SESION 2 1er parcial

Introducción a la administración de la seguridad informática

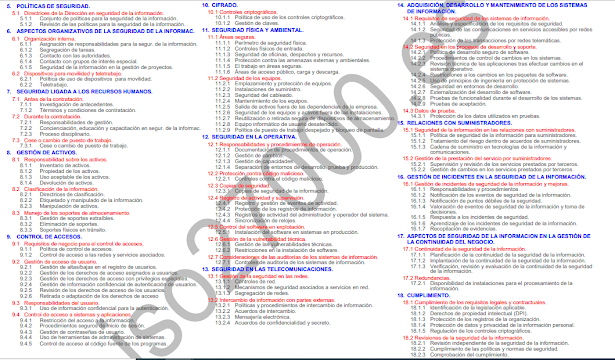
Objetivo: al finalizar la sesión el alumno identificara los conceptos base en la administración de la seguridad informática bajo estándares de certificación ISO 27000

Consideraciones teóricas: la forma internacional ISO (organización internacional de normalización) específicamente para ISO 2700 formaliza procesos, estándares, metodologías en función a sistemas de gestión de la seguridad de la información, sus directrices, gobernabilidad y administración. Define lo siguiente:

1. Administración. Procesos por etapas (planeación, organización, dirección y control) para obtener mayor productividad, un costo beneficio optimo en cualquier área de la función (nube, ciberseguridad, sistemas operativos, bases de datos, soporte técnico ti, infraestructura, redes, telecomunicaciones, etc)
2. Información. Datos, comunicación, adquisición de conocimiento digital, conocimiento humano que permite ampliar o presentar un campo, materia o área almacenado
3. Seguridad informática. Protección, salvaguarda de los activos tecnológicas, digitales en contra de amenazas, vulnerabilidades, ataques, riesgos aplicados (confidencialidad, integridad, disponibilidad)

Administración de la seguridad informática.

Apoya, organiza, planifica, automatiza, controla todas las tareas, actividades, procesos, funciones a nivel tecnológico, infraestructura de las empresas para identificar, renidminetos, productividad, identificar riesgos, amenazas , resoluciones y toma de decisiones bajo diseño, implementación y mantenimiento de sistemas de gestión de la seguridad de la información (SGSI) norma iso 27000-27040



Desarrollo:

Descargue y ejecute la herramienta MSAT (Microsoft segurity admin tool) regulado bajo la norma iso 27000 para evaluar la administración de la seguridad informática de la universidad

TEST profesional de evaluación de la administración de la seguridad informática MSAT

Incluye un cuestionario regulado por ISO 27000 y NIST permite ver los posibles agujeros, vulnerabilidades, riesgos y situaciones críticas de la empresa.

Proporciona un perfil de la situación de la seguridad en todos los ámbitos tecnológicos

Da estadísticas y gráficos de impacto importantes

Ofrece recomendaciones de las buenas prácticas de la administración de la seguridad informática

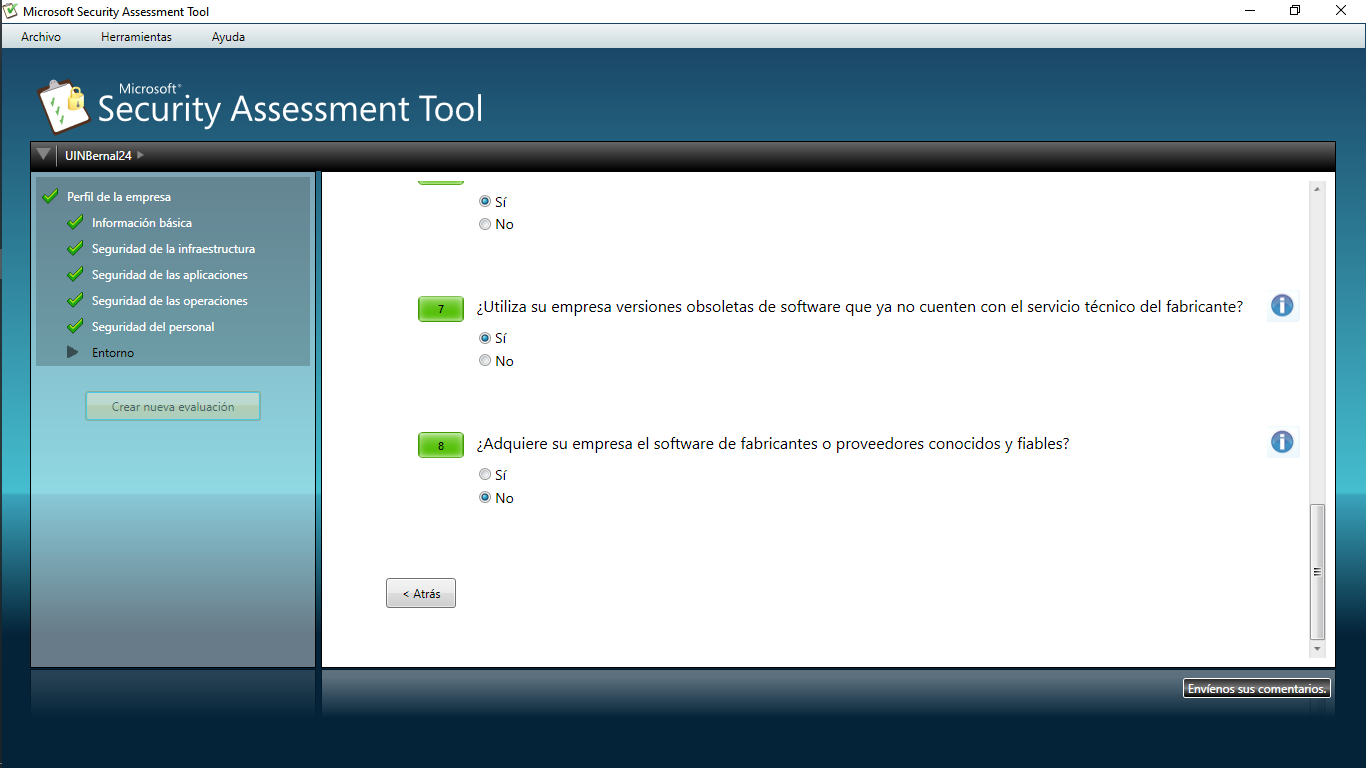
Cuestionario interactivo que da por resultado DiDI (índice de defensa) y BRP (perfil de riesgos de negocios)

Es una implementación de el marco de trabajo iso 27000-NIST es empleada con agentes de ciberseguridad CEO

uinBernal2024

escriba al menos 5 términos palabras o tecnologías desconocidas en investiguen

valor 0.3 puntos



Conclusión

La seguridad de la información en los diferentes sistemas de todos las cosas que se deben tener en cuenta para ver los rendimientos de la empresa

SESION 3 1ER PARCIAL

Plan de ciberseguridad base de MSAT y configuración de herramientas EVE-NG

Objetivo:

Al finalizar la sesión el alumno finalizara la evaluación de MSAT y formular un análisis de datos para verificar las acciones a tomar para una correcta administración de la seguridad informática

Consideraciones teóricas:

La primera fase de la administración de la seguridad informática es planeación donde se formula de estudio inicial mediante técnicas de recopilación de información (cuestionarios, entrevistas, checklist, observación, etc.).

Formulación de objetivos (SMART específicos, medibles, alcanzables, realizables y tiempos) para posteriormente implementos realizar planes de acción y operaciones a implementar en las diversas áreas de estudio (infraestructura, aplicaciones, operaciones y usuarios)

Infraestructura, defensa perimetral, autenticación, (dispositivos móviles y hosts fijs)

Aplicaciones, desarrollo, diseño, implementación

uso de aplicaciones seguras, medidas preventivas en las aplicaciones, algoritmos, criptografía, cifrado, certificados digitales, medios biométricos, llaves, operaciones verificación del entorno, vulnerabilidades, riesgos, políticas, prevención, colas de seguridad, respaldos, firewall, proxy, ID’S (sistema de detección de intrusos) HIFPS (sistema de detección y protección de intrusos) formación y consentimiento, capacitaciones

usuarios, requerimientos de seguridad de usuarios, evaluaciones de usuarios bajo conocimientos de ciberseguridad, políticas y procedimientos para mejora y elevar nivel de red seguridad

UIN CIBERSEGURIDAD el diario vivir en buenas prácticas de ciberseguridad

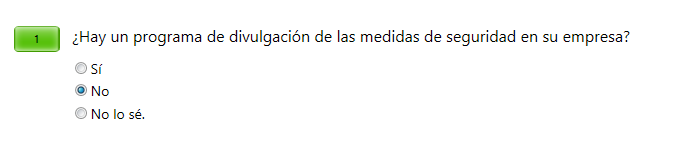
Desarrollo

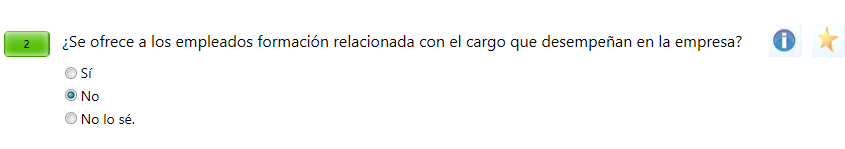
Cargue MSAT y equipos de 2 personas tome un área de estudio así mismo imprima pantallas de evidencias de algunas preguntas de checklist con respecto a su área, sus gráficas y recomendaciones

