eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Sistemas de Gestión de Seguridad de la Información 2025/2026

Examen 1 Evaluación Continua

Realización

Entra en el ordenador de laboratorio en Ubuntu, con usuario **lsi** y contraseña **lsi**.

Rellena este documento mediante Libre Office y cámbiale el nombre al archivo, usando tu nombre y apellido separados por un guión bajo: **Nombre_Apellido_SGSSI.odt**. Sube el documento junto a los archivos necesarios en la entrega habilitada en eGela.

Después de la entrega:

Borra todo lo que hayas hecho en el ordenador y apágalo.

Mantén el servidor remoto en Google Cloud encendido hasta que aparezca una notificación en eGela para apagar todos los servidores.

Contenido

En las respuestas debes dar una explicación de lo que has hecho y cómo lo puede reproducir el profesor en su ordenador, indicando qué comandos ejecutar. Intenta ser lo más específico y claro posible, ya que el objetivo de la respuesta es que cualquier persona con un mínimo conocimiento técnico pueda recrear la respuesta en su equipo. No añadas información innecesaria como comandos para instalar herramientas o logs de sistema.

Si al copiar y pegar los comandos no funcionan la respuesta no se considerará válida.

Normas

Está totalmente prohibido y supondrá la expulsión del examen con una calificación de 0:

Usar cualquier tipo de herramienta de mensajería.

Usar ChatGPT o similares.

Visitar partes de eGela que no estén relacionadas directamente con el examen (Por ejemplo enunciados de laboratorios).

Usar documentación escrita de antemano por el alumno. Por ejemplo no se pueden usar documentos subidos previamente a GitHub que contengan listas de comandos.

Está permitido:

El uso de internet. Por ejemplo, para mirar información sobre comandos.

Usar programas creados por el alumno, siempre que se cumplan estas normas:

- Se alojan en GitHub/GitLab/Bitbucket/... con el usuario propio del estudiante, en un repositorio público.
- Se provee un enlace a ese repositorio.
- Tienen que funcionar al ejecutarlos y proveer el resultado que se pide.
- El programa no puede contener comentarios que sirvan para hacer el examen.
- **El programa no puede ser una lista de comandos. Tiene que tener un objetivo claro, único y específico, y solo realizable por un programa (El programa no puede ser un solo comando).**

Universidad del País Vasco Euskal Herriko Unibertsitatea

BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Sistemas de Gestión de Seguridad de la Información 2025/2026

Nombre y apellidos: Marco Lartategui Ugarte

Responde bajo la sección “RESPUESTA” de cada pregunta.

EJERCICIO 1 [1]

En el directorio **md5.zip** que se encuentra en eGela hay un archivo de **texto plano** con un mensaje importante cuyo Hash MD5 es **9e1cda999b728d2cd7c5ddb46a662522**. ¿Cuál es el mensaje? Incluye los comandos y/o programas que hayas usado.

RESPUESTA [0/1]:

El mensaje cuyo hash MD5 es **BL.md.** Primero, he tenido que descomprimir el zip y acceder al directorio extraído. Dentro, del directorio ya mencionado, el programa de terminal que he utilizado es md5sum. También he utlizado find y una tubería. Aquí está el resultado del comando:
find . -type f -exec md5sum {} \; | grep 9e1cda999b728d2cd7c5ddb46a662522

EJERCICIO 2 [1]

En el repositorio de apuntes de la asignatura hay una carpeta por cada tema (https://github.com/mikel-egana-aranguren/EHU-SGSSI-01). Dentro de la carpeta hay tres archivos: index.html, index.pdf, y index.html.md5sum. Además, en la raiz del repositorio hay un Shell Script con el código que se muestra a continuación. ¿Para qué sirve dicho Shell Script?¿Cómo usa las técnicas descritas en clase?¿Cuál es el resultado? (Shower es la librería JavaScript que usa el profesor para generar los apuntes: https://github.com/shower/shower)

```
#!/bin/sh

for dir in */
do
    if [ $dir != "ShowerTemplate/" ] && [ $dir != "Conferencias/" ]
    then
        proper_dir=${dir%/}
        m0=$(cat $PWD/$proper_dir/index.html.md5sum)
        m1=$(md5sum $PWD/$proper_dir/index.html  | cut -d' ' -f1)
        echo $m1 > $PWD/$proper_dir/index.html.md5sum
        if [ "$m0" != "$m1" ]; then
            shower pdf --cwd $PWD/$proper_dir -o $PWD/$proper_dir/index.pdf
        fi
    fi
done
```

RESPUESTA [0/1]:

...

