# U1. Fundamentos de la seguridad informática

Descargar estos apuntes

# Índice



# Diseño de un CPD

## Objetivo

Comprender los conceptos básicos de la norma ANSI/TIA 942 para el diseño de centros de datos y aplicarlos a un caso concreto.

## Descripción de la tarea

Diseña un pequeño CPD para una empresa. El equipamiento que necesita alojar el centro incluye:

- Un rack con un servidor.
- Un switch de planta y su correspondiente patch panel.
- Una unidad NAS.
- Un SAI.

## Fases

### Primeros pasos

Mira el siguiente vídeo *Google data center*.

### Conceptos básicos de ANSI/TIA 942

Abre el fichero `diseñoCPD_01file.pdf` y completa los diagramas.

### Diseña tu CPD

Crea un esquema del CPD basado en ANSI/TIA-942 que incluya:

- Disposición de los equipos y de la infraestructura de red.
- Infraestructura eléctrica y de refrigeración.
- Medidas de seguridad física y lógica (tipos de medidas de control de acceso, sistema de extinción de incendios, SAI, etc.).

Crea un nuevo **documento de texto** que incluya:

- Esquema del CPD que has creado.
- Razonamiento de las decisiones tomadas durante el diseño del CPD.

> ⚠ **"Recuerda"**
>
> El equipamiento que necesita alojar el centro incluye:
>
> - Un rack con un servidor.
> - Un switch de planta y su correspondiente patch panel.
> - Una unidad NAS.
> - Un SAI.

## Duración

- 4 horas

## Entrega

Sube el documento de texto en PDF a Aules.

## Evaluación

Los conocimientos y habilidades adquiridas se evaluarán mediante el documento de texto entregado.

- **Documento de texto [0-10]**:
  - Esquema del CPD creado [0-5]
  - Razonamiento de las decisiones tomadas durante su diseño: [0-5].

# Política de contraseñas

## Objetivo

Reconocer la importancia de utilizar contraseñas seguras y aprender a definirlas, configurarlas y gestionarlas eficazmente.

## Tarea

La seguridad en las contraseñas sirve como primera línea de defensa contra los ciberdelincuentes que buscan el acceso no autorizado a los datos. La creación de contraseñas fuertes y seguras reduce el riesgo de que los ciberdelincuentes las adivinen y accedan a datos sensibles.

- Evalúa tus contraseñas.
- Gestiona tus contraseñas.
- Descifra contraseñas.

## Fases

### Evalúa tus contraseñas

- Busca un incidente de seguridad reciente y completa una tabla como la siguiente.
- Piensa en las contraseñas que usas habitualmente.
- Comprueba su seguridad en este sitio web.
- Experimenta con diferentes contraseñas para entender qué las hace más seguras. Prueba combinaciones de palabras, números, contraseñas cortas y largas, añade símbolos y utiliza mayúsculas para sacar tus propias conclusiones. Resume las conclusiones a las que hayas llegado.
- Reemplaza tus contraseñas habituales por *passphrases* y verifica su seguridad. Resume tu conclusión.
- Las contraseñas se almacenan en archivos cifrados protegidos. Sin embargo, una fuga de datos puede dejarlas al descubierto. Comprueba en https://haveibeenpwned.com si alguna de tus contraseñas o direcciones de correo electrónico se han visto comprometidas.
- Incluso si tus contraseñas no han sido expuestas, deberías cambiarlas inmediatamente si coinciden con alguna de las mencionadas en este artículo.
- Un gestor de contraseñas te permite utilizar contraseñas complejas de forma segura. Utiliza el gestor de contraseñas de Google y explora su herramienta **Password Checkup**, que proporciona información sobre la seguridad de tus contraseñas, indicando si hay duplicados o fugas. Haz una captura de pantalla de la herramienta. ¿La consideras segura? ¿Puedes mencionar otro gestor de contraseñas?

### Gestiona tus contraseñas

- Las políticas de contraseñas obligan a los usuarios a considerar contraseñas complejas, difíciles de adivinar.
- Establece 4 políticas de contraseña en tu sistema Linux y pruébalas. Captura tu archivo final.
  *Recurso: Políticas de contraseña en Linux.*

- Configura la expiración de la contraseña de un usuario específico utilizando el comando `chage`. Incluye una fecha de expiración, un número máximo de días, y un período de advertencia (opciones `-E`, `-W`, `-M`, `-l`). Verifica tu configuración.
  *Recurso: https://manpages.ubuntu.com/manpages/focal/en/man1/chage.1.html*
- El comando `chage` se centra en un usuario específico, pero ¿en qué archivo puedes configurar estas restricciones para todos los usuarios? Consulta este sitio web para más información. Verifica tu configuración.
- Configura una política de contraseñas en un sistema Windows y captura la ventana de configuración.
- Verifica que estas políticas están activas intentando cambiar la contraseña de un usuario con contraseñas que no cumplan con las restricciones aplicadas.
- Considera las opciones proporcionadas por ambos sistemas y sus implicaciones prácticas: ¿cuál parece más versátil, efectiva y fácil de configurar? Justifica tu respuesta.

---

## Descifra contraseñas: John the Ripper

- Agrega los siguientes usuarios y contraseñas a tu sistema: