

Cesar Denis Pasto Escalona G-21 [cesarescalona2499@gmail.com](mailto:cesarescalona2499@gmail.com)

Tutor: Lic. Ernesto R. Carbonell Rigores

Introducción

**Problemática:**

En el entorno actual de desarrollo de software, la integridad y originalidad de los códigos son fundamentales para garantizar la confianza y la autenticidad de las aplicaciones. Sin embargo, el plagio de código es un problema cada vez más común que pone en riesgo la innovación y la propiedad intelectual. En este contexto, los procesos criptográficos emergen como una solución prometedora para abordar esta problemática, al proporcionar mecanismos de protección que aseguran la autenticidad y la autoría del código fuente. En el mundo actual, donde la tecnología avanza a un ritmo rápido y constante, la seguridad del software es de suma importancia. La protección contra el plagio y las modificaciones no autorizadas es crucial para garantizar la integridad y la confiabilidad del software.

**Campo De Acción:**

**El campo de acción para esta investigación es el Protocolo de Firma Digital con Matrices Elementales de Hill**: Este protocolo es un método criptográfico que utiliza matrices elementales de Hill para generar firmas digitales. Las matrices elementales de Hill son una herramienta matemática que se utiliza matrices para transformar mensajes de texto claro en cifrado. Este proceso este proceso se extiende para incluir la generación de firmas digitales, la cual es un tipo de autenticación digital que verifica la integridad de los datos y confirma la identidad del remitente.

**Objeto de Estudio:**

**El objeto de estudio para esta investigación es el Protocolo Criptográfico Post Cuántico implementado en grupo no conmutativo:** Este protocolo es una innovación en el campo de la criptografía que utiliza conceptos post cuánticos y grupos no conmutativos para mejorar la seguridad del software.

**Los objetivos específicos de esta investigación son:**

1. Analizar la problemática del plagio y la modificación de código de software.

2. Explorar el uso del Protocolo de Firma Digital con Matrices Elementales de Hill como solución a estos problemas.

3. Investigar el Protocolo Criptográfico Post Cuántico implementado en grupo no conmutativo como una posible mejora en la seguridad del software.

4. Desarrollar estrategias y técnicas para prevenir el plagio y las modificaciones no autorizadas en el código de software utilizando el Protocolo de Firma Digital con Matrices Elementales de Hill y el Protocolo Criptográfico Post Cuántico.

**Palabras Claves:** Plagio, Modificación, Software, Protocolo de Firma Digital, Matrices Elementales de Hill, Protocolo Criptográfico Post Cuántico, Grupo No Conmutativo, Seguridad del Software, Integridad, Confiabilidad, Criptografía, Matemáticas, Innovación, Mejora, Prevención, Estrategias, Técnicas.

Desarrollo:

**1. Capítulo 1:**

**1.1. Introducción:**

En el siguiente capitulo se plantea las bases teóricas como principal concepto para el desarrollo del trabajo. Se hacen referencias a los Conceptos y Bases que facilitan la comprensión del proyecto. Para abordar el objetivo deseado de forma general se parte desde lo mas particular ampliando la investigación para resolver los problemas de Seguridad contra plagios en el Sistema GREHU. Se tienen en cuenta las herramientas básicas para la implementación del protocolo de firma digital, que llevan a la seguridad deseada.

**1.2. Sistema Informatizado de Gestión de Recursos Humanos (GREHU):**

En cuba son cada vez mayores las empresas que invierten en Sistemas de Información (SI), que apoyen y sustenten la Gestión de Recursos Humanos (RH) de tal forma asumiendo de que la formación no es gasto si no una inversión. Sin embargo, tan concepción en la GRH, que se centra la Estrategia de la Empresa. La herramienta GREHU es un software que se encuentra implantado en la mayor parte de las Empresas Cubanas. Cuenta con varios módulos como: Inventario de personal, Selección y Contratación, puesto y caso, evaluación del desempeño, prenominas, nominas, pago por resultados entre otros. El empleo de esta herramienta en los departamentos de personal y de Economía ha implicado una más ágil Realización del trabajo por parte de los trabajadores, fiabilidad y minimización de costos.

Algunas de las funcionalidades que incluye:

🡪 Efectúa el control de la Asistencia del personal.

🡪Administración de plantilla del personal de la Empresa, permite el control de la Asistencia.

🡪 Permite Gestionar a los trabajadores y candidatos para desempeñar determinados cargos, así como elaborar cargos de los mismos.

🡪Realiza la Gestión de los Dirigentes y Cuadros de las Entidades.

**1.3. Elementos de Seguridad Informática:**

Se abordan elementos de la Seguridad Informática que se tienen en cuenta para el desarrollo del Trabajo.

**1.3.1. Ataque informático:**

Cuando se habla de seguridad Informática es muy importante tener en cuenta lo que significa el Ciberataque o Ataque Informático que no es más que una acción que tiene como finalidad última producir mayor incertidumbre en el modelo de Seguridad y Control de una Organización, Nación o Empresa. En otra forma de decir más practica Revelar los puntos ciegos y ocultos que tienen en las implementaciones de Seguridad que en las Empresas y Naciones tienen. Hay que tener en cuenta que los ciberataques provienen en muchos casos de distintas fuentes pueden ser individuos o organizaciones que buscan obtener el control del Sistema.