EJERCICIO 3 [1]

Sistemas de Gestión de Seguridad de la Información 2025/2026

En tu servidor de Google Cloud, añade el siguiente contenido a la página web a la que se puede acceder mediante **HTTPS (Al acceder mediante HTTP tiene que redireccionar a HTTPS)**:

```
<h1>Examen 1 SEGURO - 831bdc94-a2a1-11f0-aae6-a3f788578463</h1>
<p>Nombre</p>
<p>Fecha</p>
```

Añade la siguiente información en la respuesta:

Dirección web (**ip** y **web** son específicos a tu servidor): https://ip/web

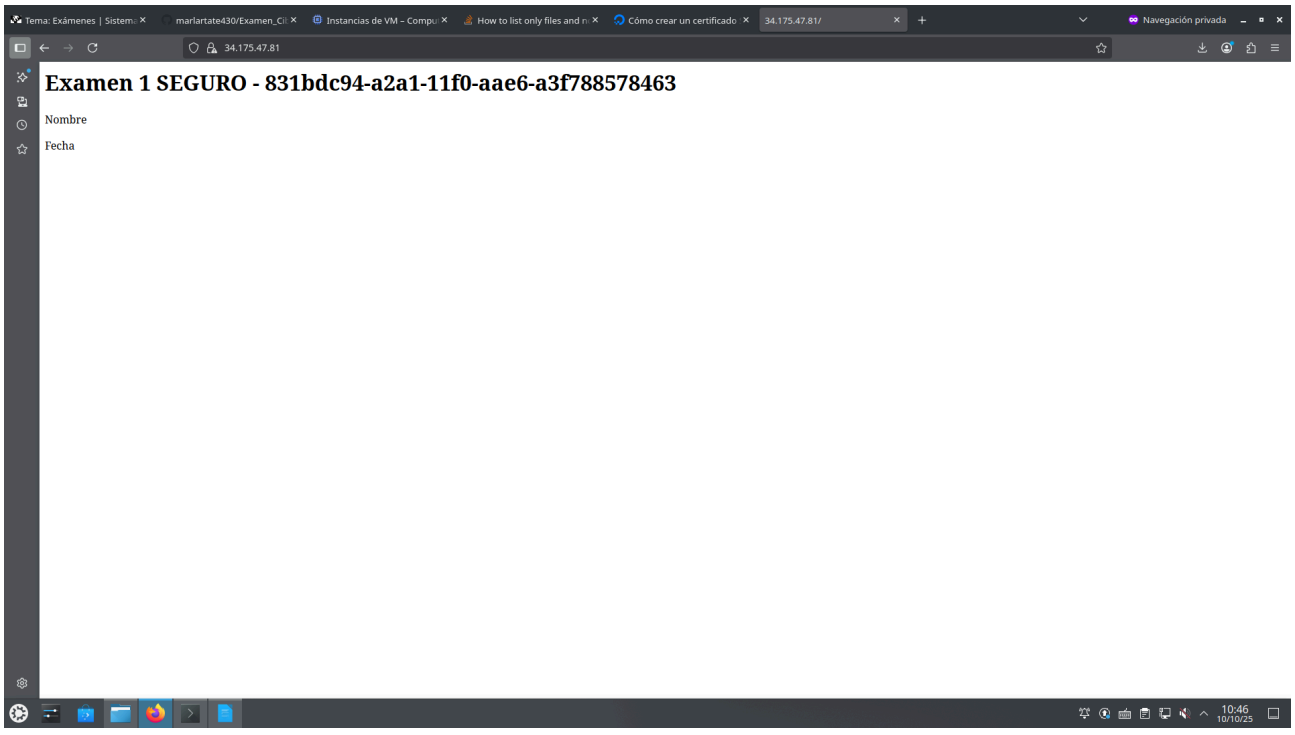
Captura de pantalla de la página web, en la que aparezca la URL.

Si al visitar la página aparece un error de certificado:

¿A qué se debe?

¿Cómo se puede solucionar?

RESPUESTA [0/1]:



https://34.175.47.81/

El error de certificado se debe a que es un certificado autofirmado y no está verificado por una Agencia de Certificación(AC) y tampoco está en la lista de certificados guardados en el navegador.

Se puede solucionar este problema obteniendo el certificado, que se encuentra en el servidor, y guardándolo en la colección de certificados del navegador.

