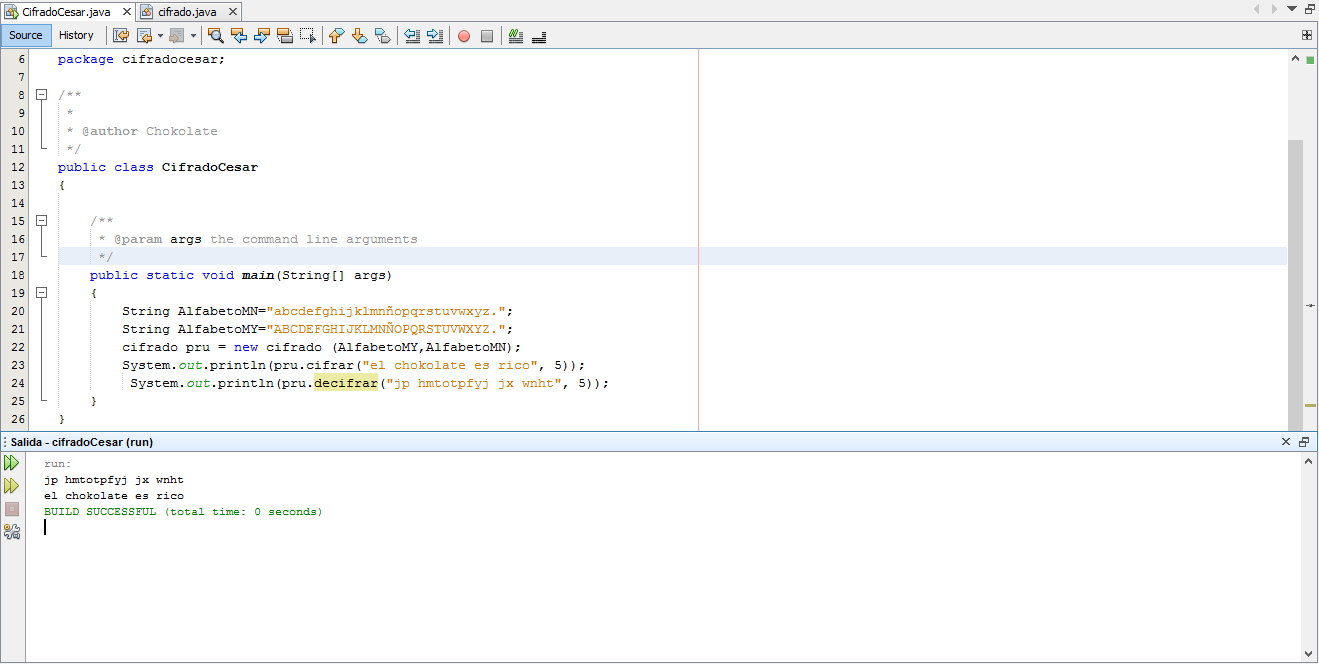
# Algoritmo Cesar





# 2.Definir cada uno de los siguientes enunciados:

## Criptosistema

Es el sistema en el cual un mensaje sin entrar es cifrado mediante procesos con claves para su envió y posterior descifrado en su destino y así garantizar un envío seguro en un canal inseguro.

Otra definición según el documento “Criptografía y seguridad de computadores” de la universidad Jaén en las paginas 23 y 24, lo describe como un quíntupla conformada por las palabras M,C,K,E,D donde las explican como: M:Mensaje sin cifrar(texto plano), C:Mensaje cifrado o criptogramas, K:Claves empleadas por los criptosistemas, E: funciones para transformación a mensaje cifrado y D: funciones para la transformación a mensaje sin cifrar. Finamente la simplifican toda en una ecuación:

La explican de la siguiente manera, un mensaje “m” lo “ciframos” empleando una clave “k” y luego lo “desciframos”, utilizando la clave “k” , obtenemos el mensaje original “m”.

No obstante, los criptosistemas tienen dos tipos según el documento mencionado anteriormente, son Criptosistema simétrico o de clave privada y criptosistema asimétrico o de clave pública. Los criptosistemas simétricos son los que poseen la misma clave k tanto para cifrar como para descifrar, lo que lleva a su principal problema que es como hacer llegar la clave tanto al emisor como al receptor por un canal que no es seguro. Por otro lado, los criptosistemas asimétricos son los que poseen dos claves dos claves k, una publica para encriptar y otra privada para desencriptar, lo que en parte soluciona el problema que posee el criptosistema simétrico.

