 5](#_Toc46045432)

[1.3 Planteamiento del Problema 6](#_Toc46045433)

[**1.3.1 Descripción del Problema** 6](#_Toc46045434)

[**1.3.2 Formulación del Problema** 6](#_Toc46045435)

[1.4 Preguntas de Investigación 6](#_Toc46045436)

[1.5 Objetivos de la investigación 7](#_Toc46045437)

[**1.5.1 Objetivo general** 7](#_Toc46045438)

[**1.5.2 Objetivos específicos** 7](#_Toc46045439)

[1.6 Alcances y limitaciones 8](#_Toc46045440)

[**1.6.1 Alcances** 8](#_Toc46045441)

[**1.6.2 Límites** 8](#_Toc46045442)

[**1.6.3 Aspectos demográficos** 8](#_Toc46045443)

[**1.6.4 Datos de la Institución** 8](#_Toc46045444)

[1.7 Hipótesis 8](#_Toc46045445)

[1.8 Definición Conceptual de Variables 8](#_Toc46045446)

[**1.8.1 Variables independientes** 8](#_Toc46045447)

[**1.8.2 Variables dependientes** 9](#_Toc46045448)

[1.9 Tipo de Investigación 10](#_Toc46045449)

[1.10 Métodos y técnicas de investigación. 10](#_Toc46045450)

[**1.10.1 Método científico** 10](#_Toc46045451)

[**1.10.2 Método inductivo** 10](#_Toc46045452)

[**1.10.3 Metodologías de desarrollo de software** 10](#_Toc46045453)

[1.11 Instrumento de Recolección de datos. 10](#_Toc46045454)

[**1.11.1 Objetivo del instrumento** 10](#_Toc46045455)

[**1.11.2 Población estadística** 10](#_Toc46045456)

[**1.11.3 Muestra** 10](#_Toc46045457)

[**1.11.4 Resultados de la encuesta** 10](#_Toc46045458)

**Índice de Figuras**

[Figura 1.Escítala con la cinta y el mensaje escrito. 2](file:///C:\Users\HRray1\Desktop\3ra%20entrega.docx#_Toc43194689)

[Figura 2. Cifrado por sustitución, Polybios. 2](file:///C:\Users\HRray1\Desktop\3ra%20entrega.docx#_Toc43194690)

[Figura 3. César con movimiento de 4 posiciones. 3](file:///C:\Users\HRray1\Desktop\3ra%20entrega.docx#_Toc43194691)

[Figura 4. Funcionamiento de máquina Enigma 3](file:///C:\Users\HRray1\Desktop\3ra%20entrega.docx#_Toc43194692)

Figura 5. Ubicación Mapa de Google. (Elaboración Propia) 14 Figura 6. Elaboración propia (Héctor Rolando Sunún Raymundo) Microsoft Word.2020 18 Figura 6. Evaluación de Unidades (Héctor Rolando Sunún Raymundo). 19 Figura 7. Áreas de Trabajo (Héctor Rolando Sunún Raymundo). 20 Figura 8. Protección de datos (Héctor Rolando Sunún Raymundo). 21 Figura 9. Envío de Información (Héctor Rolando Sunún Raymundo). 22 Figura 10. Protección de Datos Institucional (Héctor Rolando Sunún Raymundo). 22 Figura 11. Confidencialidad de información (Héctor Rolando Sunún Raymundo). 23 Figura 12. Herramienta para Cifrado (Héctor Rolando Sunún Raymundo). 23 Figura 13. Mejora de seguridad de Información (Héctor Rolando Sunún Raymundo). 24 Figura 14. Datos Personales (Héctor Rolando Sunún Raymundo). 25 Figura 15. Conocimiento de Cifrado de Información (Héctor Rolando Sunún Raymundo). 25 Figura 16. Combate de vulnerabilidades (Héctor Rolando Sunún Raymundo). 26

**Índice de Tablas**

[Tabla 1. Viabilidad Técnica 7](#_Toc43201644)

[Tabla 2. Viabilidad Económica (Recursos Humanos) 7](#_Toc43201645)

[Tabla 3. Viabilidad Económica (Recursos Tecnológicos) 8](#_Toc43201646)

[Tabla 4. Viabilidad Económica (Recursos Materiales) 8](#_Toc43201647)

[Tabla 5. Viabilidad Económica (Totales) 9](#_Toc43201648)

[Tabla 6. Variable Independiente 12](#_Toc43201649)

[Tabla 7. Variable dependiente 13](#_Toc43201650)

**DESARROLLO DE ALGORITMO DE CIFRADO PERSONALIZADO.**

# **CAPITULO I**

# **MARCO CONCEPTUAL**

En este marco se presenta el punto de partida sobre la necesidad de nuestra privacidad, es un tema que ha existido desde mucho tiempo atrás incluso antes de la era informática, en el que se cifraba letras, caracteres. En la era moderna ya se ve involucrada la computación, es esta ya se trabaja sobre bits y bytes, pero siempre con el mismo objetivo de resguardar la información. Se da conocer parte de la historia, evolución, los algoritmos que han existido y los tipos de cifrados de la actualidad, la argumentación del porqué darle importancia al cifrado de nuestros datos, **a nivel de usuarios individuales, así como distintas corporaciones. Y finalmente el objetivo de crear o diseñar un nuevo algoritmo de cifrado.**

## 1.1 Antecedentes

**Historia de la Criptografía**

**Es importante conocer el origen etimológico de la palabra, según DMATIC Departamento de Matemática Aplicada a las Tecnologías de la Información y Comunicaciones “La palabra Criptografía proviene del griego “Kryptos” que significa oculto, y “graphia”, que significa escritura, y su definición según el diccionario es “Arte de escribir con clave secreta o de un modo enigmático”.**

**El tema de la criptografía proviene desde hace miles de años, el deseo innato de los seres humanos de privacidad, de ocultar o resguardar información de los demás. Desde los primeros estados entre ellos Egipto, Babilonia, Roma, especialmente utilizados en el ámbito militar y por los gobernantes.**

**Primeros métodos criptográficos**

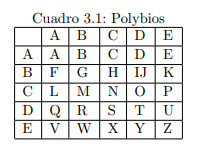
**Hacia los años 400 a.c se usó un método denominado Escitala, por los espartanos la cual fue por Transposición, escondía el verdadero significado de determinado texto, cambiando la ubicación de los signos, en el caso de los militares griegos, redactaban sus escritos en una tela, que se envolvía sobre una vara al que le llamaban Escítala. Se mandaba la cinta a la persona que recibía el mensaje, tanto el emisor cómo el receptor debía tener varas iguales, para poder leer el mensaje. Fue una forma sencilla similar al cifrado de César, en este caso fue de sustitución. Se reemplazaba cada letra por la que se encontraba tres puestos posteriormente.**



Copyright 2016 por Javier Martínez De La Torre

**Figura 1**.Escítala con la cinta y el mensaje escrito.

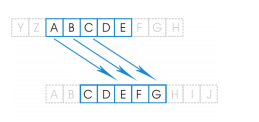
**Polybios**

**Esto se dio en el siglo II a.c en Grecia Por un historiador Polybios, quien creó un sistema de cifrado en el que se reemplazaba un carácter por otro, dicho carácter se encontraba en una tabla ya construida.**

Copyright 2016 por Javier Martínez De La Torre

**Figura 2.** Cifrado por sustitución, Polybios.

**César**

**También fue a.C. dado en Roma, este cifrado de César consistía en reemplazar una letra por la letra que se encontraba tres posiciones a la derecha.**

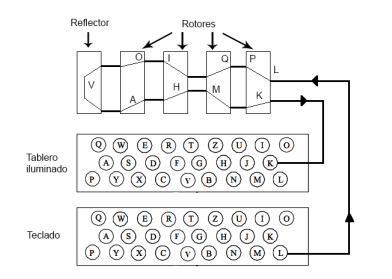
Copyright 2016 por Javier Martínez De La Torre

**Figura 3.** César con movimiento de 4 posiciones.

**Cifrados polialfabéticos**

**León Battista Alberti en el año 1466, inventó el cifrado por sustitución, consistía en varios abecedarios que se encontraban en un círculo.** Tanto quien enviaba cómo el que recibía el mensaje, establecía una posición de los círculos para crear palabras.