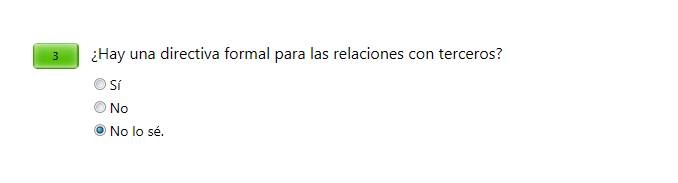
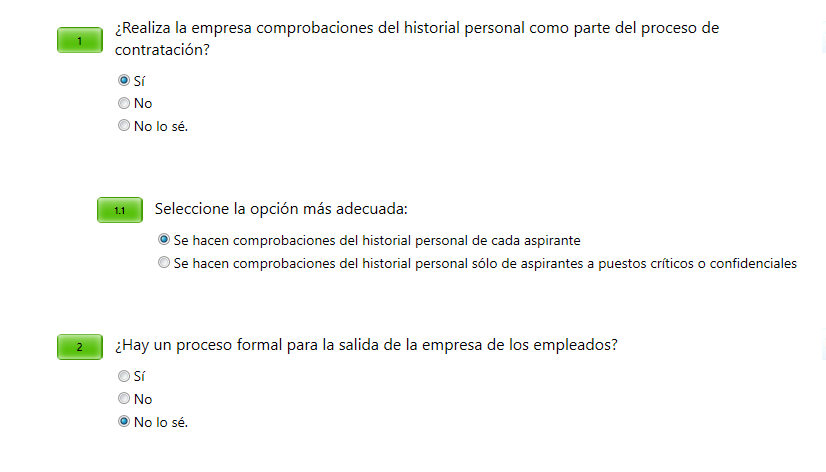
EQUIPO 4 USUARIOS

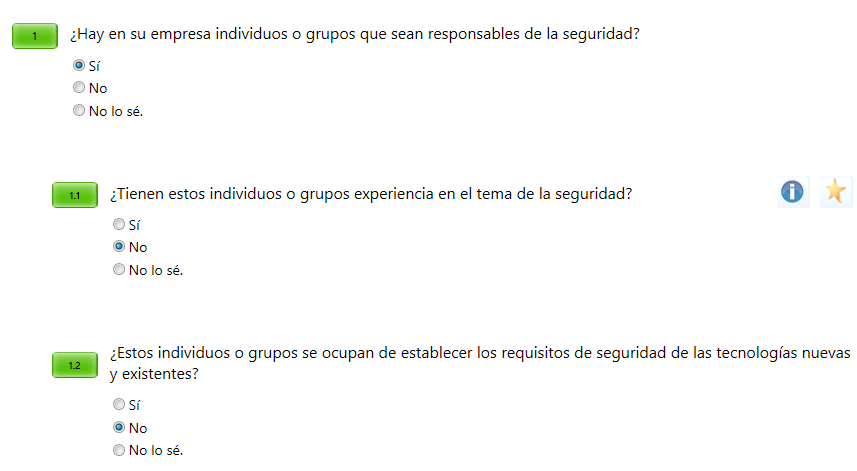
Axel Guízar

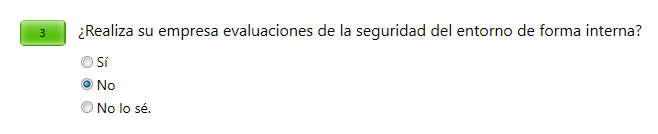
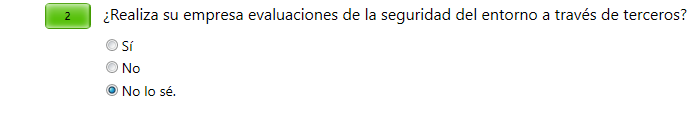
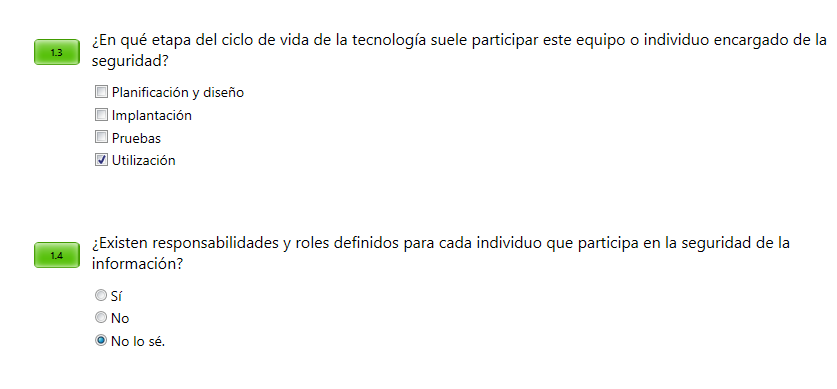
Antonio Bernal











Imprima y redacte cada uno de los equipos

**Infraestructura**

Uso correcto de como se debe tener la infraestructura para seguridad y segmentación optimizada de todas las áreas y cada uno tenga un área especial y no se tenga acceso rápido a otra sin un permiso solicitado

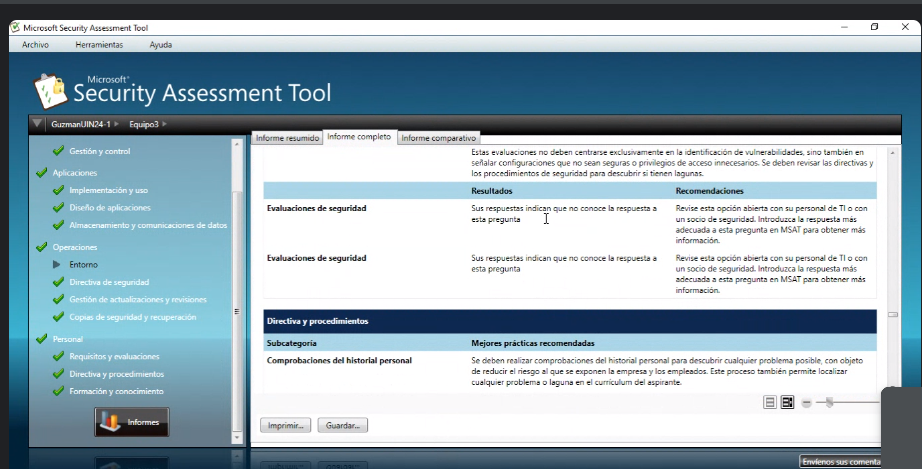
**Aplicaciones**

La seguridad métodos de como tener seguras todas las aplicaciones

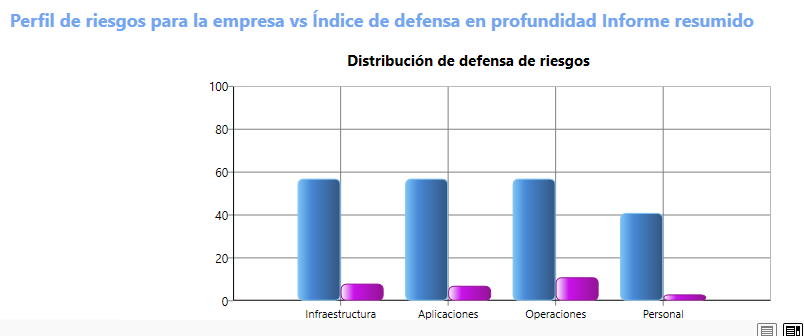
Y el uso de como cifrar archivos



**Operaciones**

****

**Usuarios**



Conclusión

Uso y funciones de la red especifica para el uso de los componentes y como tiene sus deficiencias la empresa y áreas a mejorar

SESION 4 1ER PARCIAL

Capa de usuarios para la seguridad informática.

Objetivo: al finalizar la sesión el alumno identificara diversas técnicas, estrategias tecnológicas para la capa de usuarios aplicando CRIPTOGRAFIA, manejo de contraseñas seguras.

Consideraciones teóricas:

La administración de la seguridad informática en la capa de usuarios estable los principios de integridad, disponibilidad, protección y salvaguarda de datos, utilizado diversos mecanismos como:

1. criptografía

Es la disciplina computacional en el área de ciberseguridad que se encarga del estudio de los principios, métodos y medio de transformar los datos para ocultar su significado Estudio principios, métodos para ocultar, transformar, garantizar la integridad, autoridad y prevenir repudio.