## Cifrado Vigenere

Según el archivo “Criptografía y seguridad de computadores” de la universidad Jaén en las pagina 65 es un cifrado poli alfabético lo que significa que la sustitución aplicada a cada carácter varía en función de su posición que tenga dentro del texto plano. Esto se da gracias a una clave cíclica, conformada por varios caracteres que se distribuirá por la cadena de caracteres del texto plano. Como resultado todas sustituciones tendrán una combinación diferente, presentes en una table conformada por múltiples alfabetos idénticos cruzados y desplazados un carácter por columna.

## Cifrado Transposición

Según el archivo “Criptografía y seguridad de computadores” de la universidad Jaén en las pagina 66, es un cifrado que no sustituye símbolos por otros, en cambio cambia su orden dentro del texto. Existen varios métodos de transposición pero para entender el concepto, este consiste en, dividir la palabra en diferentes segmentos de la misma longitud de tamaño n y permutar sus segmentos con una clave como {3,2,1} donde los números indican el segmento 1 o el segmento 2.

## No repudio o Irrenunciabilidad

Según el archivo “Seguridad y Alta Disponibilidad” de la editorial RAMA en las pagina 13, consiste en probar la participación de las partes en la comunicación, lo que genera os tipos de no repudio. El no repudio en origen el cual consiste en que el emisor no puede negar él envió y El no repudio en Destino el cual consiste en que el receptor no puede negar que recibió el mensaje.

## 270001

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en las pagina 5, lo define como la normativa que proporciona requisitos establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información.

En este se explica todos los lineamientos a tener en cuenta para un sistema de gestión de la seguridad de la información.

## un sistema de gestión de la seguridad de la información

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en las pagina 5, lo define como el que tiene que otorgar confiabilidad, integridad y disponibilidad de la información al aplicar un proceso de gestión de riesgos. Además de proporcionar confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada.

## Planificación y control Operacional

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en las pagina 13, consiste en planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información. Por consecuente se debe controlar los cambios planificados y revisar las consecuencias de los cambios no planificados.

## Plan de tratamiento de riesgos

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su sección 8.3, consiste en implementar un plan de tratamiento del riesgo de la información en base a la información que se levante en la evaluación de riesgo de la seguridad de la información, la cual se debe realizar en intervalos planificados o cuando se proponga u ocurra cambios significativos en los procesos, con el objetivo de tener actualizado el plan de tratamiento de riesgos.

Otra definición, según el mismo archivo en su sección 6.1.3, es donde se debe seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de evaluación de riesgos. Siguiendo algunos parámetros como determinar todos los controles, que son necesarios para implementar las opciones de tratamientos de riesgo de la seguridad de la información escogida.

## Monitoreo, Medición, Análisis y Evolución de Desempeño

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su sección 9.1, explica que se debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la seguridad de la información. Por medio de determinar que se necesita monitorear, medir, analizar y evaluar según corresponde para asegurar resultados válidos.

## Política de la gestión de la información

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su Apéndice A.5, lo define como un documento orientativo para la dirección en la tarea de seguridad de la información, de acuerdo con los requisitos del negocio y a las regulaciones y leyes pertinentes.

## PDCA o PHVA

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su sección 10, se define como Planificar, hacer, verificar y actuar según sus siglas y es conocido como ciclo de mejora continua, el cual se usa repetidas veces en el documento como concepto base.

## Stakeholder

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su sección 4, se define como personas u organizaciones afectadas por las actividades y las decisiones de una empresa.

## Control Disuasorio

Según el archivo “Seguridad y Alta Disponibilidad” de la editorial RAMA en las pagina 52, consiste en controles que prevengan el acontecimiento de un riesgo para la organización. Como por ejemplo disuadir el uso de memorias USB personales en computadores de la organización, estableciendo una norma que los prohíba y un control que “registre esta actividad”.

## Trazabilidad

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su totalidad de secciones, consiste en llevar la información en todos los puntos del proceso, por ello al final de cada sección dice “la organización debe conservar la información documentada ……”.

## Plan de continuidad de negocio

Según el archivo “Norma Chilena NCh-ISO 270001” en su segunda edición del año 2013, en su sección 10, consiste reaccionar ante la no conformidad y si es necesario tomar acciones para controlarla o encargarse de las consecuencias.

Por otro lado, en el mismo documento en el Anexo A.17, lo definen como la incorporación de la continuidad de la seguridad de la información en la gestión de la continuidad del negocio. Por medio de la planificación, implementación y verificación y evaluación de la continuidad de la seguridad de la información.