**La máquina Enigma**

Fue creado a inicios del siglo XX, posterior a las ruedas de León Battista, en esa época se inventaron los teletipos (se refiere a unos aparatos telegráficos que tienen un teclado, que envía y recibe mensajes y los imprime). Estas máquinas tenían una secuencia de rotores, lo que permitía que giraran al pulsar una tecla, si se le compara con una máquina de escribir, a cada golpe de una letra mostraba otra letra, que era elegida según las letras de la máquina. Un claro ejemplo es el de la máquina Enigma, inventada por Arthur Scherbius de Alemania, utilizada por los Nazis, era una máquina de rotor capaz de cifrar información, el cual fue descifrado.

Copyright 2016 por Javier Martínez De La Torre

**Figura 4.** Funcionamiento de máquina Enigma.

**El inicio del computador**

Alan Turín creó una máquina considerada el primer computador, que descifró la máquina Enigma. Con la creación de esta máquina se logró el análisis de miles de combinaciones de Enigma.

**Criptografía en la era moderna**

**Con la automatización se inició con sistemas o métodos de mayor complejidad para cifrar información. Muchas veces se considera que la encriptación es algo que involucra únicamente a grandes corporaciones, gobernantes o militares, pero si se aterriza, se comprende que para un cajero automático por ejemplo al ingresar la clave de una tarjeta de débito o crédito, en realidad se está enviando una información cifrada que sólo el banco y el usuario debería leer.**

**Otro claro ejemplo es el de los correos electrónicos, cada vez que un usuario envía un mensaje debería ver la información únicamente el receptor.**

## ****1.2 Justificación****

**Debido al incremento del poder computacional aplicar fuerza bruta a sistemas de cifrado con altos valores es cada día más viable elevar las tasas de prueba.**

**La ley de Moore predice la tendencia computacional, indicando que el poder se duplica cada 18 meses con una tendencia de reducción o mantención de costos. En el mundo de la criptografía al darse 10 iteraciones (período de 15 años) se pueden hacer = 1024 veces más cálculos computaciones con el mismo costo que en la actualidad. Por lo que surge la necesidad de mejorar o implementar algoritmos de cifrado.**

Es importante seguir creando nuevos algoritmos de cifrados para seguir ampliando posibilidades de protección de datos y seguir combatiendo las amenazas.

## ****1.3 Planteamiento del Problema****

### **1.3.1 Descripción del Problema**

**En el mundo de la informática, el cifrado de datos ha sido un elemento fundamental de la seguridad de datos, es una manera importante de impedir que alguien robe o lea información de un sistema informático con fines malintencionados, a nivel de usuarios individuales, así como distintas corporaciones. Sin embargo, en estos últimos años ha habido un crecimiento de usuarios de Internet en el mundo de un 7% a comparación del año 2019, y alcanza los 4.540 millones aproximadamente en este año 2020. Y en promedio, estos usuarios de internet pasan 6 horas 43 minutos conectados cada día. Indiscutiblemente la privacidad de los mismos está en la mira.**

**Dentro de las amenazas de información van desde códigos maliciosos, o la explotación de vulnerabilidades, hasta el robo de dispositivos móviles. El manejo adecuado de la información es fundamental a la hora de sufrir algún incidente.**

**Debido al aumento de intercambio de información, surge la necesidad de buscar una manera segura de comunicación, es por ello la existencia de distintos sistemas de cifrado.**

### **1.3.2 Formulación del Problema**

La privacidad es un tema importante, por ende, es necesario proteger los datos, desde la entidad hasta evitar la clonación de tarjetas de débito, crédito. Los algoritmos actuales enfrentan grandes desafíos ya que cada día la capacidad computacional aumenta y eso facilita el descifrado de mensajes.

Dentro los tipos de algoritmos existen el cifrado simétrico el cual presenta ciertas debilidades de seguridad, por lo que es necesario buscar algoritmos aptos de acorde a la realidad.

¿Es posible desarrollar un nuevo algoritmo de cifrado que supere la deficiencia de los algoritmos actuales?

## ****1.4 Preguntas de Investigación****

**¿Cuáles son las ventajas y desventajas de la criptografía simétrica**?

¿Actualmente, en los datos que se envían en línea, pueden ser mal utilizados con fines delictivos y perjudicar gravemente a una empresa y a sus usuarios?

¿Es común utilizar herramientas para el cifrado que admite protección de datos de smartphones, emails, navegadores, discos duros e información en la nube?

¿El cifrado de información cuando se navega por internet es una función importante para proteger cualquier actividad o información que se intercambia o los datos que se publican?

¿Es esencial practicar el uso algoritmos de cifrado para cuando se envíe información y proteger dicha información privada?

¿Es necesario usar Internet para obtener los beneficios del cifrado?

¿El cifrado se usa solo cuando los datos están “en tránsito” (envío de información a través de Internet, Correo electrónico) o cuando están en “Proceso” (cuando se encuentran almacenados en un dispositivo, ¿disco rígido o un medio extraíble)?

## ****1.5 Objetivos de la investigación****

### **1.5.1 Objetivo general**

**Desarrollar e implementar un algoritmo de cifrado personalizado.**

### **1.5.2 Objetivos específicos**

1. **Conocer los diferentes tipos de cifrados de la actualidad.**
2. **Estudiar y analizar el funcionamiento de los tipos de cifrado, así como las vulnerabilidades, ventajas y desventajas de cada uno.**
3. **Desarrollar un nuevo algoritmo simétrico para cifrar los datos.**
4. **Realizar pruebas del nuevo algoritmo, para su posterior implementación.**

## ****1.6 Alcances y limitaciones****

En esta fase se describe el logro que se obtendrá por medio del desarrollo de un nuevo algoritmo de cifrado de información así mismo de los límites que se tendrán.

### **1.6.1 Alcances**

**a) El presente estudio explorará los distintos tipos de cifrados actuales y el uso que cada uno tiene. Abarcará tanto a las personas individuales cómo a las corporaciones que los utilizan, las vulnerabilidades, para posteriormente diseñar un nuevo algoritmo.**

**b) La implementación del algoritmo se realizará con el lenguaje de programación Java, así mismo se realizará el algoritmo en Pseudocódigo para poder utilizarlo en cualquier lenguaje de programación.**

### **1.6.2 Límites**

**a) La falta de cultura de seguridad,** privacidad y uso de cifrado de parte de los agentes de Policía Nacional Civil, al momento de implementar el nuevo algoritmo.

b) En la Universidad Mariano Gálvez de Guatemala no hay un criptoanalista.

