# DESAFÍO 16 - SEGURIDAD EN LINUX: SERVER HACKING

## OBJETIVO

Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) para una organización que aloja aplicaciones en la nube.

Desplegar un conjunto de controles de seguridad que incluyan medidas técnicas, organizativas y de gestión para reducir los riesgos asociados con el alojamiento de aplicaciones en la nube.

Incorporar un plan de continuidad del negocio, que permita recuperar los servicios en caso de desastres naturales o fallas en la infraestructura.

El SGSI será diseñado para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para cumplir con las normativas y estándares de seguridad aplicables.

## LINUX

Objeto de estudio: Sistema operativo + web server + base de datos.

1. Implementar un programa completo del ciclo PDCA que contenga al menos dos aspectos de seguridad y desarrollar, un objetivo o más, en cada aspecto de seguridad seleccionado (en total, 2 objetivos a desarrollar):
    a. Identificación y autentificación.
    b. Autorización.
    c. Integridad.
    d. Auditoría.

    **CONSIDERACIONES**

    - **Planificar**: Elaborar un “plan estandarizado” para aplicar a futuros despliegues. Esto incluye la identificación de un problema, una oportunidad de mejora o la creación de un plan de acción para abordarlo.
    - **Do** (**Hacer**): Implementar y documentar las tareas a realizar según lo planificado. Realizar un paso a paso que incluya ficheros de configuraciones, instalación de paquetes, capturas de pantallas, y otros.
    - **Check**: Realizar una verificación de las tareas realizadas en la etapa “*Do*”. Indicar, al menos, 2 puntos a mejorar incluyendo

aspectos que no se hayan tenido en cuenta en la etapa de “planificar”.

- **Actuar**: Elaborar un checklist para futuros despliegues de la imagen seleccionada, que incluya aspectos resultantes de la etapa “*check*”.

## GITHUB

1. Publicar la documentación en un *readme* de su repositorio personal.

Es importante que se trabaje el *readme* del repositorio (incluso pueden agregar un *readme* por carpeta con más información para probar cada parte de este).

El objetivo es que una persona pueda visualizar su repositorio y testear (es decir, probar todo en conjunto y también cada una de las partes por separado).

## MODALIDAD DE TRABAJO

En el archivo, documentar lo siguiente:

- Comandos.
- Capturas de pantalla que respaldan la documentación.
- Problemas que se presentaron, pasos a seguir para encontrar la solución, etc.

Además, el documento debe tener una portada, datos personales y titulo del desafío.

## ENTREGABLE

Los documentos son almacenados en la carpeta compartida que tienen en *Google Drive* con el formato:

<carpeta con su nombre>/<Fase>/<desafío>/archivo.

Por ejemplo, el instructivo se debe almacenar en la carpeta compartida con el nombre del alumno, en una carpeta llamada Fase 4, dentro debe tener otra carpeta llamada Desafío 17 y, por último, almacenar dentro de ella todos los archivos relevantes a este desafío.

Se esperan los siguientes archivos:

- Instructivo.

- Enlace del repositorio de código donde publican los archivos creados (dentro del instructivo).
- Archivos adicionales.

Recuerden seguir las instrucciones para los entregables.

## CONSEJOS

- No hace falta crear la imagen como resultado final, solo centrarse en crear el informe PDCA desde los aspectos de seguridad seleccionados.