Se base en criptosistemas modernos y clásicos

Sus elementos base son:

Criptograma. Mensaje encriptado

Cifrador. Ente o elemento aplicador del método

Canal. Medio en que se envía

Generación de claves. Datos de seguridad encriptados o simples

Descifrador. Proceso inverso para generar la información inicial

criptoanálisis. aplicación de algoritmos, técnicas, estrategias criptográficas su función es recuperar claves e información cifrada

tipos de algoritmos criptográficos

1. clásicos. fundamento principal abecedario y sus permutaciones combinaciones

algoritmo inverso

algoritmo cesar

algoritmo de transposición

1. Modernos

Llaves secretas (simetría)

Llave publica (asimetría)

Algoritmo DES o 3DES estándar en encriptación de datos

Funciones Hash

Firmas digitales

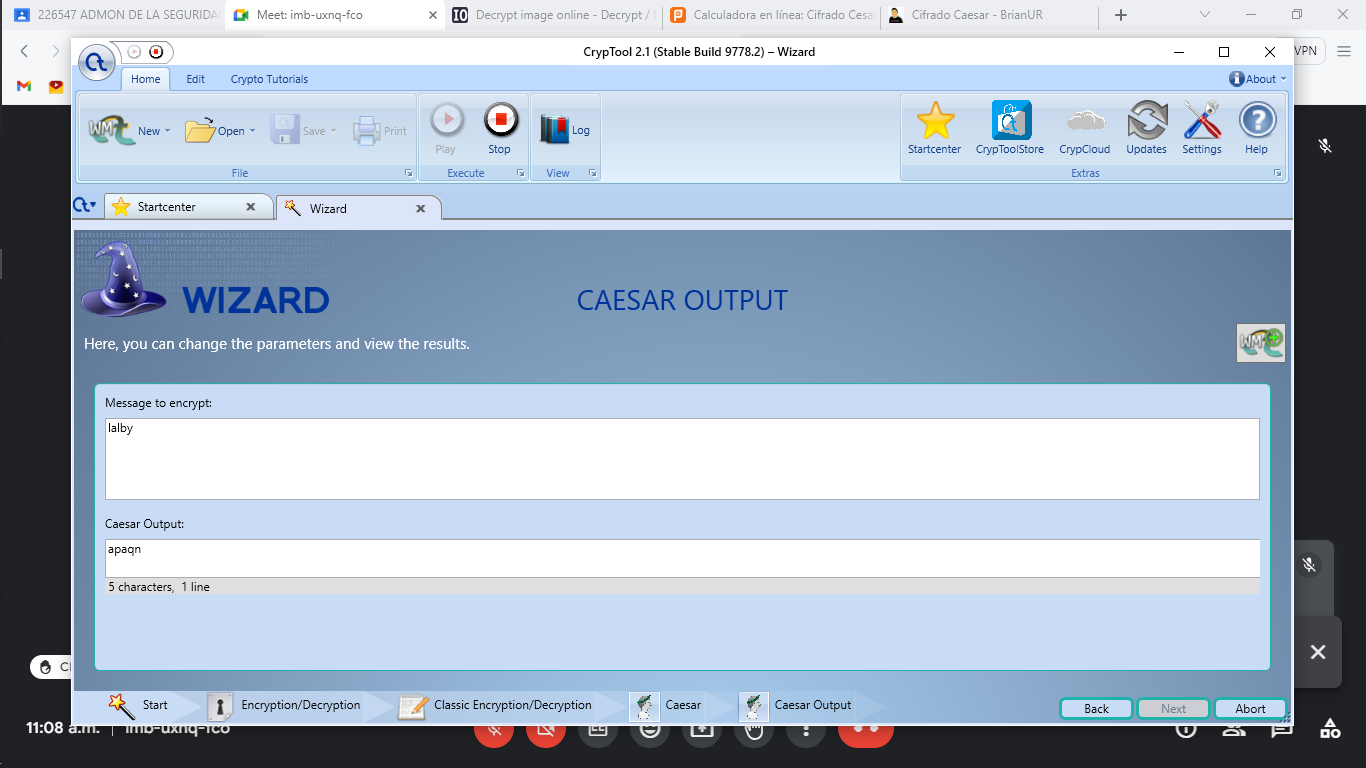
Desarrollo 1. Aplique algoritmo cesar a una frase de tipo ciberseguridad en clave 1 (posición 1 del alfabeto) NIVEL 1 de aplicación de ciberseguridad o protección de datos

“divide y venceras”

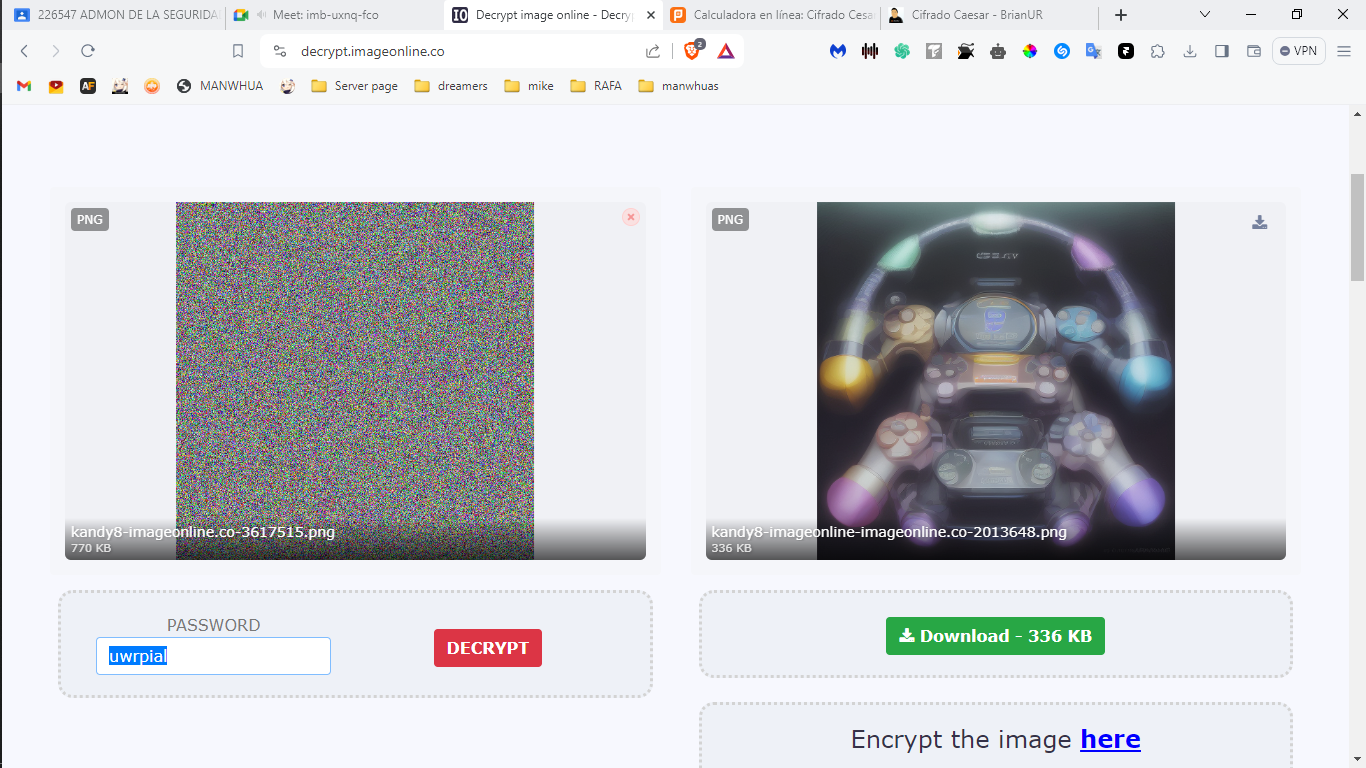
ejwjef z wfñdfsbt

desarrollo 2

descargue e instale la herramienta criptográfica CryptoTool (mensaje 500 algoritmos criptográficos tanto clásicos como modernos) y confirme el descifrado del ejercicio anterior



desarrollo 3. Encripte una imagen llamada imagen1crypto\_Bernal con password algoritmo clásico cesar, guardar y enviar a compañero de trabajo para que le desencripte