Sistemas de Gestión de Seguridad de la Información 2025/2026

EJERCICIO 4 [1]

Descarga el siguiente archivo de GitHub:

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/blob/main/README.md

Fírmalo con tu clave GPG, y sube el archivo firmado a tu servidor Google Cloud, al directorio **/home/bgpegarm/**. El profesor debe bajarlo, desencriptarlo y comprobar la firma del archivo: ¿Qué pasos debe seguir?

RESPUESTA [0/1]:

sftp bgpegarm@34.175.47.81

get README.md.gpg

exit

gpg --decrypt README.md.gpg > resultado_readme.md

Al desencriptarlo verás un mensaje en pantalla de que la firma es correcta.

EJERCICIO 5 [1]

La clave de Paco (paco@gmail.com) que está en eGela (**Paco.asc**) tiene que aparecer como de confianza total (**[full]**) en el sistema GPG del profesor. Tienes que conseguir esto usando tu clave GPG, sabiendo que el sistema GPG del profesor estará configurado para tener confianza total en tu clave pública. Explica en la respuesta las instrucciones que tiene que seguir el profesor y añade los archivos necesarios.

RESPUESTA [0/1]:
gpg --import Pablo.asc
gpg --edit-key Pablo

trust Pablo

EJERCICIO 6 [1]

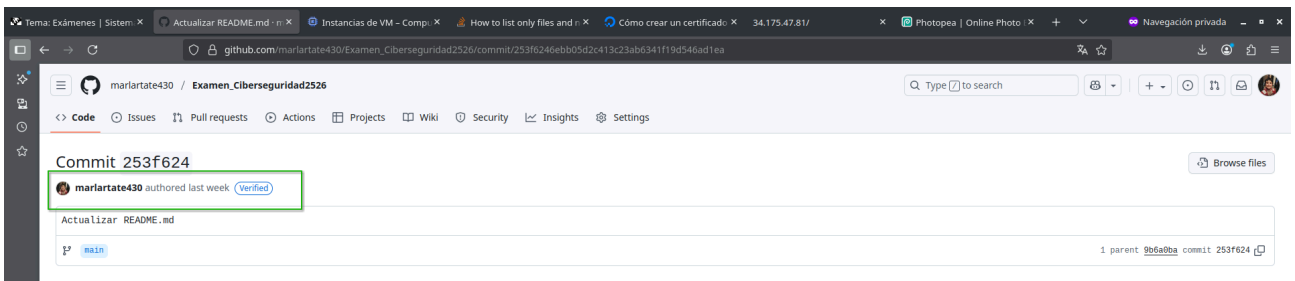
En un repositorio público de GitHub que uses tiene que aparecer un commit firmado por ti, con la palabra clave “Verified”, es decir firmado con tu clave GPG. Como respuesta, añade la URL del commit. Si el commit ya lo hiciste en el laboratorio, también es válido como respuesta. ¿Qué pasos tiene que seguir el profesor para verificar la firma del commit?

RESPUESTA [0/1]:

https://github.com/marlartate430/Examen_Ciberseguridad2526/commit/253f6246ebb05d2c413c23ab6341f19d546ad1ea

Los pasos que debe seguir el profesor son los siguientes:

Acceder al enlace y ver encima de la descripción del commit si pone la palabra verified, como lo



indica el rectángulo verde:

...

EJERCICIO 7 [1]

En el repositorio GitHub de apuntes de la asignatura, el siguiente commit esta firmado por el profesor:

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/commit/517b04879408606ab47c93119abbc5154e3e5537

Ha sido firmado por la clave privada asociada a la clave pública disponible en eGela **Mikel_Clave_Publica_GPG_GITHUB.asc**. ¿Como comprobarías la firma del commit? Describe los pasos y añade capturas de pantalla.

RESPUESTA [0/1]:

```
# En caso de tener la clave sin importar en GPG y situada en .
gpg --import Mikel_Clave_Publica_GPG_GITHUB.asc
git clone https://github.com/mikel-egana-aranguren/EHU-SGSSI-01
cd EHU-SGSSI-01/
git log --show-signature 517b04879408606ab47c93119abbc5154e3e5537
```

