**PORTADA**



**HARDERING DE WINDOWS SERVER 2022**

(En entorno empresarial)

**Nombre del alumno o de la alumna: Valentin Cuellar Sanchez**

**Curso académico: ASIR 2do ONLINE**

**Tutora/Tutor del proyecto: Luis Miguel Pacheco**

**ÍNDICE PAGINADO**

1. **JUSTIFICACIÓN DEL PROYECTO**

La razón por la cual he elegido esta temática para el proyecto es porque considero que la \*\*securización de servidores\*\* es un aspecto fundamental e \*\*imprescindible\*\* para cualquier tipo de empresa, ya sea pequeña, mediana o grande. En un entorno empresarial actual, donde las \*\*amenazas cibernéticas\*\* son cada vez más frecuentes y sofisticadas, garantizar la seguridad de los sistemas y los datos se ha convertido en una \*\*prioridad crítica\*\*.

En este proyecto, nos centraremos en la \*\*securización de un servidor Windows Server 2022\*\*, una plataforma ampliamente utilizada en el ámbito corporativo debido a su escalabilidad, rendimiento y capacidades avanzadas de gestión. La elección de este sistema operativo se debe a su relevancia en entornos empresariales, donde la protección contra intrusiones, malware y accesos no autorizados es esencial para mantener la \*\*continuidad del negocio\*\* y el \*\*cumplimiento normativo\*\*.

Además, la implementación de medidas de seguridad robustas no solo ayuda a prevenir \*\*ataques externos\*\*, sino que también mitiga riesgos internos, como fugas de información o configuraciones erróneas que puedan comprometer la integridad del sistema. Entre los aspectos clave que abordaremos se incluyen:

* Hardening del sistema: Aplicación de políticas de seguridad estrictas y desactivación de servicios innecesarios.
* Gestión de usuarios y permisos: Implementación de principios como el mínimo privilegio para reducir posibles vectores de ataque.
* Protección contra malware: Instalación y configuración de soluciones avanzadas de seguridad.
* Actualizaciones y parches: Mantenimiento del sistema siempre actualizado para corregir vulnerabilidades conocidas.
* Monitorización y registro de eventos: Configuración de herramientas de logging para detectar actividades sospechosas en tiempo real.

Este proyecto no solo tiene un enfoque técnico, sino también estratégico, ya que una infraestructura segura contribuye a la \*\*confianza de los clientes\*\*, el \*\*respaldo legal\*\* y la \*\*eficiencia operativa\*\* de la empresa. Al finalizar, se habrá establecido un entorno más resistente a ciberamenazas, asegurando la disponibilidad, confidencialidad e integridad de los datos corporativos.

En definitiva, la securización de servidores no es un lujo, sino una \*\*necesidad empresarial\*\* en un mundo digital donde los riesgos evolucionan constantemente. Este proyecto busca proporcionar las bases para un despliegue seguro y confiable de Windows Server 2022, adaptado a las demandas actuales de ciberseguridad.

1. **INTRODUCCIÓN**
2. **OBJETIVOS**
   1. OBJETIVO GENERAL
   2. OBJETIVOS ESPECÍFICOS

**4. DESARROLLO**

* 1. FUNDAMENTACIÓN TEÓRICA: lo que vamos a hacer, procedimientos, resolución de la hipótesis o situaciones planteadas, tareas a realizar
  2. Materiales y métodos: estrategias de búsqueda, metodología y técnicas utilizadas
  3. Resultados y análisis

**5. CONCLUSIONES**

**6. LÍNEAS DE INVESTIGACIÓN FUTURAS**

**(No son obligatorios, pero pueden aparecer)**

**7. BIBLIOGRAFÍA**

**8. ANEXOS**

**9. OTROS PUNTOS**

**(No son obligatorios, pero pueden aparecer)**

* Aportaciones personales
* Retos profesionales
* Restos personales
* Agradecimientos