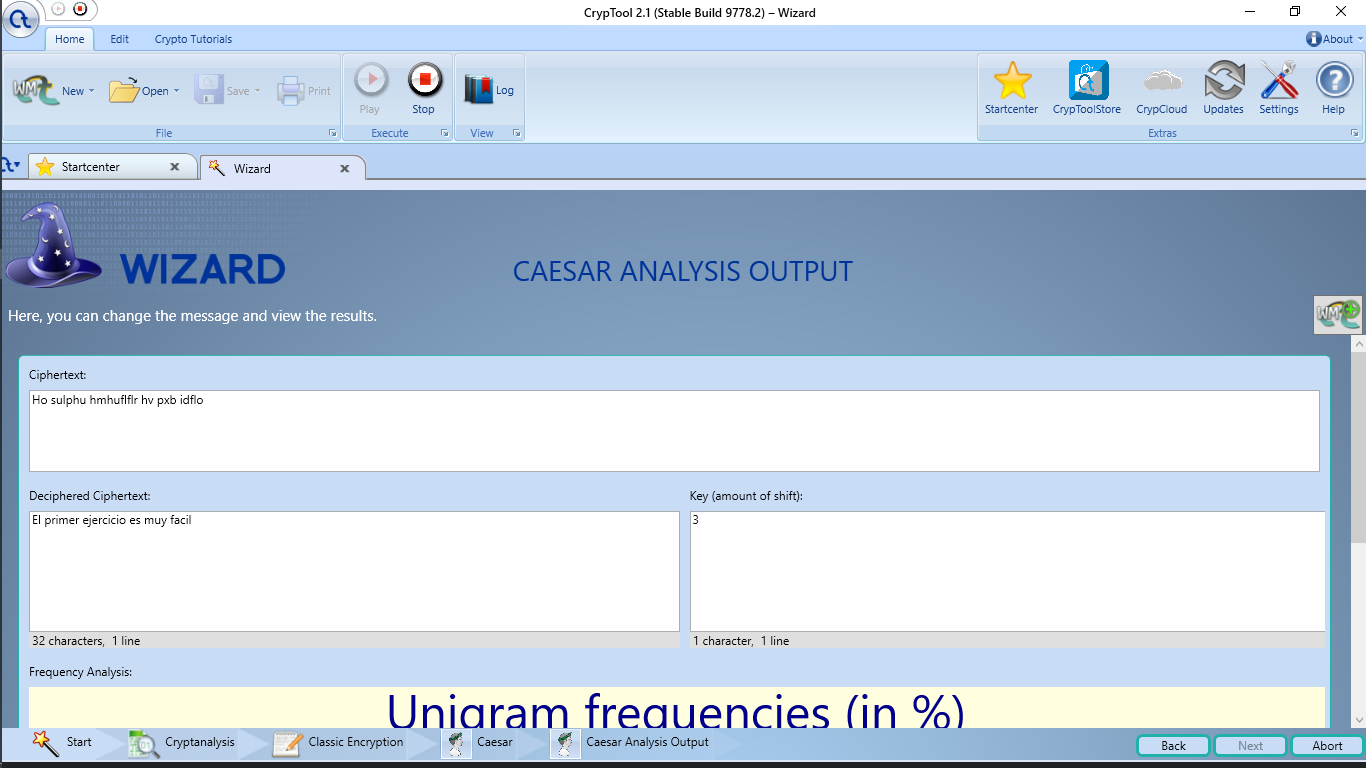


+0.2

DESARROLLO 4

Realice un cripto análisis del sig. Texto cifrado en algoritmo clásico e indique el numero de clave

+0.2



Conclusión

Uso de herramientas para tener una mayor seguridad y no sean accesibles fácilmente

SESION 5 1ER PARCIAL

Criptografía moderna

Objetivo: al finalizar la sesión el alumno identificara algunos algoritmos criptográficos modernos para el tratamiento de información segura

Las técnicas, estrategias, mecanismos que permiten ocultar de forma digital la información y datos se realizan mediante la criptografía modernos se dividen en:

1. Cifrado en flujo

El emisor usa un algoritmo moderno secreto (generar pseudoaleatorio) para generar secuencias binarias, hexadecimales con permutación y factorización. Realizando una misma operación para un descifrado, utiliza una clave.

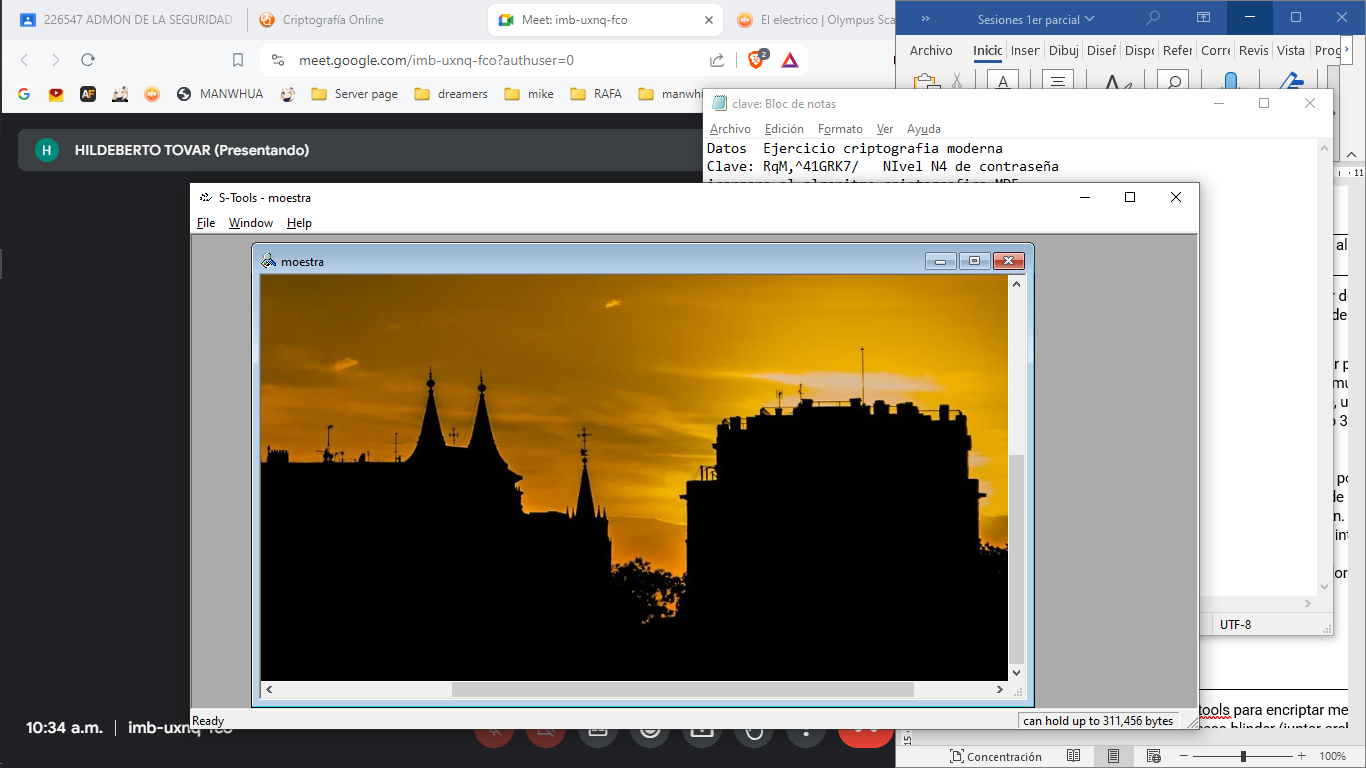
Ejemplo algoritmo DES estándar de datos encriptado 3DES, Algoritmo 4RC

1. Cifrado en bloque. La información y datos se dividen por secciones y en cada sección se aplicará un algoritmo criptográfico y puede ser en distintos componentes o elementos de envió de la información. Utiliza una clave para cifrar y descifrar IDEA (algoritmo de encriptación de datos internacional), algoritmo Rijndael

Algortimi por hash toma una cadena y regresa un valor de longitud MD% de 128 bits y SHA1, SHA2, SHA3, de 256 bits

1. Cifrado en llave
2. Cifrado por certificados

Desarrollo. Descargue la herramienta Stools para encriptar mensaje en texto (Frase célebre de ciberseguridad) y con el proceso blinder (juntar archivos) en una imagen tipo bmp adjuntar las imágenes y el texto seleccione el algoritmo IDEA



Desarrollo 2. En una imagen BMP guarde las definiciones de algunos autores de administración de seguridad informática

Suba ejercicios a tablón con sus datos precisos

Clave w4S\_=k86U6q=R|h

Password

cfd6f6c95313dd5e91e31b7180fcf69a

esteganografía el arte ocultar.

Aplicar el mismo procedimiento de ocultar la información en un texto clave

Ejemplo

Esta noche clara la luna esta radiante el punto es la plaza donde hay un festival a la media noche se presenta un cantante famoso donde su éxito mayor es huida y despedida con desesperación no olides nada.