Sistemas de Gestión de Seguridad de la Información 2025/2026

```
commit 517b04879408606ab47c93119abbc5154e3e5537 (origin/release_25_26_2)
gpg: Firmado el lun 06 oct 2025 12:04:22 CEST
gpg:                usando EDDSA clave 1815AC43C4D0801522A4672A63E068D403BF4DEF
gpg: Firma correcta de "Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>" [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 1815 AC43 C4D0 8015 22A4  672A 63E0 68D4 03BF 4DEF
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Mon Oct 6 12:04:22 2025 +0200

    Release 25 26 2

commit 1cb431a6b82015c4355e444cd28d0a91f1479be5
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Mon Oct 6 11:51:58 2025 +0200

    rm test_sign

commit 6176ac9c479797c698b153c7750fa3e4421f445d
gpg: Firmado el mar 16 sep 2025 15:46:26 CEST
gpg:                usando EDDSA clave 1815AC43C4D0801522A4672A63E068D403BF4DEF
gpg: Firma correcta de "Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>" [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 1815 AC43 C4D0 8015 22A4  672A 63E0 68D4 03BF 4DEF
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Tue Sep 16 15:46:26 2025 +0200

    sign again?

commit 4a9bce0b6b11fdbfd82c3ac46a47c42094f1b07d
gpg: Firmado el mar 16 sep 2025 15:40:02 CEST
gpg:                usando EDDSA clave EDFE07159FB3BC26A99086B3E6DBECE68A62E856
gpg: Imposible comprobar la firma: No hay clave pública
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Tue Sep 16 15:40:02 2025 +0200

    test sign

commit 5945e2fb2988c921a3740fad59f77a0bf8328099 (origin/release_25_26_1)
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Fri Sep 5 11:15:54 2025 +0200

    Release 25 26 1

commit 9492929b0e3853609a3a499f134fe1cfaa2f072b
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Thu Sep 4 15:08:07 2025 +0200

    Semana 1

commit 92eae4b1285360e1501f6954501cc3837e926351
Author: Mikel Egaña Aranguren <mikel.egana.aranguren@gmail.com>
Date:   Thu Sep 4 10:16:02 2025 +0200
:
```

…

EJERCICIO 8 [1]

Sistemas de Gestión de Seguridad de la Información 2025/2026

Descarga de eGela:

El archivo firmado mediante GPG **MikelFirmado.gpg**.

La clave pública perteneciente al email mikel.egana@ehu.eus **Mikel_Clave_Publica_GPG.asc**.

Comprueba la firma del archivo y responde:

Describe los pasos que has seguido, y los resultados de cada uno.

¿La firma es **correcta** y de **confianza**?

RESPUESTA [0/1]:

Describe los pasos que has seguido, y los resultados de cada uno.

gpg --import Mikel_Clave_Publica_GPG.asc

No hay resultado

gpg --decrypt MikelFirmado.gpg > resultado.txt

gpg: Firmado el lun 06 oct 2025 11:23:04 CEST

gpg: usando EDDSA clave EDFE07159FB3BC26A99086B3E6DBECE68A62E856

gpg: emisor "mikel.egana@ehu.eus"

gpg: Firma correcta de "Mikel Egaña Aranguren (Github?) <mikel.egana@ehu.eus>" [desconocido]

gpg: alias "Mikel Egaña Aranguren <mikel.egana@ehu.eus>" [desconocido]

gpg: WARNING: The key's User ID is not certified with a trusted signature!

gpg: No hay indicios de que la firma pertenezca al propietario.

Huellas dactilares de la clave primaria: EDFE 0715 9FB3 BC26 A990 86B3 E6DB ECE6 8A62 E856

¿La firma es **correcta** y de **confianza**?
La firma sí es correcta, pero no de confianza. Tampoco se sabe si la clave es de la persona que aparece en la clave, no hay validez.

EJERCICIO 9 [1]

Crea un archivo llamado **Ejercicio9.md** que contenga:

```
# Ejercicio 9

* **Nombre**: tu_nombre

* **Fecha**: fecha_actual
```

Mediante GPG, fírmalo para que el profesor pueda verificar tu firma, y cífralo para que solo el profesor lo pueda leer. Indica en la respuesta los pasos que tiene que seguir el profesor para descifrarlo y verificar la firma, adjuntando cualquier archivo necesario en la entrega de eGela.

Sistemas de Gestión de Seguridad de la Información 2025/2026

RESPUESTA [0/1]:

gpg --decrypt Ejercicio9.md.gpg

…

Al desencriptarlo aparecera un mensaje por pantalla sobre quién a firmado el archivo.

EJERCICIO 10 [1]

Sube el archivo **1017d7ea-a2a9-11f0-aea5-8fdf51dfad9d**, disponible en eGela, al servidor remoto Google Cloud, al directorio **/home/bgpegarm/**. Como respuesta, escribe la IP del servidor.

RESPUESTA [0/1]:

34.175.47.81

…