### **1.6.3 Aspectos demográficos**

Colindancia: El territorio guatemalteco en sus limitaciones territoriales en el lado norte y Oeste con México, el Mar Caribe y Honduras, al Sureste con El Salvador, lado sur con el Océano Pacífico.

Extensión: cuenta con una extensión territorial de 108,890 km2.

### **1.6.4 Datos de la Institución**

Nombre: Policía Nacional Civil de Guatemala.

Dirección: Cuenta con una Academia, ubicada en 15A Calle Col Cipresales 16-00 Z.6. Guatemala, con coordenadas 14.656235 -90.493672. Tiene 6 jefaturas, 27 comisarías a nivel nacional, 6 en la capital y una por departamento. 127 Estaciones y 343 Subestaciones. Tiene 2 Direcciones y 10 subdirecciones. Como se describe a continuación.

1. Dirección General
2. Dirección General Adjunta
3. Subdirecciones
4. Subdirección General de Operaciones
5. Subdirección General de Investigación Criminal
6. Subdirección General de Personal
7. Subdirección General de Apoyo y Logística
8. Subdirección General de Análisis de Información Antinarcótica
9. Subdirección General de Estudios y Doctrina
10. Subdirección General de Prevención del Delito



## 

Figura 5. Ubicación Mapa de Google. (Elaboración Propia)

## 1.7 Hipótesis

Con el desarrollo e implementación de un nuevo algoritmo criptográfico simétrico, tomando cómo base el algoritmo AES (Advanced Encryption Standard), brindará mayor seguridad al momento de cifrar datos o información también ofrece una mayor independencia matemática. Así mismo promoverá la importancia de la criptografía.

Ho: Tomando cómo base el algoritmo AES (Advanced Encryption Standard) no brindará mayor seguridad al momento de cifrar datos o información tampoco ofrece una mayor independencia matemática.

Ha: Con el cifrado de Información basado en el algoritmo AES (Advanced Encryption Standard) se fortalecerá la seguridad de información en las secciones que manejan datos más sensibles dentro de la institución policial.

## 1.8 Definición Conceptual de Variables

### **1.8.1 Variables independientes**

En el caso de este algoritmo de cifrado, será para contribuir con los algoritmos ya existentes, manteniendo la firme convicción de buscar siempre la protección de los datos y que terceros no accedan a la misma.

**Tabla 6.**

Variable Independiente

|  |  |  |
| --- | --- | --- |
| **Variable** | **Dimensiones** | **Indicadores** |
| Desarrollo de Algoritmo de encriptación, basado en el algoritmo Estándar de Encriptación Avanzada AES | Conjunto de Cadenas de entrada.  Conversión de texto sin cifrar a binario. | Cantidad posible de salidas de la función. |
| Cifrado de la información. |

Fuente: Capitulo II, Variable independiente. Elaboración propia (Héctor Rolando Sunún Raymundo) Microsoft Word.2020

### **1.8.2 Variables dependientes**

Para el cifrado moderno, al querer acceder a la información será utilizando la fuerza bruta.

**Tabla 7.**

Variable dependiente

|  |  |  |
| --- | --- | --- |
| **Variable** | **Dimensiones** | **Indicadores** |
| Diseño del nuevo algoritmo, para que los datos sean más aleatorios. | Conjunto de Cadenas de entrada. | Cantidad posible de salidas de la nueva función. |
| Análisis de las funciones del nuevo algoritmo. | Conjunto de Cadenas de entrada. | Cantidad posible de salidas de la función. |

Fuente: Capitulo II, Variable independiente. Elaboración propia (Héctor Rolando Sunún Raymundo) Microsoft Word.2020

## 1.9 Tipo de Investigación

Esta investigación según el nivel o alcance de la investigación es descriptivo porque se describen los distintos algoritmos de encriptación y especialmente el AES( Advanced Encryption Standard), el cual es una buena base para el desarrollo de un nuevo algoritmo.

También según el nivel o alcance, esta investigación es de tipo correlacional, porque pretende dar a conocer las características o propiedades importantes. Se analizan los algoritmos de cifrado, para conocer cada uno su nivel de seguridad,

Según la tendencia es de tipo cualitativo porque se describe, explora y explica la evolución de la criptografía desde la era clásica hasta la era moderna con la presencia de los ordenadores. Así como los tipos de cifrados.

## 1.10 Métodos y técnicas de investigación.

### **1.10.1 Método científico**

Según la Khan Academy (Marzo 2016) el método científico se usa en todas la ciencias, tales cómo la química, física, geología y psicología. Los científicos en esos campos hacen diferentes preguntas y realizan distintas pruebas, sin embargo, usan el mismo método para encontrar respuestas lógicas y respaldadas con evidencia.

Se utilizó este método porque primero se realizó una observación de la problemática actual de la seguridad de datos, por ser una institución encargada de la seguridad de la ciudadanía, planteando preguntas, formulando una hipótesis o explicación de algo que pueda ser probable, haciendo predicciones para posteriormente poner a prueba esas predicciones.

### **1.10.2 Método inductivo**

Gabriela González (2020)en la página lifeder el método inductivo es una forma de razonamiento para llegar a conclusiones que empieza desde lo más específico y va hasta las generalizaciones y teorías más amplias. Se comienza con unas observaciones y medidas específicas para llegar a unas conclusiones generales.

También refiere que este método consiste en tres etapas: observación, captar/observar un patrón y desarrollar una teoría.

Se utiliza este método porque basados en algunas delegaciones de la unidad antinarcótica, cómo en otras unidades de la institución policial que requieren de mayor seguridad de datos, se tiene el mismo patrón o tendencia, por lo que se considera que es necesario buscar métodos o estrategias para seguir mejorando la protección de la información especialmente de información sensible.

### **1.10.3 Metodologías de desarrollo de software**

## Dentro de las metodologías se eligió una metodología ágil, ya que representa mejor calidad y una reducción tanto en tiempo como en costo.

La metodología Scrum es incremental, se va realizando en pequeñas partes, dividiendo en varias etapas como análisis, desarrollo y testing (pruebas). En el proceso de desarrollo se dan lo que se denomina iteraciones de proceso o Sprint, que son entregas parciales del producto final.

## 1.11 Instrumento de Recolección de datos.

Se utilizará la aplicación de Google Forms, para la realización de encuestas a personal de la Policía Nacional Civil, tanto al personal operativo como administrativo, ya que independientemente del área en el que se desempeñan, interactúan todo tipo de información.

### **1.11.1 Objetivo del instrumento**

Determinar por medio de una encuesta respuestas que posteriormente se puedan analizar y tomar decisiones, esta encuesta se realizará de manera online, debido a la situación actual del Covid-19 enviando un enlace vía correo electrónico, en un sitio web a los participantes.

### **1.11.2 Población estadística**

La Policía Nacional Civil es una institución jerarquizada, cuenta con personal operativo, administrativo, así como diferentes funciones, cuenta con 33,000 personas activas, dentro de los cuales tienen distintos grados jerárquicos, se tomará un porcentaje de la población para la muestra, que servirá para el análisis respectivo.