Mensaje principal: esparase a a la medianoche en la plaza es punto de encuentro

Un archivo de texto guardarlo como esteganografiaBernal

Conclusión, final general

El uso de herramientas para encriptar con más de 1 método para que sea más difícil obtener los datos que han sido encriptados, uso de MD5 y esteganografía para una mayor seguridad

SESION 6 1ER PARCIAL

Objetivo: al finalizar la sesión el alumno identificara los elementos y componentes del algoritmo de cifrado IDEA para encriptación y generación de llaves

Consideraciones teóricas:

Rivest, Shamir y Adlman son los creadores del algoritmo RSA que factoriza números muy grandes a partir de divisiones sucesivas Sus aplicaciones principales para la administración de la seguridad informática son:

Encriptación

Desencriptación

Generación de llaves publicas (para diversos usuarios) y llaves privadas (de forma especial uno o varios usuarios selectos)

Firmado digital

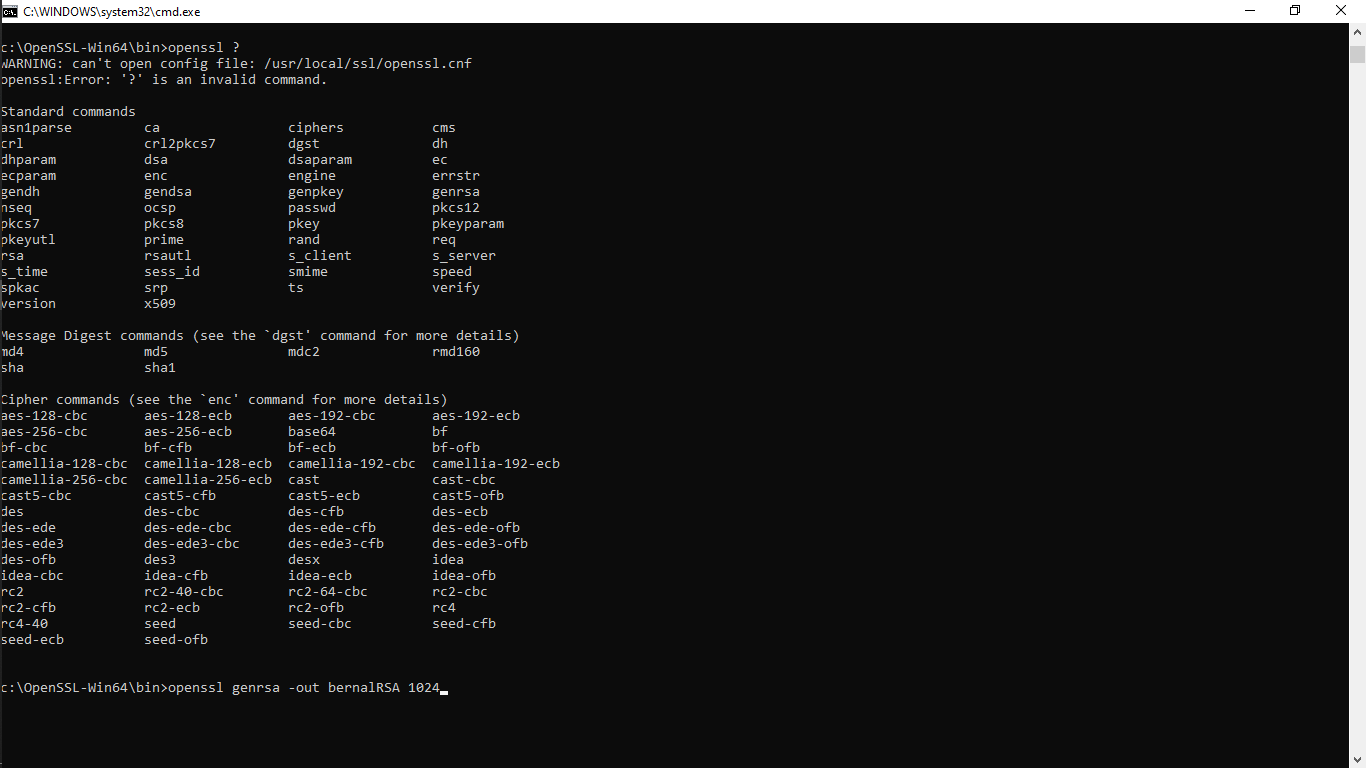
Certificados digitales

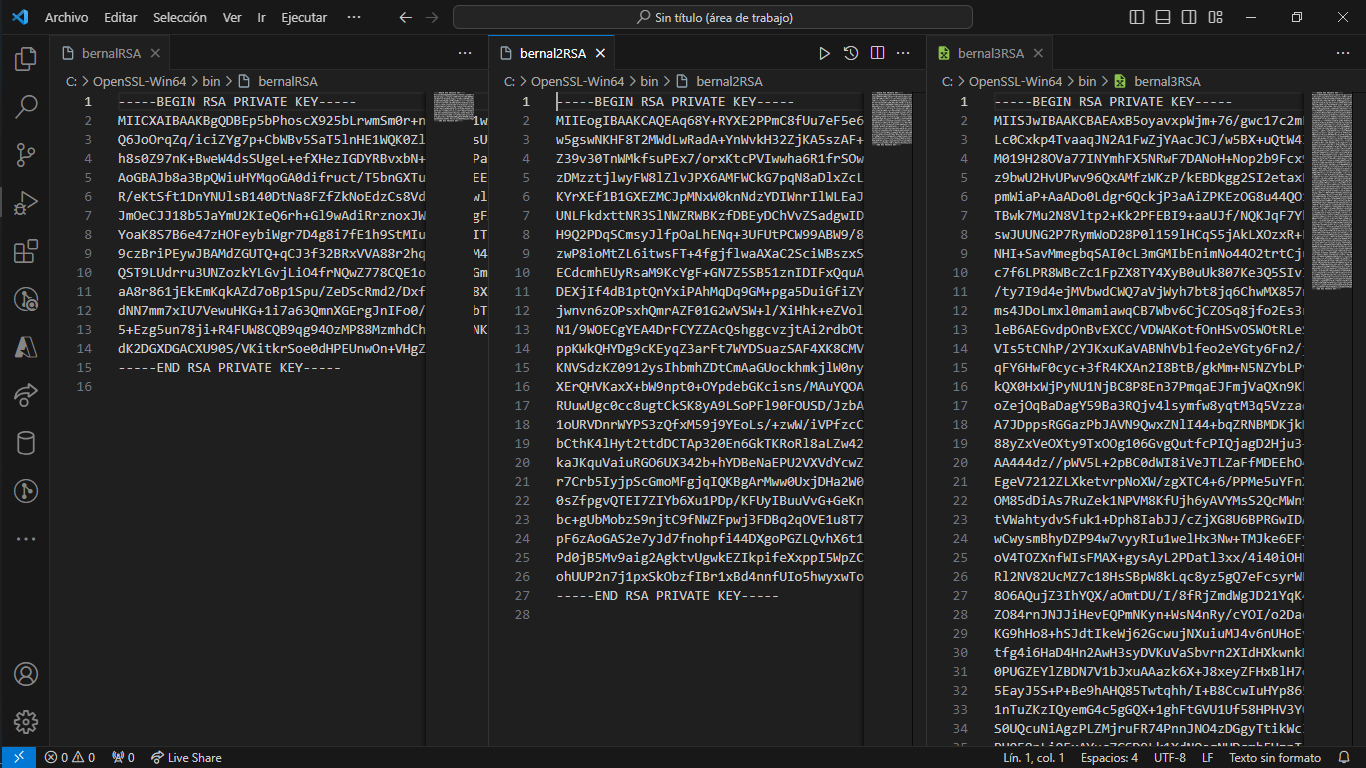
Su base es binaria por lo cal se puede tener en paridad de bits

