# RESUMEN

En esencia el presente documento estudia lo que es una infraestructura de clave pública o PKI, además de las leyes que regulan el uso de dicha infraestructura y las herramientas a ser utilizadas para la implementación de la misma. Una infraestructura de clave pública o PKI, es un conjunto conformado por software, hardware y políticas de seguridad, con el fin de garantizar la integridad y confidencialidad de la información. Esta infraestructura se basa en la criptografía asimétrica, es decir se basa en el uso de un par de claves, una que cifra la información y otra que la descifra, según el caso una puede ser privada y la otra pública. Por otro lado, tenemos las leyes que rigen todos los procesos orientados a la implementación y uso de la PKI. Para ello también se debe tener un profundo conocimiento de la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", y por las políticas emitidas por la ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones); enfocándonos específicamente al Capítulo II "De los Certificados de Firma Electrónica", y al Capítulo III "De las Entidades de Certificación de Información". Y finalmente, se analizan las herramientas a ser utilizadas para la implementación de la infraestructura, y el proceso de instalación y configuración de dichas herramientas y plataformas a ser utilizas. Además de esto se va a programar una nueva herramienta llamada pkiEjercitoEC, cuyo fin es acoplar toda esta infraestructura a la realidad tecnológica del Ejército Ecuatoriano. Como podemos apreciar el presente documento más que teórico es práctico, y la implementación de esta nueva tecnología en las Fuerzas Armadas del Ecuador, permitirán una mejora significativa de las Seguridades Informáticas e incrementará el nivel de confianza en los Sistemas que desarrollamos.

**PALABRAS CLAVE:**

- ✓ **INFRAESTRUCTURA DE CLAVE PÚBLICA**
- ✓ **FIRMA ELECTRÓNICA**
- ✓ **SEGURIDAD INFORMÁTICA**
- ✓ **PROGRAMACIÓN**
- ✓ **CONFIGURACIÓN LINUX**

# ABSTRACT

In essence this document explores what is a PKI, or public key infrastructure as well as the laws governing the use of such infrastructure and tools to be used for the implementation of the same. A PKI, or public key infrastructure is a set consisting of software, hardware and security policies, in order to ensure the integrity and confidentiality of the information. This infrastructure is based on asymmetric cryptography, i.e. based on the use of a pair of keys, one that encrypts information and other decoding, depending on the case one can be private and the other public. On the other hand, we have the laws that govern all of the processes aimed at the implementation and use of the PKI. This also should be a deep knowledge of the "law of electronic commerce, data messages and electronic signatures", and by the policies issued by the ARCOTEL (Agency for the regulation and Control of telecommunications); focusing specifically on chapter II "Of the certificates of signature electronic", and chapter III "certification of information entities". And finally, is analyzed the tools to be used for the implementation of the infrastructure, and the process of installation and configuration of these tools and platforms to be use. In addition to this, you will schedule a new tool called pkiEjercitoEC, which aims to connect all this infrastructure to the technological reality of the Ecuadorian army. As can appreciate the present document rather than theoretical is practical, and the implementation of this new technology in them forces armed of the Ecuador, will allow an improves significant of them securities computer e will increase the level of confidence in the systems that develop.



**KEYWORDS:**

- ✓ **PUBLIC KEY INFRASTRUCTURE**
- ✓ **ELECTRONIC SIGNATURE**
- ✓ **COMPUTER SECURITY**
- ✓ **PROGRAMMING**
- ✓ **LINUX CONFIGURATION**