### **1.11.3 Muestra**

La unidad de análisis será todo el personal policial, para la desviación estándar se utilizará un 50% de heterogeneidad, es decir la diversidad del universo. Un margen de error de 5% y un nivel de confianza del 95%, por lo que el tamaño de muestra necesaria es de 380.

Interpretación

Si se encuesta a 380 personas, el 95% de las veces el dato que se quiere medir estará en el intervalo de ±5% respecto al dato que se observe en las encuestas.

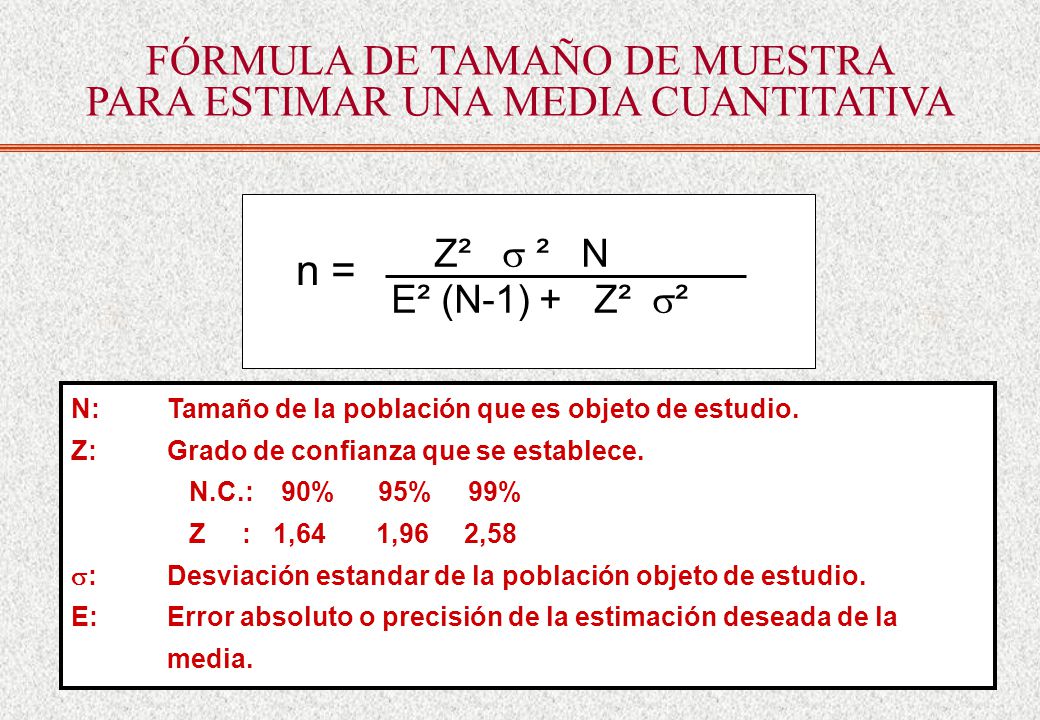


Figura 6. Elaboración propia (Héctor Rolando Sunún Raymundo) Microsoft Word.2020

En donde:

**n** = es el tamaño de la muestra poblacional a obtener.

**N** = Tamaño de la población que es objeto de estudio (33,000).

**σ** = Desviación estándar de la población objeto de estudio (0.5). Es la diversidad del universo.

**Z** = Grado de confianza. Para este caso se utilizará un 95% (equivale a 2.8)

**E** = Error absoluto o precisión de la estimación deseada de la media (0.05)

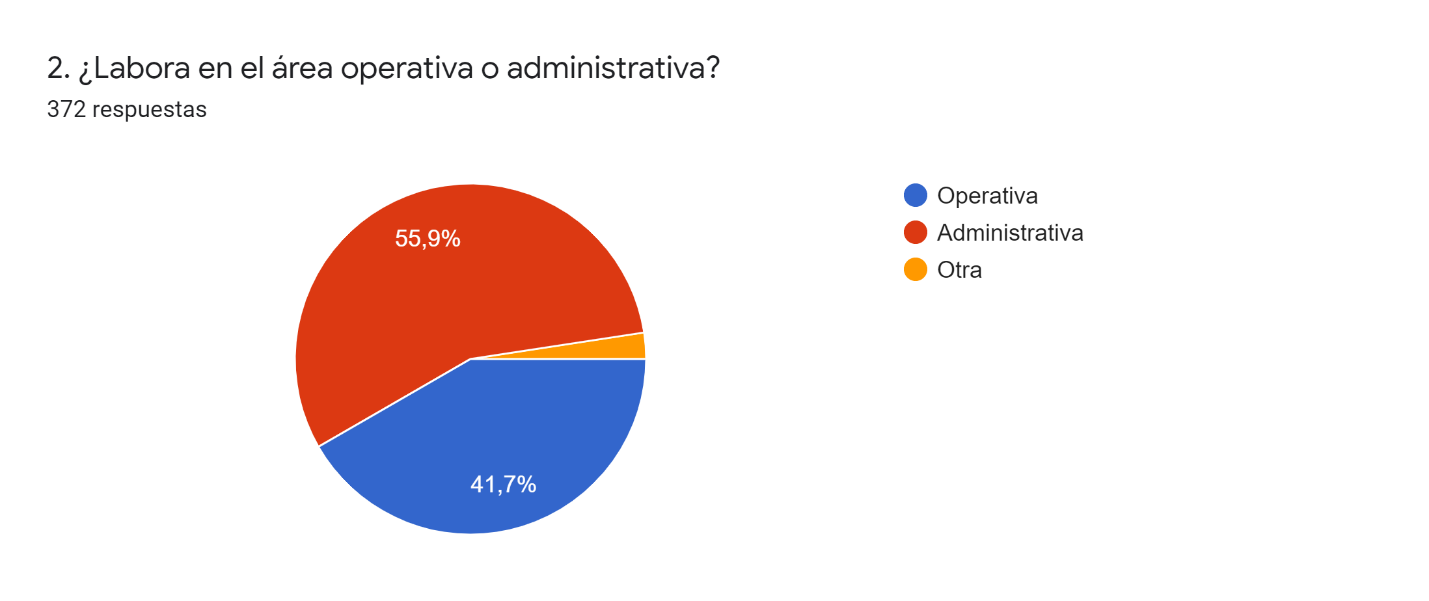
**1.11.4 Resultados de la encuesta**

Se muestran los resultados de la encuesta realizada a 383 elementos de la Policía Nacional Civil, dentro de los cuales hubo agentes y oficiales superiores, así como del área operativa y administrativa.

Figura 6. Evaluación de Unidades (Héctor Rolando Sunún Raymundo).

Debido a la existencia de distintas unidades dentro de la Policía Nacional Civil, se optó por realizar encuestas a las distintas comisarías (comisarías 12, 13, 14, 15, de la ciudad capital, comisarías 21, 31, 32, 33, 34, 41, 51, 52, 53, 62, 72, 74 de departamentos). Unidades Especializadas cómo SGAIA(Subdirección General de Análisis de Información Antinarcótica), SGDP (Subdirección General de Personal), DISETUR (División de Seguridad Turística), DIPAFRONT (División de Puertos, Aeropuertos y Puestos Fronterizos), DIP (Departamento de Investigación Policial), DIDAE (División de Investigación y Desactivación de Armas y Explosivos), DIFEP (División de Fuerzas Especiales), Academia de PNC, Departamento de Tránsito y DEIC (División Especializada en Investigación Criminal.

