

# Practica Final.

---

Apartado A. Especificación de Requisitos.

Carlos Contreras Sanz      NIA: 100300562

Álvaro Gómez Ramos      NIA: 100307009

UNIVERSIDAD CARLOS III DE MADRID

## Introducción

Este documento es una especificación de requisitos software para la empresa Paca Garse S.L., especializada en la provisión de servicios de seguridad especializada y de servicios de detectives privados. Esta especificación se ha estructurado inspirándose en las directrices dadas por el estándar “IEEE Recommended Practice for Software Requirement Specifications IEEE 830 1998”.

## Propósito

El objeto de este documento es definir de manera clara y precisa todas las funcionalidades y restricciones del componente que se desea desarrollar para la empresa anteriormente mencionada.

## Ámbito del Sistema

La empresa Paca Garse S.L. necesita un componente software que pueda integrarse y ser usado en otros sistemas que ya utiliza.

## Visión General del Documento

En este documento se va a enumerar y describir todas las características del componente a desarrollar. El documento consta de una Introducción, una Descripción General del Software, y el repaso detallado de todos los requisitos.

## Definiciones

No se consideran necesarias definiciones para el desarrollo de este documento.

## Acrónimos

R	-	Requisito
F	-	Funcional
NF	-	No Funcional
E	-	Entrada
O	-	Operación
S	-	Salida

## Referencias

IEEE Recomendad Practices for Software Requierements especification ANSI/IEEE 830 1998.

Transparencias de la asignatura “Principios de Desarrollo del Software”.

## Descripción General

En esta parte del documento se describe todo lo relacionado con el componente de cifrado que se va a desarrollar y las características que se desea que tenga, así como funcionalidades o servicios que se desea que preste. No se describen los requisitos, si no lo relacionado con ellos, y donde se enmarcan, para hacer más fácil su entendimiento cuando luego los vemos en detalle.

## Perspectiva del Producto

El producto es un componente software que deberá prestar servicio a la empresa Paca Garse S.L. y deberá ser integrado con otros ya existentes de la compañía.

En términos generales este componente deberá proporcionar las siguientes funcionalidades, relacionadas con el cifrado y descifrado de cadenas de texto:

- Ser capaz de cifrar y descifrar mensajes cortos de texto (de 3 a 144 caracteres), en “castellano”, “frances” e “ingles”.
- Ser capaz de aplicar el algoritmo attbash.
- Ser capaz de aplicar el algoritmo cesar.
- Ser capaz de aplicar el algoritmo vigenere.
- Ser capaz de aplicar el algoritmo vernam.

## Interfaces con Sistemas Externos

Como ya se ha mencionado este componente deberá de comunicarse con distintos servicios de la empresa ya existentes, para ello ha de desarrollarse en J2EE.

## Restricciones y Dependencias

Todo el componente ha de estar desarrollado en J2EE para una correcta integración con los demás servicios. Además se exigirá que el texto de entrada pertenezca a uno de estos tres idiomas: castellano, francés o inglés.

Los caracteres que contemplarán en los mensajes cortos de texto a cifrar solo podrán estar compuestos de las letras de los alfabetos, en mayúsculas y minúsculas (incluyendo diacríticos), los números del 0 al 9 y signos de puntuación (incluido el espacio en blanco) contemplados en cada uno de los idiomas considerados para este componente, de tal manera, que un mensaje de entrada solo será correcto si está formado por los caracteres establecidos para ese idioma.

No se especifican requisitos de rendimiento, ni de seguridad, ni de desarrollo, ni tecnológicos, ni ninguno no mencionado.

## Requisitos Específicos

En este apartado vamos a describir cada uno de los requisitos que se le exigen al componente. Todos los requisitos son necesarios para que el componente cumpla con las expectativas del cliente. Estas especificaciones se podrán diferenciar por el número identificador que le ponemos a cada requisito. Además de diferenciarse por este identificador, también se puede diferenciar entre requisitos funcionales y no funcionales.

## Requisitos Funcionales

Antes de empezar con los requisitos se debe señalar que todas las entradas deber ser correctas, conforme a lo especificado en las demás partes de este documento.

A pesar de que en los requisitos figura la comprobación de la entrada, no se hará específicamente en cada algoritmo, su no de forma inicial previa.

**RF1:** El componente debe cifrar y descifrar texto usando el algoritmo atbash.

**RF1 - E1:** Texto a cifrar.

**RF1 - E2:** Indicador de cifrado/descifrado.

**RF1 -E3:** Idioma del texto.

**RF1 - O1:** Comprobar que E1 cumple los requisitos.

**RF1 - O2:** Realizar el cifrado/descifrado mediante atbash del texto de E1.

**RF1 - S1:** Texto cifrado/descifrado mediante este método.

**RF2:** El componente debe cifrar y descifrar texto usando el algoritmo cesar.

**RF2 - E1:** Texto a cifrar.

**RF2 - E2:** Clave de cifrado/descifrado (número).

**RF2 - E3:** Indicador de cifrado/descifrado

**RF2 - E4:** Idioma del texto

**RF2 - O1:** Comprobar que E1 cumple los requisitos.

**RF2 - O2:** Realizar el cifrado/descifrado mediante cesar del texto de E1.

**RF2 - S1:** Texto cifrado/descifrado mediante este método.

**RF3:** El componente debe cifrar y descifrar texto usando el algoritmo vigenere.

**RF3 - E1:** Texto a cifrar.

**RF3 - E2:** Clave de cifrado/descifrado (caracteres).

**RF3 - E3:** Indicador de cifrado/descifrado

**RF3 - E4:** Idioma del texto

**RF3 - O1:** Comprobar que E1 cumple los requisitos.

- RF3 - O2:** Comprobar que E2 cumple los requisitos (longitud desde 2, hasta mitad más uno de la longitud de E1).
- RF3 - O3:** Realizar el cifrado/descifrado mediante vigenere del texto de E1.
- RF3 - S1:** Texto cifrado/descifrado mediante este método.

- RF4:** El componente debe cifrar y descifrar texto usando el algoritmo vernam.
- RF4 - E1:** Texto a cifrar.
- RF4 - E2:** Clave de cifrado/descifrado (caracteres).
- RF4 - E3:** Indicador de cifrado/descifrado
- RF4 - E4:** Idioma del texto
- RF4 - O1:** Comprobar que E1 cumple los requisitos.
- RF4 - O2:** Comprobar que E2 cumple los requisitos (longitud igual a la longitud de E1).
- RF4 - O3:** Realizar el cifrado/descifrado mediante vernam del texto de E1.
- RF4 - S1:** Texto cifrado/descifrado mediante este método.

## Requisitos no Funcionales

### Restricciones:

- El sistema debe de estar desarrollado en la plataforma J2EE para que este componente pueda ser integrado y usado en los sistemas que ya utiliza la empresa (enumerados anteriormente).
- Los idiomas con los que podrá tratar este componente serán:
  - castellano  
("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !,;.:ÁÉÍÓÚáéíóú")
  - Ingles  
("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !,;.:")
  - francés  
("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !,;.:çÇÂâÊêÎîÔôÛûÀàÈèÙùËëÏïÜüŸÿÁÉÍÓÚáéíóúŒœ")
- Podrá tratar con mayúsculas, minúsculas, números de 0 a 9 y signos de puntuación, incluido el espacio en blanco.