256, 512, 1024, 2048, 4096 y mayores

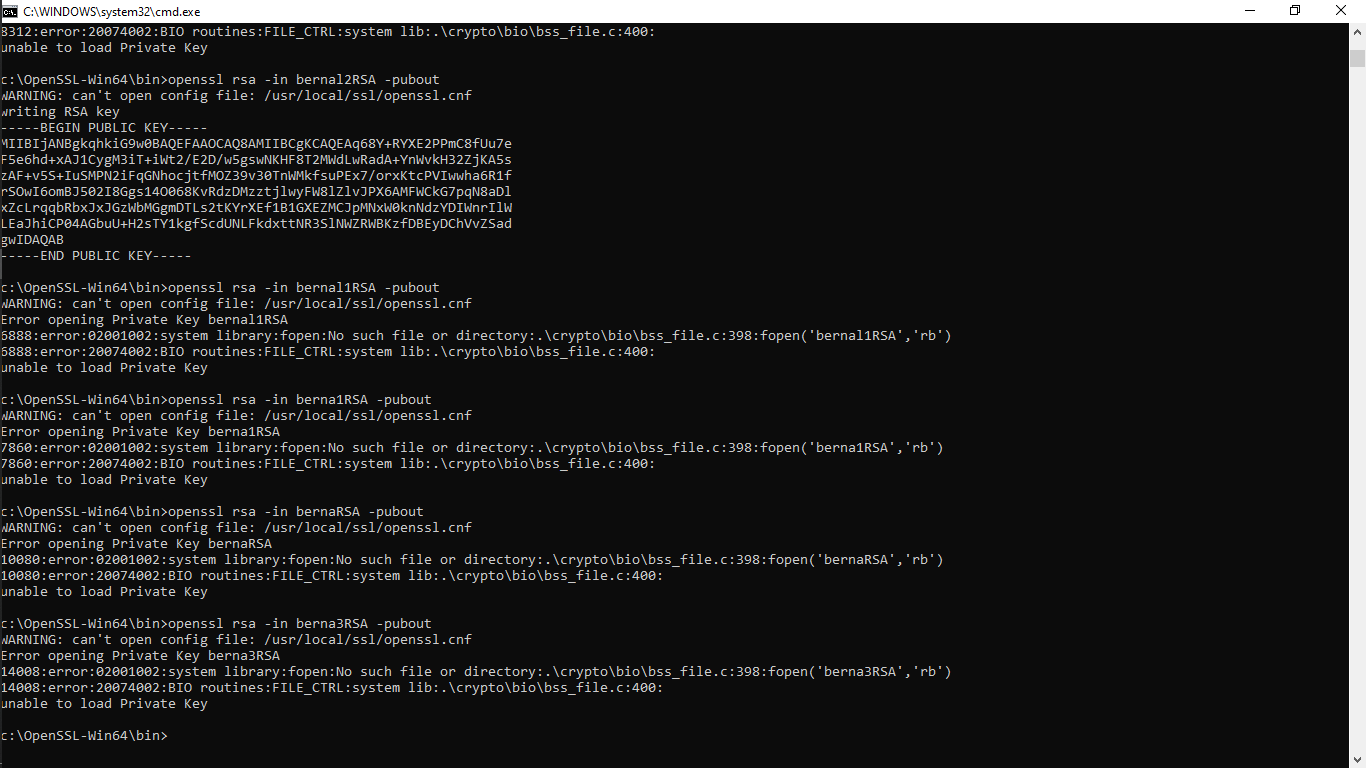
Desarrollo. Descargue Openssl para la generación de llaves RSA genere una de tipo publica y privada de 1024 bits, 2048 bits, 8192 bits

Definición de openSSL. Herramienta de código abierto que contiene un conjunto de funciones para la criptografía, toolkit para claves de cifrado RSA, firmas DSA, creación de certificados para páginas web x509, CRS, CRL SSL segurity socket layer y tls transport layer segurity



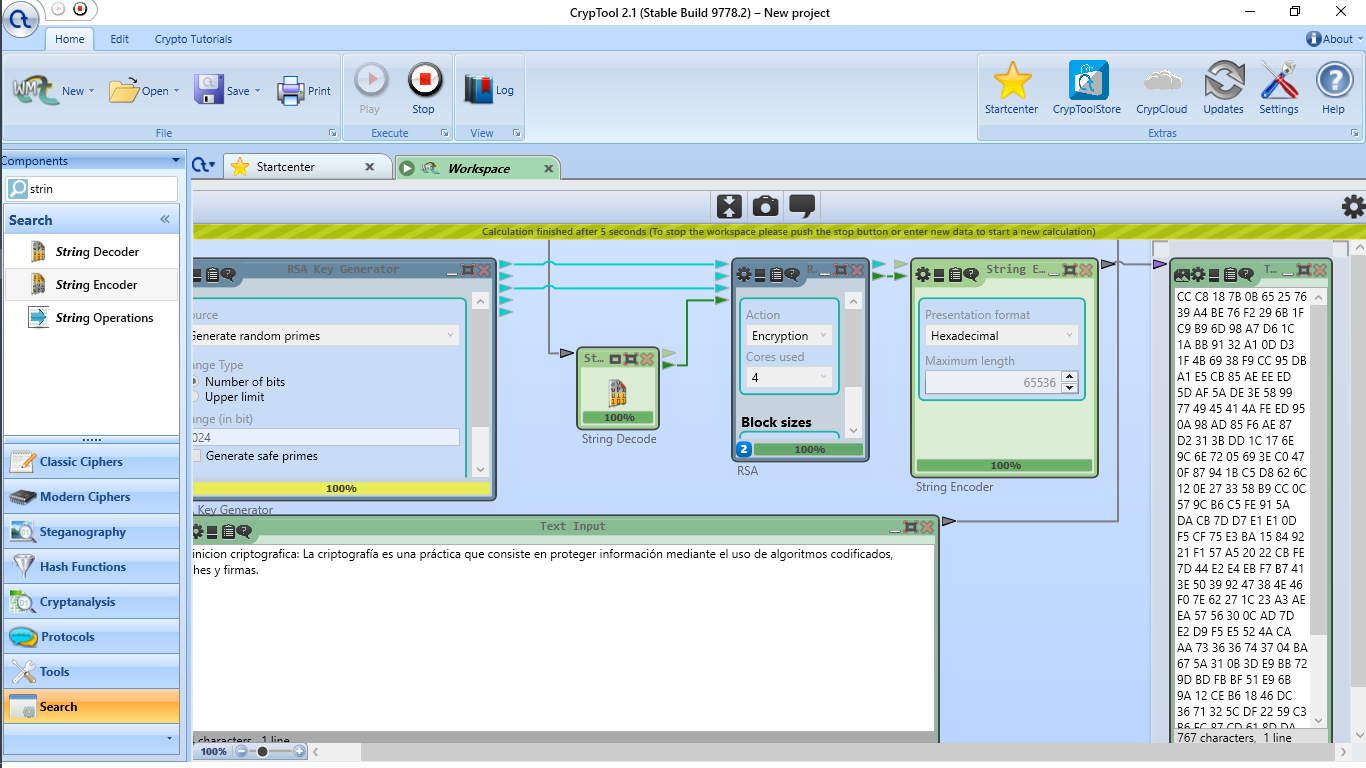


Desarrollo 1. Genere 2 llaves RSA de tipo publica y virtualice su estructura



Desarrollo 2. Genere 2 llaves RSA de tipo publicas y virtualice su estructura

Desarrollo 4 en la herramienta cryptool cifre la definición de criptografía, identifique todos sus componentes



Conclusión

Usar los correctos parámetros y funciones necesarias para su uso e implementación, así como los datos correctos a colocar en toda la actividad

SESION 7 1ER PARICAL

FIRMAS Y CERTIFICADOS DIGITALES

Al finalizar la sesión el alumno realizara firmas y certificados digitales x509 y DSA

Consideraciones teóricas: los certificados digitales apoyan a la administración de la seguridad informática a la cooficialidad. integridad. autenticación de mensajes, no repudio. Imprentado las siguientes acciones: Control de acceso, cifrar, descifrar, seguridad física, mecanismos de anonimato, auditoria y supervisión continua, monitoreo de actividades, demostración de la persona que genero la acción, solo la persona que firma puede reproducir sus acciones.

Una firma digital es el conjunto de procesos y técnicas de algoritmos criptográficos los cuales son emitidos po CA (Entidad certificadora) y llaves públicas y privadas.

Un estándar x509 define un formato de los certificados de clave publica sobre SSL/TLS con firmas digitales y cifrado. Los datos base son:

Para estado de ludan (localidad), organización, giro o ramo de la empresa o persona moral, dirección electrónica

DSA es otro estándar Algoritmo de Firma Digital estándar de gobierno Federal de USA o FIPS, algoritmo asimétrico (Ambas direcciones envía y recibe). Genera claves por medio de números primos, verificando por permutaciones

Desarrollo 1. Genere un Certificado x509 identificando y comentando sus procesos en cada uno de los comandos

Microsoft Windows [Versión 10.0.19045.3930]

(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\tekke>cd ..

C:\Users>cd ..

C:\>ls

"ls" no se reconoce como un comando interno o externo,

programa o archivo por lotes ejecutable.

C:\>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 3A17-36D2

Directorio de C:\

25/09/2023 10:25 a. m. <DIR> $WINDOWS.~BT

27/08/2023 05:54 p. m. <DIR> Autodesk

10/02/2024 04:57 p. m. <DIR> Certbot

02/10/2023 11:08 a. m. <DIR> Dev-Cpp

25/09/2023 11:12 a. m. <DIR> ESD

13/02/2024 01:09 p. m. <DIR> Intel

08/02/2024 10:06 a. m. <DIR> OpenSSL-Win64

07/12/2019 03:14 a. m. <DIR> PerfLogs

12/02/2024 12:03 a. m. <DIR> Program Files

12/02/2024 12:05 a. m. <DIR> Program Files (x86)

24/05/2023 07:21 p. m. <DIR> Users

25/01/2024 11:54 a. m. <DIR> Windows

24/05/2023 05:47 p. m. <DIR> Windows.old

14/06/2023 10:02 p. m. <DIR> xampp

0 archivos 0 bytes

14 dirs 45,912,354,816 bytes libres

C:\>cd OpenSSL-Win64

C:\OpenSSL-Win64>cd bin

C:\OpenSSL-Win64\bin>mkdir certificados

C:\OpenSSL-Win64\bin>cd certificados

C:\OpenSSL-Win64\bin\certificados>mkdir x509 dsa

C:\OpenSSL-Win64\bin\certificados>cd x509

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSL genrsa1024 > privatekey.pem

Invalid command 'genrsa1024'; type "help" for a list.