Esta gráfica representa la inclusión de cierto porcentaje de cada unidad para determinar la situación actual en a la seguridad de información y la disposición que los mismos tienen para mejorar la cultura de protección de datos.

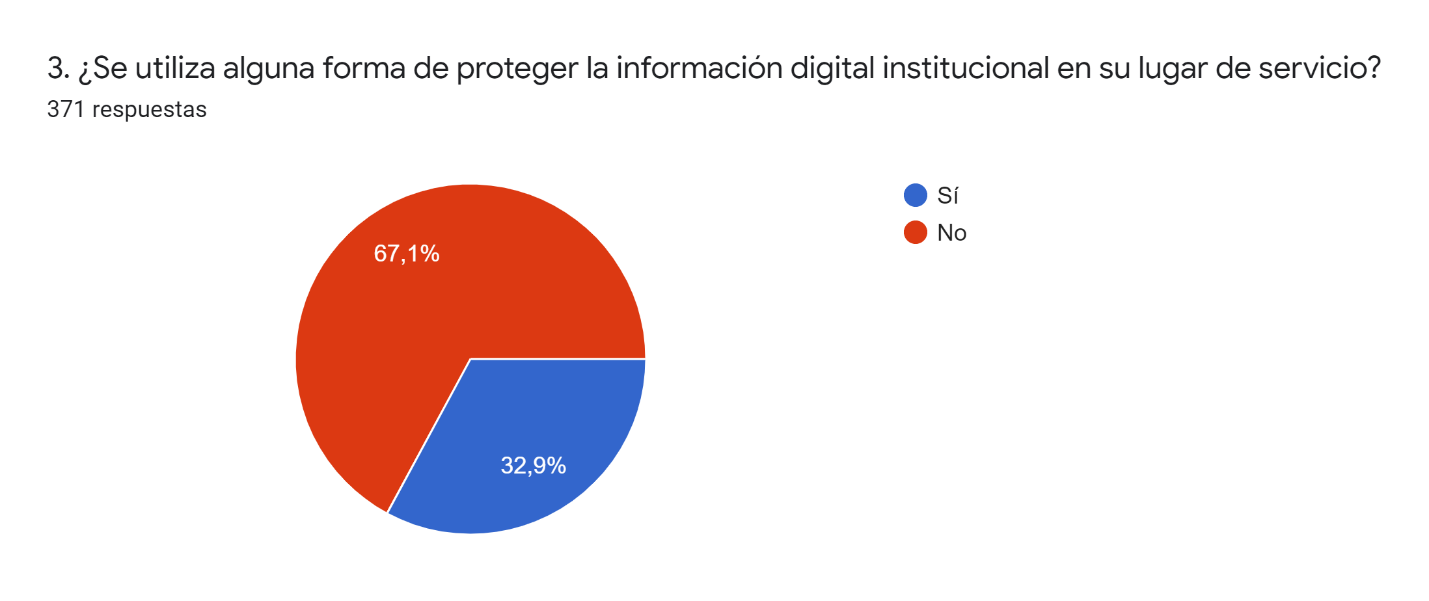


383 respuestas

Figura 7. Áreas de Trabajo (Héctor Rolando Sunún Raymundo).

El 55.9% de la población encuestada se encuentra desempeñando funciones administrativas, y el 41.7% funciones operativas y el 2.4% en otras áreas.

Esta gráfica representa al personal que labora tanto en el área operativa, administrativa entre otras funciones, se maneja información en todos los niveles, pero cabe resaltar que en el área administrativa es donde se concentra la mayor parte de información. Se optó por encuestar a nivel general porque cómo se mencionó con anterioridad, que la información fluye en todos los niveles, y por lo tanto debe fortalecerse la protección de datos desde el eslabón más bajo que sería el usuario final.

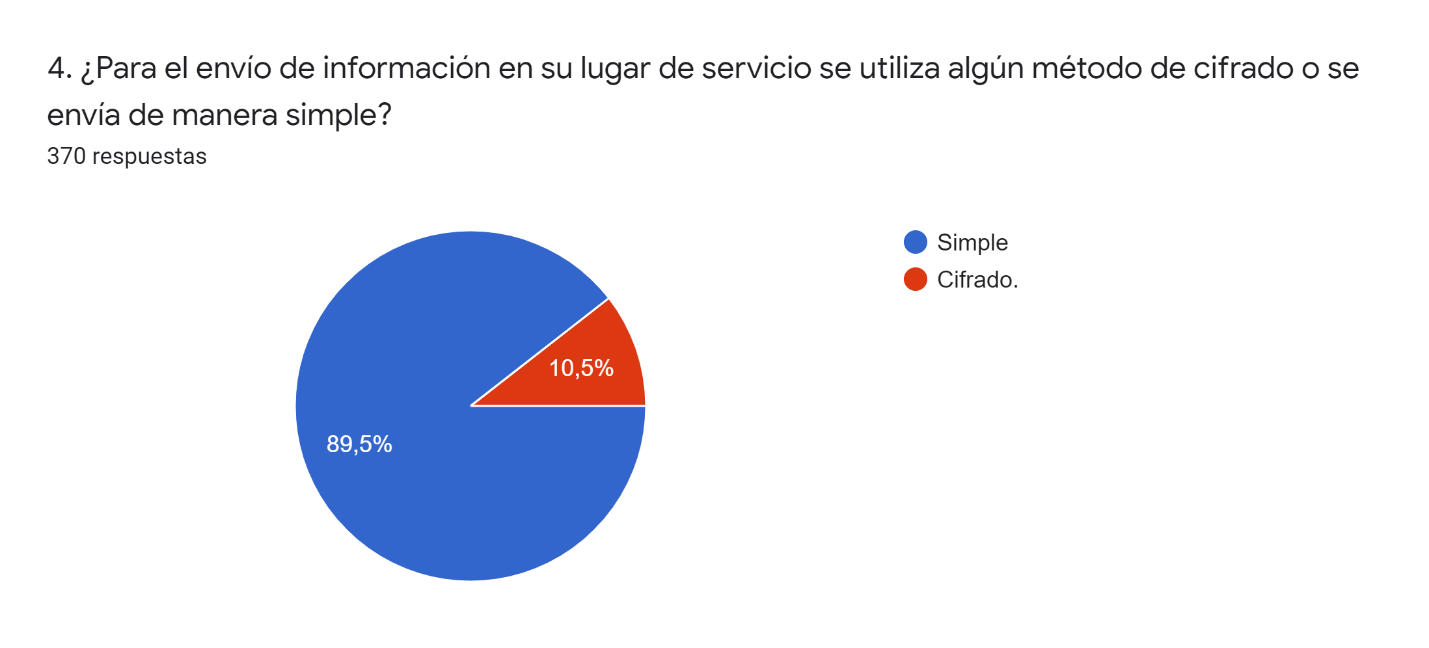


383 respuestas

Figura 8. Protección de datos (Héctor Rolando Sunún Raymundo).

El 67.1% indicó que no tenían una manera de proteger la información en el lugar donde se encuentran actualmente, comisaría, unidades especializadas u otro destino, el 32.9 % refirió que sí utiliza algún método de protección de datos.

