Maestría en Seguridad de Tecnologías de Información
Controles Criptográficos de Seguridad
2023-3

Profesor: Maestro Sánchez García Isaac Daniel

ENTREGABLE FINAL:

"PROPUESTA DE PROYECTO EJECUTIVO DE MÉTODOS DE CIFRADO Y PORTAFOLIO DE EVIDENCIAS"

Alumna: Kuhliger Martínez Martha Guadalupe

Número de Cuenta: 334011227

04 de junio del 2023

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo consiste en implementar y reforzar los conocimientos y las tecnologías que se aprendieron en el curso de Controles Criptográficos de Seguridad para el diseño de una propuesta que proporcionará una mayor seguridad en el intercambio de información dentro de una organización para un caso de estudio de una empresa real, la cual se nombrará *MKuhliger S.A. DE C.V*. para este efecto.

El caso de estudio consistió en desarrollar una estrategia para implementar métodos de cifrado a los datos y documentos que la organización transfiere mediante el uso del correo electrónico para proteger la organización y guiarla adecuadamente, y así prevenir amenazas dañinas debido al mal manejo de la información y a la explotación de intrusos y ciberdelincuentes que vean como una oportunidad de acceder a información confidencial para sus propios intereses.

Se realizó una recopilación y análisis de información con respecto a los distintos métodos de cifrado que se han desarrollado desde su inicio, los algoritmos de cifrado, las herramientas que existen para facilitar el uso de los métodos de cifrado, su aplicación a la industria, las funciones de cifrado unidireccionales, problemas y explicaciones de cómo se realizan los métodos de cifrado y recomendaciones que se deben seguir para llevar a cabo una implementación exitosa y eficiente de los métodos de criptografía.

Con base en lo anterior, se desarrolló una propuesta para garantizar un mejor control de datos y gestionar la información, ejecutando métodos de cifrado y herramientas como OpenSSL y GNUPG, y generar llaves de cifrado para la organización *MKuhliger S.A. DE C.V*.

Se anexaron dentro del contenido del trabajo los entregables que se realizaron durante el curso, lo cuales son el ensayo sobre cifrado y esteganografía, la práctica de funciones de cifrado unidireccional el problemario de los métodos de cifrado clásicos, así como el cuestionario del curso.

De esta forma se podrá minimizar y mitigar los accesos a la información confidencial para proteger la integridad de los datos de la organización *MKuhliger S.A. DE C.V*. y de sus clientes, ante un ataque o amenaza, ya sea una acción voluntaria o involuntaria que puede surgir y causar un daño a la organización.

Por confidencialidad se ha modificado el nombre de la organización por *MKuhliger S.A. DE C.V.*, así como algunos detalles de la biografía de la organización.

ABSTRACT

The present work consists of implementing and reinforcing the knowledge and technologies learned in the Cryptographic Security Controls course for the design of a proposal that will provide greater security in the exchange of information within an organization for a case study of a real company, which will be named *MKuhliger S.A. DE C.V.* for this purpose.

The case study consisted of developing a strategy to implement encryption methods to the data and documents that the organization transfers through the use of email to protect the organization and guide it properly, and thus prevent harmful threats due to mishandling of information and exploitation of intruders and cybercriminals who see it as an opportunity to access confidential information for their own interests.

A compilation and analysis of information was carried out regarding the different encryption methods that have been developed since their inception, encryption algorithms, tools that exist to facilitate the use of encryption methods, their application to the industry, one-way encryption functions, problems and explanations of how encryption methods are performed and recommendations that should be followed to carry out a successful and efficient implementation of cryptography methods.

Based on the above, a proposal was developed to ensure better data control and information management, implementing encryption methods and tools such as OpenSSL and GNUPG, and generate encryption keys for the *MKuhliger S.A. DE C.V*. organization.

The deliverables that were made during the course, which are the essay on encryption and steganography, the practice of unidirectional encryption functions, the problem of classical encryption methods, as well as the course questionnaire, were annexed within the content of the work.

In this way it will be possible to minimize and mitigate access to confidential information to protect the integrity of the data of the organization *MKuhliger S.A. DE C.V.* and its customers, before an attack or threat, either a voluntary or involuntary action that may arise and cause damage to the organization.

For confidentiality reasons, the name of the organization has been changed to *MKuhliger S.A. DE C.V*., as well as some details of the organization's biography.