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSL genrsa 1024 > privatekey.pem

C:\OpenSSL-Win64\bin\certificados\x509>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 3A17-36D2

Directorio de C:\OpenSSL-Win64\bin\certificados\x509

13/02/2024 10:09 a. m. <DIR> .

13/02/2024 10:09 a. m. <DIR> ..

13/02/2024 10:10 a. m. 932 privatekey.pem

1 archivos 932 bytes

2 dirs 45,935,390,720 bytes libres

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSl req -new -key privatekey.pem -out csr.pem

Can't load ./.rnd into RNG

5C360000:error:12000079:random number generator:RAND\_load\_file:Cannot open file:crypto\rand\randfile.c:106:Filename=./.rnd

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:mx

State or Province Name (full name) [Some-State]:CDMX

Locality Name (eg, city) []:BJ

Organization Name (eg, company) [Internet Widgits Pty Ltd]:UIN

Organizational Unit Name (eg, section) []:EDUCATION

Common Name (e.g. server FQDN or YOUR name) []:www.uin.com

Email Address []:uin@uin.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:War034272@

An optional company name []:War034272@

C:\OpenSSL-Win64\bin\certificados\x509>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 3A17-36D2

Directorio de C:\OpenSSL-Win64\bin\certificados\x509

13/02/2024 10:29 a. m. <DIR> .

13/02/2024 10:29 a. m. <DIR> ..

13/02/2024 10:29 a. m. 1,024 .rnd

13/02/2024 10:29 a. m. 766 csr.pem

13/02/2024 10:10 a. m. 932 privatekey.pem

3 archivos 2,722 bytes

2 dirs 45,932,564,480 bytes libres

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSl x509 -req -days 365 -in csr.pem -signkey privatekey.pem -out public .crt

x509: Extra option: ".crt"

x509: Use -help for summary.

C:\OpenSSL-Win64\bin\certificados\x509>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 3A17-36D2

Directorio de C:\OpenSSL-Win64\bin\certificados\x509

13/02/2024 10:29 a. m. <DIR> .

13/02/2024 10:29 a. m. <DIR> ..

13/02/2024 10:29 a. m. 1,024 .rnd

13/02/2024 10:29 a. m. 766 csr.pem

13/02/2024 10:10 a. m. 932 privatekey.pem

3 archivos 2,722 bytes

2 dirs 45,939,888,128 bytes libres

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSl x509 -req -days 365 -in csr.pem -signkey privatekey.pem -out public.crt

Certificate request self-signature ok

subject=C=mx, ST=CDMX, L=BJ, O=UIN, OU=EDUCATION, CN=www.uin.com, emailAddress=uin@uin.com

C:\OpenSSL-Win64\bin\certificados\x509>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 3A17-36D2

Directorio de C:\OpenSSL-Win64\bin\certificados\x509

13/02/2024 10:39 a. m. <DIR> .

13/02/2024 10:39 a. m. <DIR> ..

13/02/2024 10:29 a. m. 1,024 .rnd

13/02/2024 10:29 a. m. 766 csr.pem

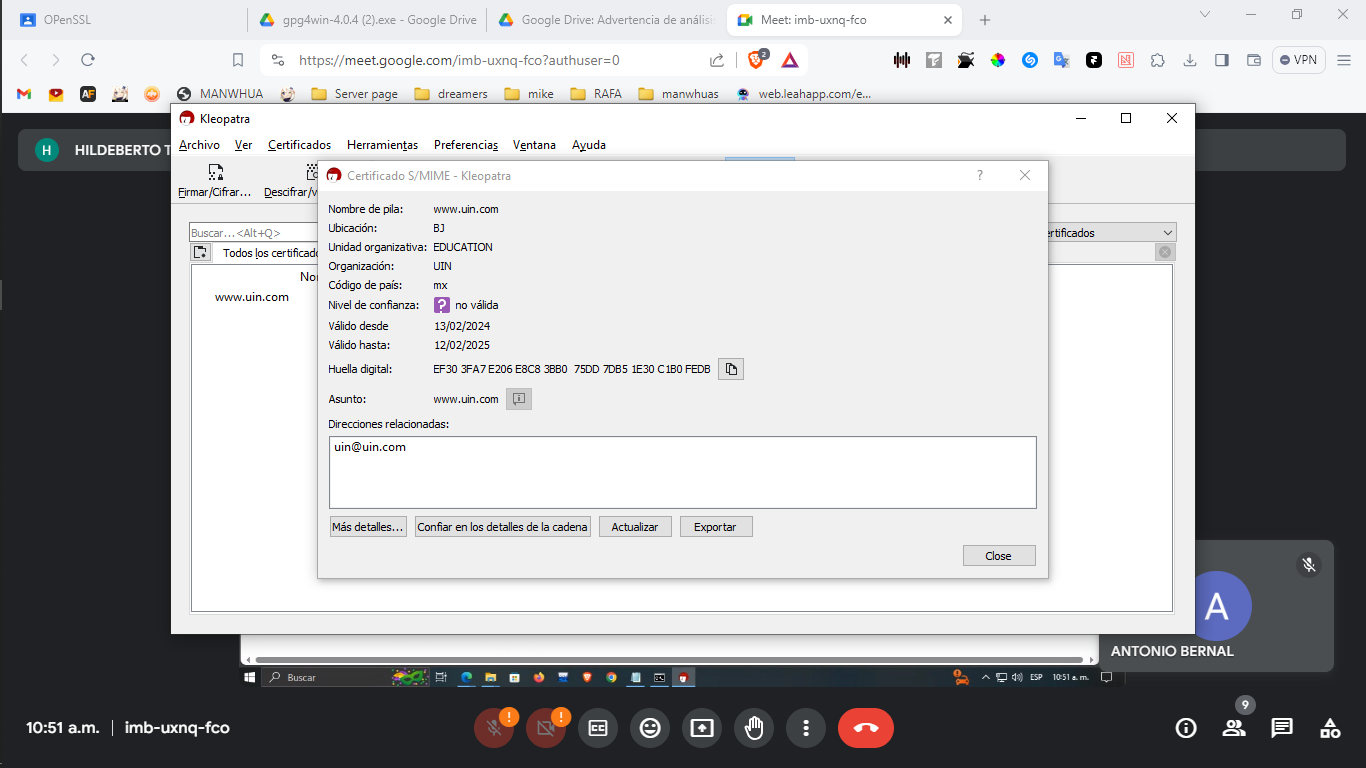
13/02/2024 10:10 a. m. 932 privatekey.pem