En base a los resultados obtenidos se puede determinar que sí existe una parte de la población que tiene métodos de protección de datos pero que no existe una estandarización a nivel nacional.

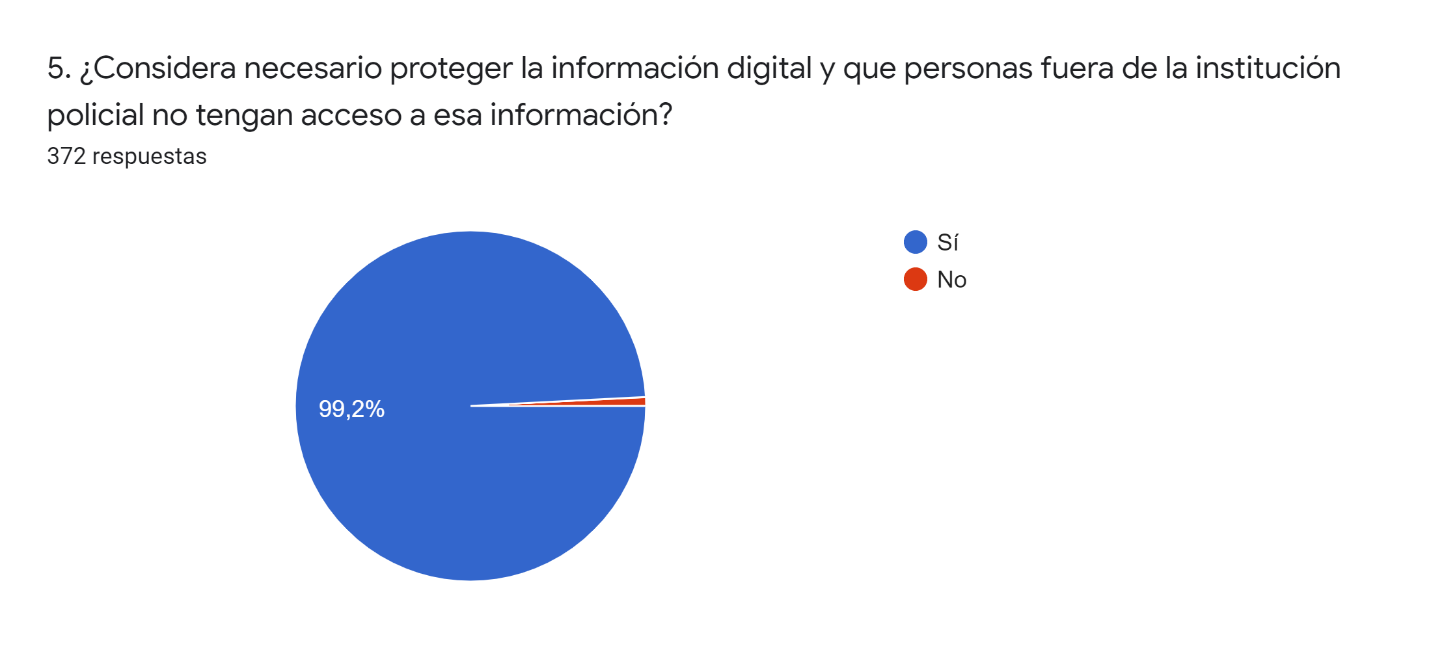


383 respuestas

Figura 9. Envío de Información (Héctor Rolando Sunún Raymundo).

El 89.5% indicó que no utilizan algún método para cifrar información durante el envío de información y el 10.5% indicó que sí utilizan algún método.

Actualmente existen correos electrónicos institucionales .gob con Outlook el cual ofrece cifrado de mensajes de correo automáticamente pero que no ha alcanzado a todas la unidades existentes dentro de la institución Policial.

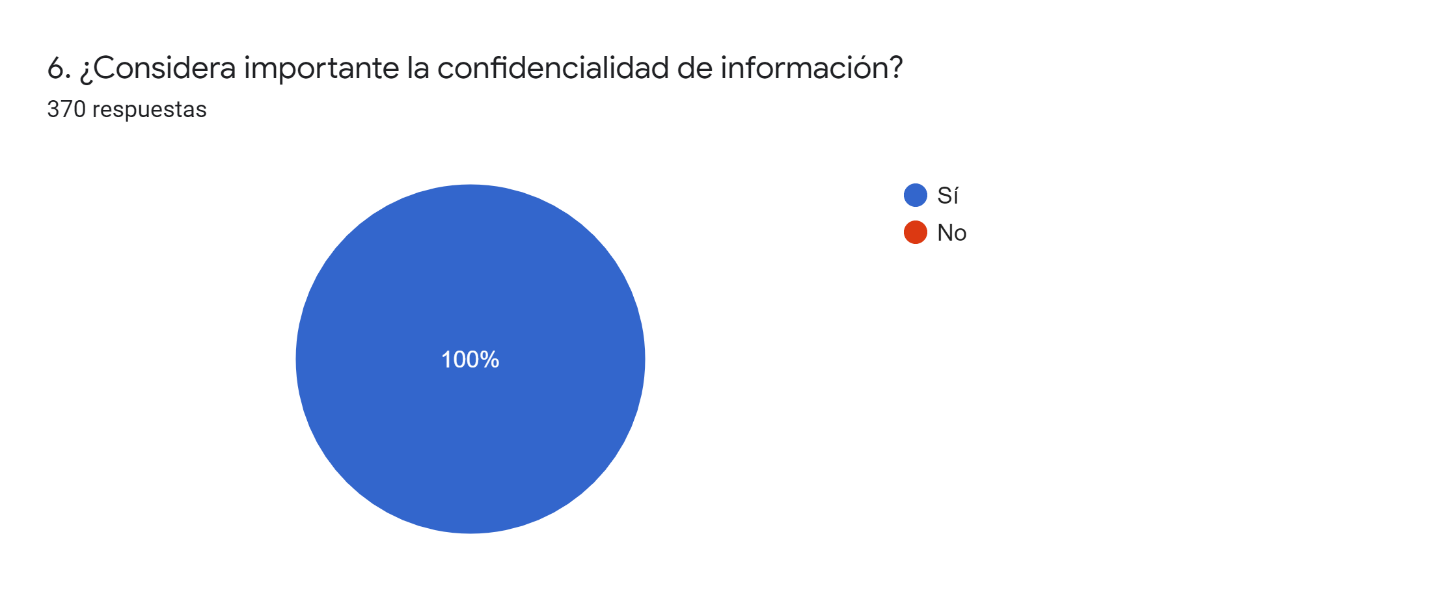


383 respuestas

Figura 10. Protección de Datos Institucional (Héctor Rolando Sunún Raymundo).

El 99.2% del personal policial indicó que es necesario de datos y que personas ajenas a la institución no tengan acceso a la información institucional y el 0.8% indicó que no era necesario la protección de datos.

Los resultados muestran el interés del personal en proteger toda la información referente a la institución, recordando que la institución es la encargada de la seguridad nacional por lo que hay información exclusiva.



383 respuestas

Figura 11. Confidencialidad de información (Héctor Rolando Sunún Raymundo).

