|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DATOS DE LA ACTIVIDAD | | | | | | | |
| No. de Actividad: | **3.2** | **Investigación** | **Actividad 3.2 Investigación: Criptografía** | | | | |
| Unidad: | Unidad 3: Configuración de SSH y VPN | | | | | | |
| Carrera: | Tgo. en Desarrollo de Software | | | | | | |
| Materia | SEGURIDAD EN INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN | | | | | Clave | **18MPEDS0835** |
| Profesor: | Andrés Figueroa Flores | | | | | | |
| Alumno: | Esmeralda Itzel Rodríguez Guareño | | | | | Registro: | 19100256 |
| Institución: | **Centro de Enseñanza Técnica Industrial plantel Colomos** | | | | | | |
| Semestre: | 8 | Grupo: | B1 | Período: | Ago-Dic 2022 | Fecha: | 03/11/2022 |
| Compet. Genéricas | | 4.1, 4.5, 5.2, 5.5 | | Compet.. Profesional | | 12 | |

# **Propósito u objetivo:** Identificar los principales conceptos de la criptología

1. **Instrucciones**:  
   1. Investigar los siguientes conceptos: Integridad, Confidencialidad, Disponibilidad, Criptografía, Criptología, Criptoanálisis, y dar un ejemplo de cada uno o como se aplican.  
   Puedes Revisar el tema 2.2 Tríada de CID del curso Cybersecurity Essentials en <https://www.netacad.com/portal/learning>  
     
   2. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.  
     
   3. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.
2. **Línea del tiempo**

* **Integridad**: La integridad es la precisión, uniformidad y confiabilidad de los datos durante su ciclo de vida. Otro término para la integridad es el de calidad. Los datos experimentan varias operaciones como captura, almacenamiento, recuperación, actualización y transferencia.
* **Confidencialidad**: La confidencialidad previene la divulgación de información a las personas los recursos y los procesos no autorizados. Por ejemplo, un programador no debe tener acceso a la información personal de todos los empleados.
* **Disponibilidad**: La disponibilidad de los datos es el principio que se utiliza para describir la necesidad de mantener la disponibilidad de los sistemas y servicios de información en todo momento. Por ejemplo, alterar la disponibilidad de los sitios web de la competencia al eliminarla puede proporcionar una ventaja a su rival. Los métodos utilizados para garantizar la disponibilidad incluyen la redundancia del sistema, las copias de seguridad del sistema, mayor recuperabilidad del sistema, mantenimiento del equipo, sistemas operativos y software actualizados y planes para recuperarse rápidamente de desastres no planificados.
* **Criptografía**: En informática, la criptografía se refiere a técnicas de comunicación e información seguras derivadas de conceptos matemáticos y cálculos basados ​​en reglas llamados algoritmos, para transformar los mensajes en formas difíciles de descifrar. Se utilizan tres tipos de criptografía, la simétrica, la de llaves públicas y la de hash.

En la primera tanto el remitente como el receptor comparten una única clave. El remitente utiliza esta clave para cifrar texto sin formato y enviar el texto cifrado al receptor. Por otro lado, el receptor aplica la misma clave para descifrar el mensaje y recuperar el texto sin formato.

* **Criptología**: Es el estudio de la criptografía y el criptoanálisis. Por ejemplo, aplicar algoritmo de criptografía en un sistema. Como la criptografía simétrica descrita anteriormente.
* **Criptoanálisis**: El criptoanálisis se utiliza como método para descifrar un texto cifrado en texto sin formato. Un criptoanalista puede proteger los datos y la red aprovechando estas técnicas de criptoanálisis:

El trabajo principal es investigar y probar nuevas teorías y aplicaciones de criptología.

* Capaz de probar modelos computacionales para lograr confiabilidad y precisión.
* Garantiza que los datos de transmisión de mensajes (red inalámbrica, teléfono seguro, teléfonos móviles, correo electrónico, etc.) no sean conocidos ilegalmente o se alteren durante el tránsito de datos.
* Protege la información vital para que no sea interceptada, copiada, modificada o eliminada.
* Capaz de decodificar mensajes crípticos y sistemas de codificación para agencias militares, políticas y fuerzas del orden.

**Reflexión**

En esta actividad vimos todo lo relacionado a la criptología que es el estudio de la criptología y la criptografía. La segunda ya es la aplicación de algoritmos y métodos como la criptografía simétrica, la de la llave publica y el hash. Además, que conceptos básicos como confidencialidad, integridad y disponibilidad.

# Bibliografía

Ciberseguridad. (s.f.). *CRIPTOANÁLISIS, TODO LO QUE DEBES SABER.* Obtenido de Ciberseguridad: https://ciberseguridad.com/guias/prevencion-proteccion/criptoanalisis/#:~:text=El%20criptoan%C3%A1lisis%20se%20utiliza%20como,est%C3%A1%20sujeta%20a%20ninguna%20regla.

Equipo de Expertos en Ciencia y Tecnología. (09 de 08 de 2021). *Qué es la criptografía y cuáles son sus usos.* Obtenido de Universidad Nacional de Valencia: https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos#:~:text=Hoy%20en%20d%C3%ADa%2C%20la%20criptograf%C3%ADa,la%20empresa%20y%20los%20clientes.

HURTADO, J. S. (08 de 08 de 2022). *Qué es la criptografía y para qué sirve.* Obtenido de IEBS: https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/#:~:text=de%20t%C3%A9cnicas%20criptogr%C3%A1ficas%3A-,Criptograf%C3%ADa%20de%20clave%20sim%C3%A9trica,recuperar%20el%20texto%20sin%20formato.