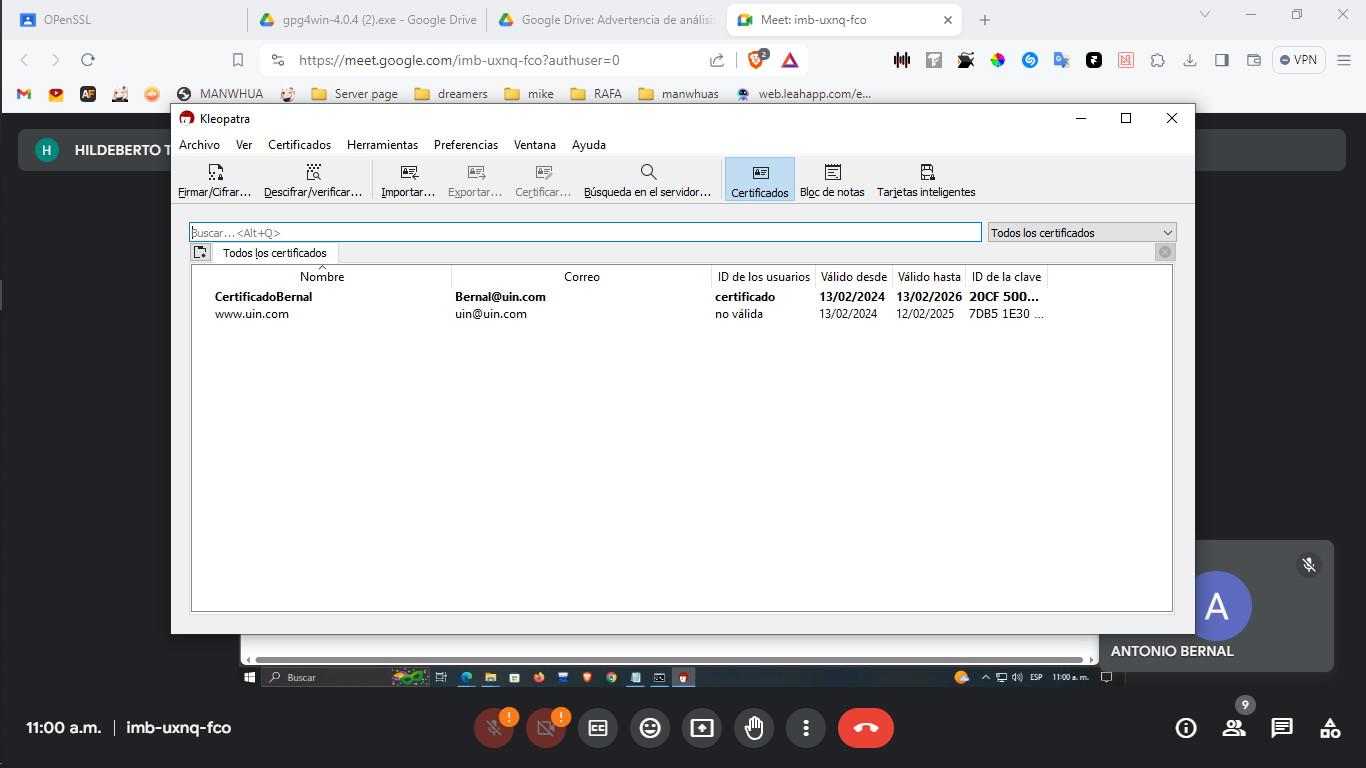
13/02/2024 10:39 a. m. 994 public.crt

4 archivos 3,716 bytes

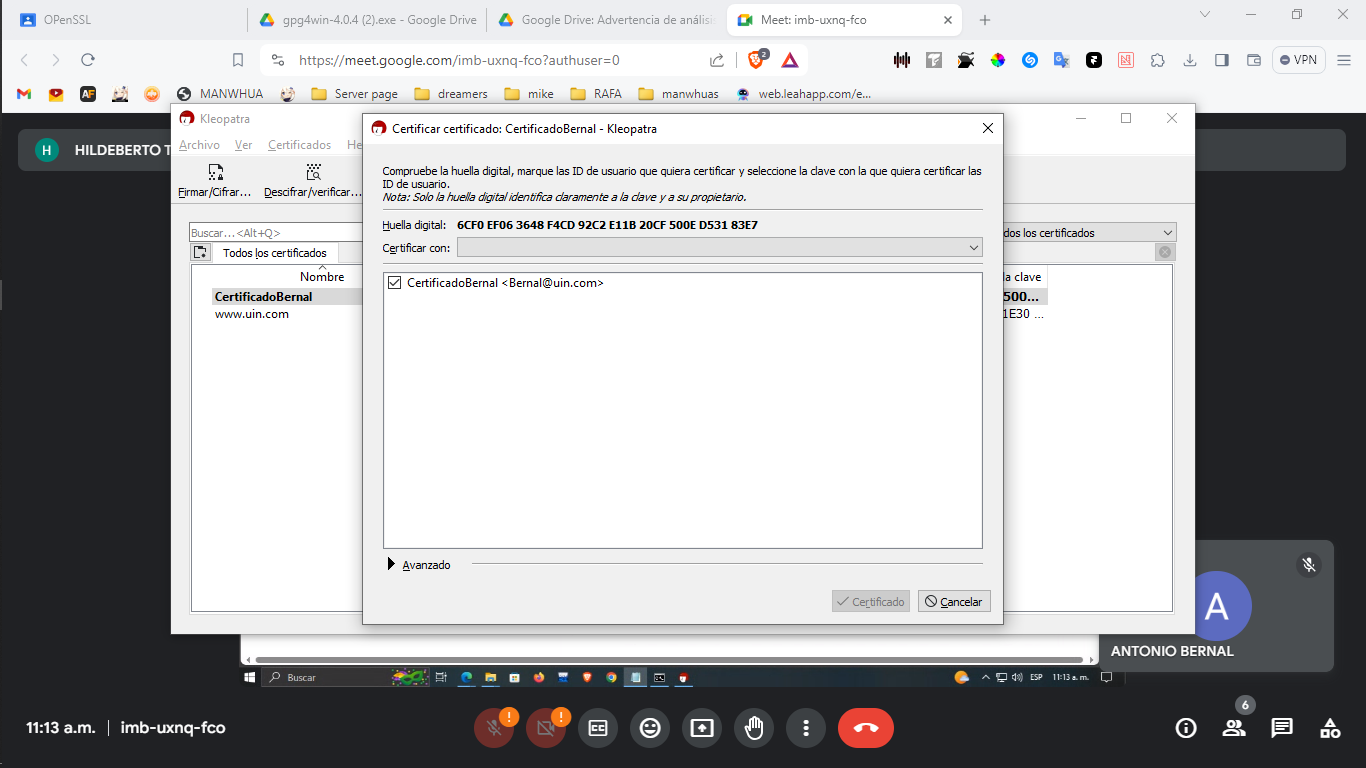
2 dirs 45,939,634,176 bytes libres

Desarrollo 2. Descargue e instale GPG y genere un certificado





Conclusión la generación claves de seguridad en 2 formas cleopatra y modo consola, el modo consola es más fácil ya que son 2 líneas de comando y con tener los archivos en la carpeta se puede hacer, en cambio en cleopatra tiene su ventaja de que es más intuitivo y fácil de usar



SESION 8 1ER PARCIAL

Desarrollo de aplicaciones seguras

OBJETIVO: al finalizar la sesión el alumno configurara y realizara pruebas en desarrollo de aplicaciones Java Web

Consideraciones teóricas.

OWAS Open Web Aplication Security Proyect

Es un proyecto de código abierto dedicado a determinar, combatir las causas que hacen que el software, aplicaciones, sistemas, programas sean seguros. Organismo internacional con las mejores prácticas, gestión de calidad de proyectos de software, enfocados principalmente al desarrollo web multiplataforma.

Para la administración de la seguridad informática determina los riesgos recabados en las sig. Áreas:

1.- Inyección. Los ataques de inyección ocurren cuando se envían datos desde formularios, archivos digitales con diversos formatos y con procesos ETL (explotación, transportación y carga de datos). Sobre bases de datos SQL (Oracle, Mysql, MarioBD, Infomix, SQL Server, PostgreSQL, BD2, BD1 BD2) relacionales y NO SQL (PostgreSQL, MondoBD, FireBird) Json OWASP minimiza los ataques de inyección.

2.- Autenticación rota. Fuga de datos, métodos inseguros GET

3.- exposición de datos duros, confidenciales

Exposición de información en el frond end de la aplicación y su almacenamiento visible en base de datos

4.- XXE Entidades XML Internas y externas

Referencia a códigos de etiquetas compuestas y simples de lenguaje extendido marcado

5.- pedidas de control de acceso

Validación desde base de datos vulnerables sin métodos criptográficos, contraseñas inseguras

6.- mala configuración de la seguridad

Excesivos controles, listas negras sin configuración y funcionamiento

7.- Scripting enter sites

Microcódigos, scripts añadidos por URL o inyección SQL, envíos de correos electrónicos, actividades de tareas del usuario

8.- deserialización no segura

Descargar datos de fuentes no confiables generando ataques DDOS ataques de inyecciones remotas, apis y platillas web

9.- componentes con vulnerabilidades

Código redundante no protegido, parches de seguridad, códigos no comprobados

10.- registro, supervisiones insuficientes

Mejoras no continuas, 3er día, actualizaciones sin verificación, análisis técnicos de profundo plan de mantenimiento en el ambiente de producción

Se implementarán para las áreas también de  
infraestructura de TI

Análisis de datos

Administración de proyectos seguros

Redes y comunicaciones seguras

Desarrollo 1. Descargue NetBeans web y genere un proyecto bajo servidor de aplicativos TomCat con

Usuario: Bernalowsap

Password: Encriptado shai >java1

455765d5eed19715f100e22ca54016e3034f8820031

SESION 9 1ER PARCIAL

Respaldos y repositorios de aplicación

Objetivo: al finalizar la sesión el alumno identificara el respaldo y almacenamiento de proyecto en la nube

Consideraciones teóricas

Los principios de la administración de la seguridad informática en base a los fundamentos ISO 27000 y OWASP nos indican realizar respaldos y repositorios de proyectos en infraestructura de TI, desarrollo de aplicaciones en producción, para tal propósito se tiene un software repositorios en la nube como GITHUB, BUTBUKET, CETRIX que permiten desde computadores centrales y locales trabajar un túnel SSL Segurity Socket Layer hasta repositorios de almacenamiento y respaldo en la nube.

Git es una terminal local en fragmento Linux con bibliotecas y núcleo de administración seguro SSH para ser el enlace puente en la nube de GITHUB plataforma de administración y control de proyectos e información

Desarrollo.

Genere un proyecto JAVA WEB particionado en 3 secciones, tipo responsivo-adaptativo (BootsTrap) y agregue este mismo proyecto a un respaldo repositorio en GITHUB