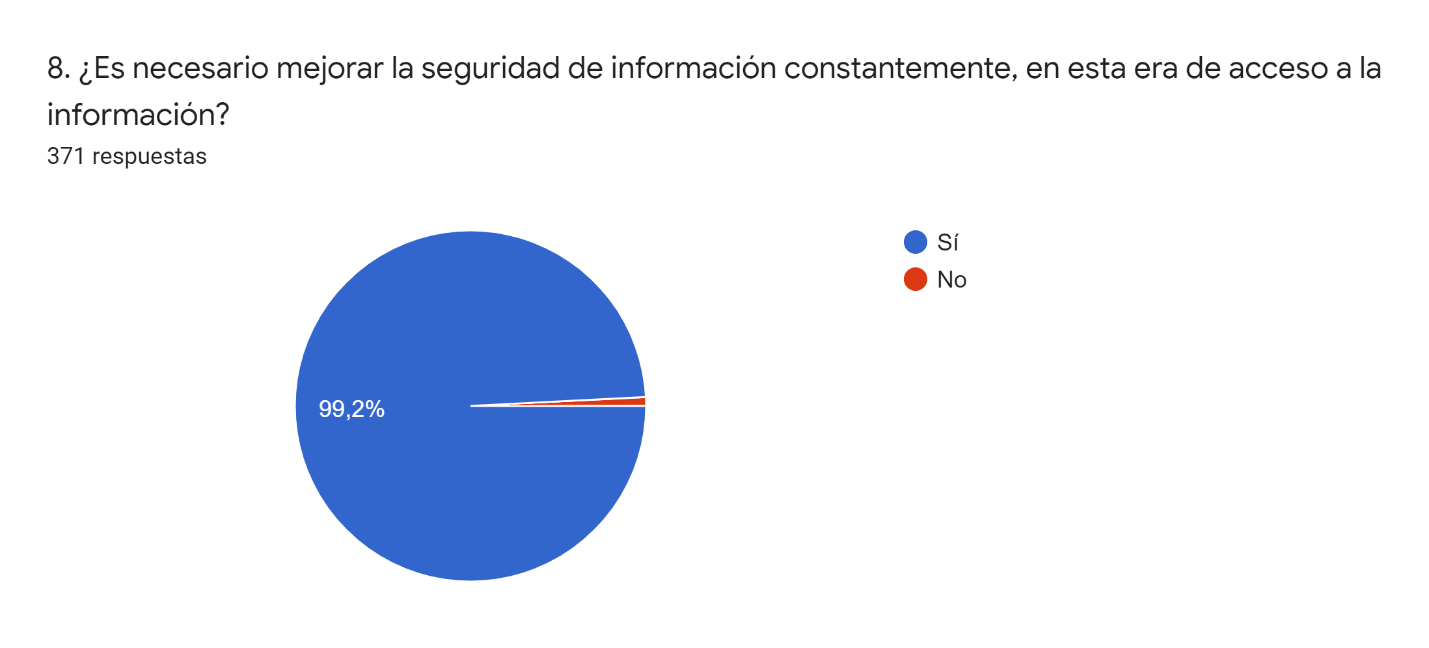
En 100% de los encuestados indicaron que es importante la confidencialidad de la información, el primer paso para seguir mejorando cómo organización es que cada uno de los integrantes reconozcan la situación actual y buscar mejoras continuas.



383 respuestas

Figura 12. Herramienta para Cifrado (Héctor Rolando Sunún Raymundo).

El 89.9% indicó que sí utilizaría una herramienta para el cifrado de datos y el 10.1 indicó que no. En esta gráfica se refleja la voluntad de seguir buscando herramientas para cifrar la información, reconociendo la importancia y delicadeza de la misma.

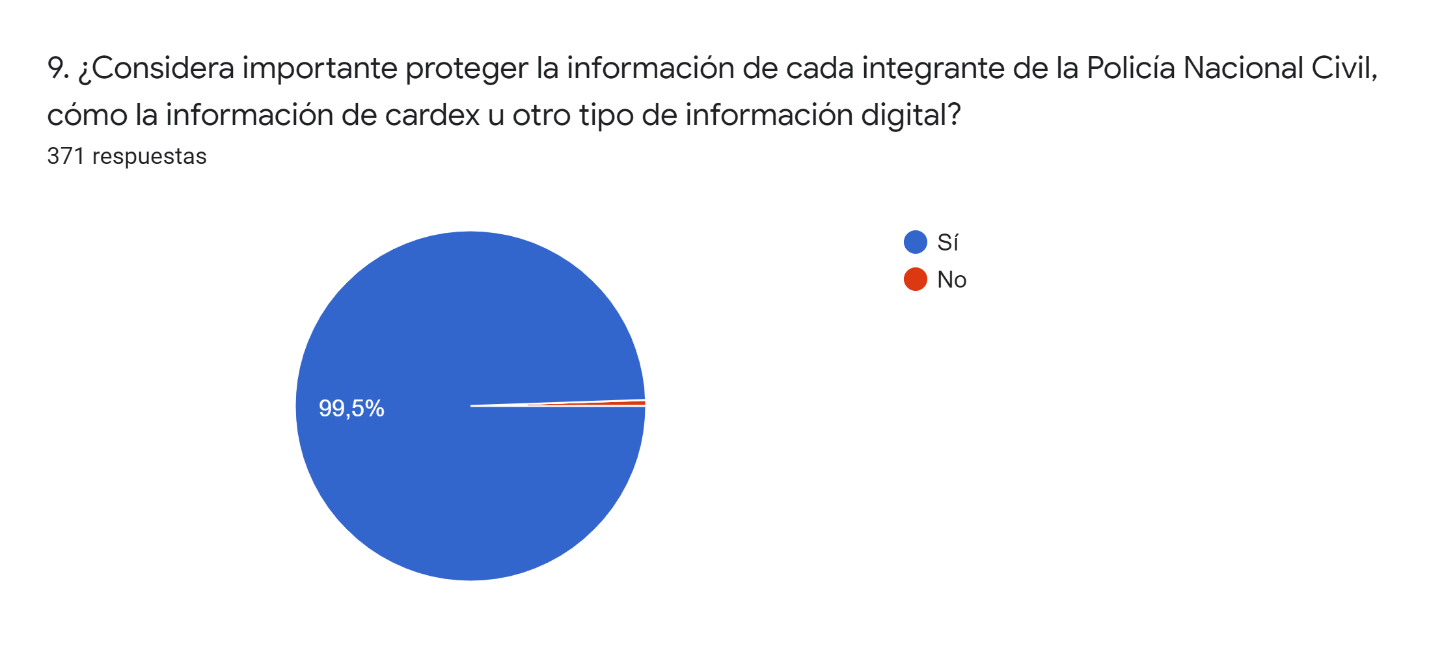


383 respuestas

Figura 13. Mejora de seguridad de Información (Héctor Rolando Sunún Raymundo).

El 99.2% del personal de la Policía Nacional civil indicó que en esta era dónde fluye mucho la información es necesario aumentar la seguridad de las mismas.

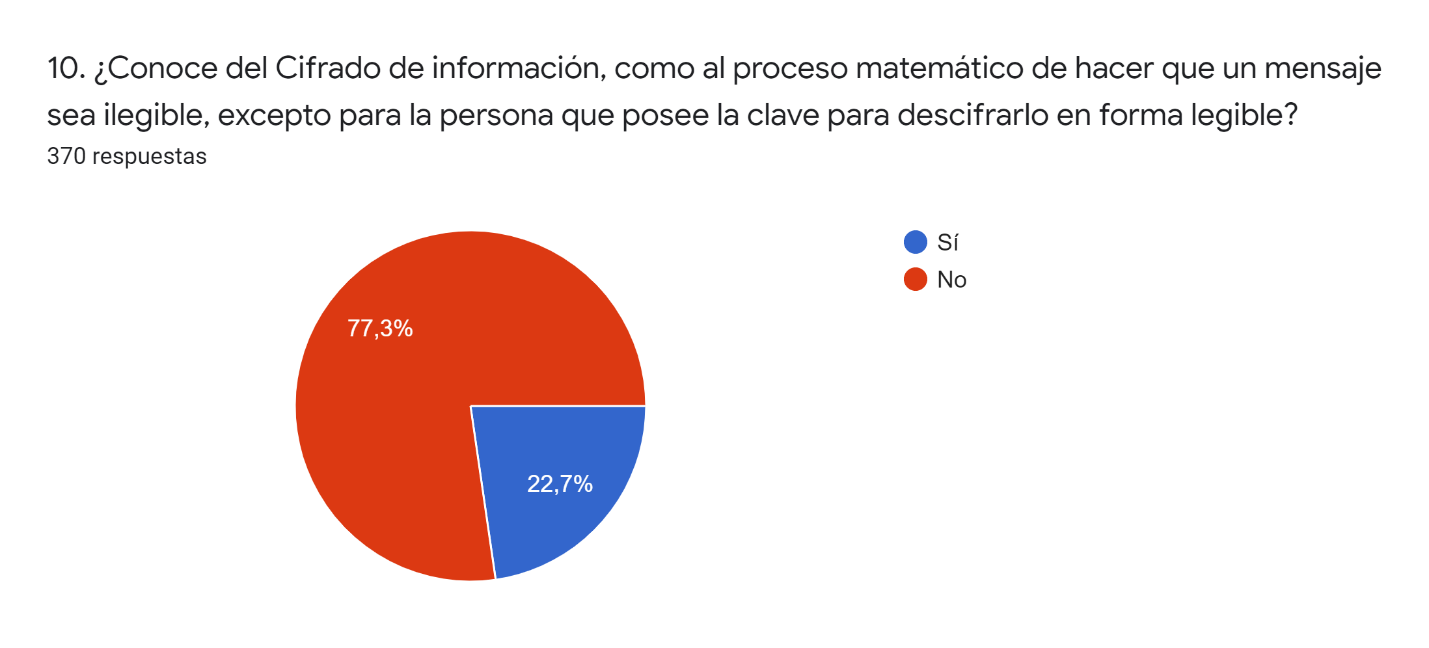
En esta gráfica se muestra que el personal reconoce que la información debe ser clasificada y exclusiva, especialmente cuando las mismas fluyen con más facilidad en estos tiempos, significa que también es necesario ir mejorando la seguridad de información.



383 respuestas

Figura 14. Datos Personales (Héctor Rolando Sunún Raymundo).

El 99.5% indicaron que información personal debe ser protegida, el 4.5% indicó que no, se refleja que como seres humanos tenemos esa necesidad de privacidad, especialmente con nuestra información personal y más aún cuando se pertenece a una institución de seguridad, en el que se que se tiene uno de los principios de secreto profesional.

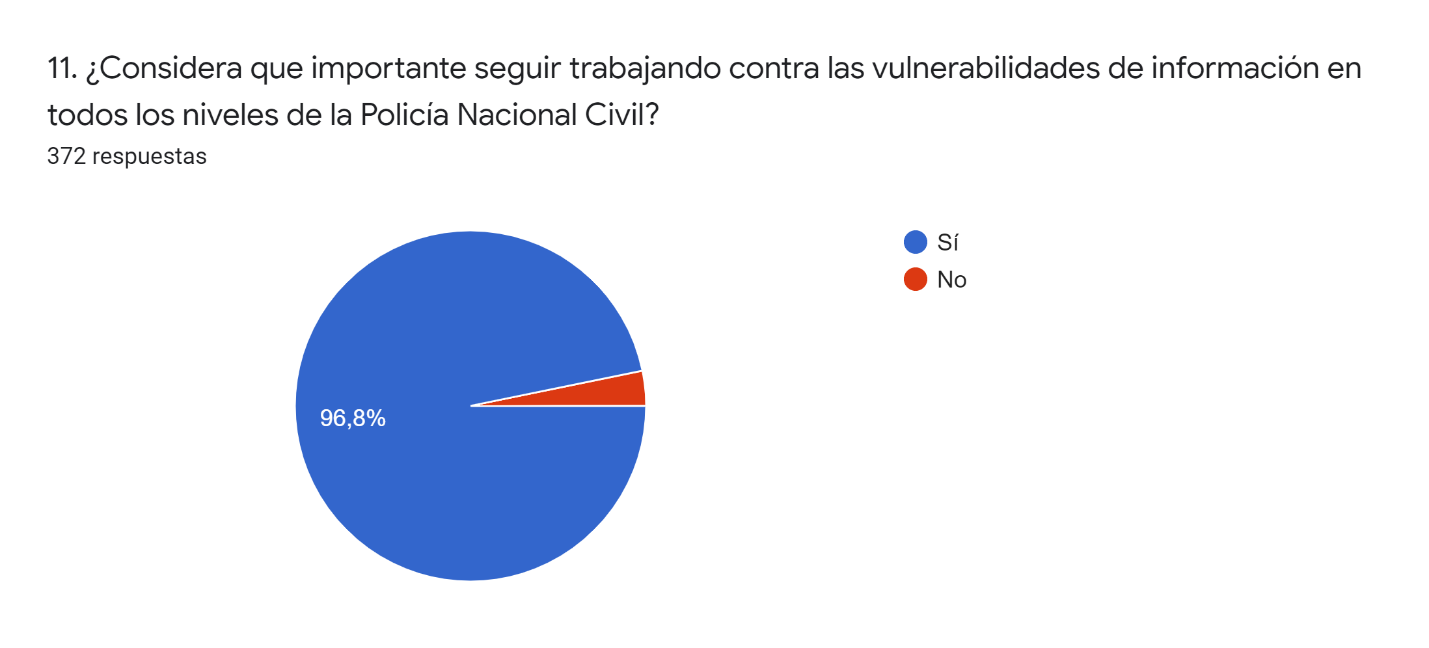


383 respuestas

Figura 15. Conocimiento de Cifrado de Información (Héctor Rolando Sunún Raymundo).

El 77.3% de los encuestados respondió que no conocía el cifrado de información y el 22.7% respondió que sí.

En la gráfica se refleja que buena parte de la población policial no conoce a profundidad el tema de cifrar la información, aunque reconocen la importancia de resguardar la información es un tema que no se ha dado la importancia cómo debería.



383 respuestas

Figura 16. Combate de vulnerabilidades (Héctor Rolando Sunún Raymundo).

El 96.8 % indicó que es necesario seguir trabajando en las vulnerabilidades de información y el 3.2% indicó que no.

Con esta gráfica se refleja que se necesita ir mejorando en el tema del cifrado de información cómo una manera de combatir las diferentes vulnerabilidades existentes, a la medida que aumenta el poder computacional es necesario seguir buscando métodos de protección de datos.