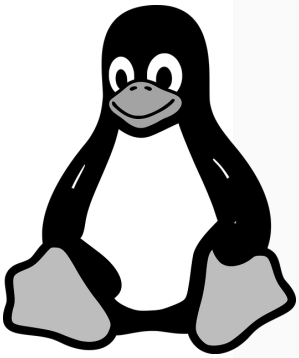
INSTITUTO NEBRIJA | Formación Profesional

“Infraestructura Dual: Comparativa e Implantación de entornos Windows y Linux en una organización”



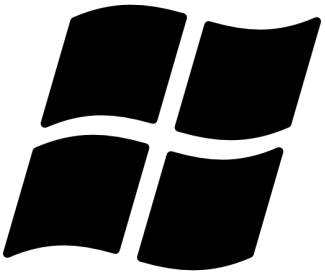
Integrantes: Manuel Pérez, Cristian Guerrero, Victor García, Alberto Rodero

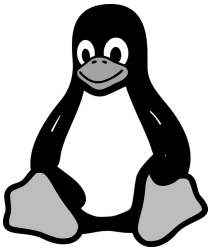
Curso académico: Implantación de Sistemas Operativos

Tutora/Tutor del proyecto: Carmelo Escribano López

Enlace a vuestro repositorio de GitHub:
https://github.com/Kris0121/ISO-2025

ÍNDICE PAGINADO





1.JUSTIFICACIÓN DEL PROYECTO

La empresa farmacéutica en cuestión cuenta con una trayectoria sólida en la fabricación y comercialización de medicamentos, pero presenta un grave retraso tecnológico. Con 120 empleados distribuidos en distintas áreas (producción, I+D, administración, comercial, etc.), la empresa opera actualmente de forma completamente manual:

Toda la documentación es en papel: desde la producción hasta las nóminas, pedidos y registros de laboratorio.

No existe red interna: no hay servidores, ni ordenadores conectados entre sí, ni acceso a bases de datos compartidas.

No hay sistema operativo estandarizado: los pocos ordenadores disponibles son antiguos, sin actualizaciones ni gestión centralizada.

No tienen backups ni medidas de ciberseguridad activas, lo que pone en riesgo la integridad de su información.

2. MAQUETACIÓN

La maquetación propuesta establece una estructura clara y escalable para la implementación de los sistemas operativos y la red corporativa de la empresa farmacéutica. Se segmenta por departamentos y se asigna un sistema operativo específico según las necesidades funcionales.

Preparar ISOs maquetadas (preconfiguradas) con:

El sistema operativo correspondiente (Windows o Linux).

Software necesario según el departamento.

Configuraciones de red base (nombre del equipo, dominio, etc.)

Configuración de la seguridad de los equipos

3.OBJETIVOS

A. OBJETIVO GENERAL:

Modernizar integralmente la infraestructura tecnológica de la empresa farmacéutica mediante la implementación de un sistema digitalizado y automatizado que permita optimizar los procesos operativos, mejorar la gestión documental, incrementar la eficiencia en la comunicación interna y garantizar la seguridad y protección de la información, contribuyendo así a la competitividad y sostenibilidad de la empresa en el mercado.

B. OBJETIVOS ESPECÍFICOS

Digitalizar toda la documentación administrativa y operativa de la empresa, incluyendo procesos de producción, nóminas, pedidos y registros de laboratorio, con el fin de eliminar el manejo manual en papel y facilitar el acceso, almacenamiento y control de la información.

Diseñar e implementar una red interna (intranet) que conecta a todos los departamentos y áreas de la empresa, asegurando una comunicación fluida, rápida y segura entre los empleados y facilitando el acceso a bases de datos y recursos compartidos.

Renovar y estandarizar el parque informático de la empresa, instalando sistemas operativos actualizados y homogéneos en todos los equipos para garantizar la compatibilidad, el soporte técnico y la gestión centralizada de software y hardware.

Establecer protocolos y herramientas de seguridad informática, incluyendo sistemas de respaldo (backups) periódicos y medidas de ciberseguridad (antivirus, firewalls, control de accesos), para proteger la integridad, confidencialidad y disponibilidad de los datos corporativos frente a posibles amenazas y pérdidas.

Capacitar al personal en el uso y manejo de las nuevas tecnologías implementadas, promoviendo una cultura digital dentro de la empresa que facilite la adaptación al cambio, mejore la productividad y reduzca errores derivados de la transición tecnológica.

Evaluar continuamente el desempeño de los sistemas implementados y realizar ajustes necesarios para asegurar la mejora continua de los

procesos tecnológicos y su alineación con los objetivos estratégicos de la empresa.

4. DESARROLLO:

1. **ANALISIS COMPARATIVO**
2. **ESCENARIOS DENTRO DE LA EMPRESA**
3. **PRESUPUESTOS**
4. **INSTALACIÓN DE MAQUINA VIRTUAL**
5. **SERVIDOR**
6. **SEGURIDAD**

1. Análisis Comparativo

A partir de la necesidad de implementar los nuevos sistemas operativos, se presentan las siguientes diferencias clave entre Distribuciones de Linux y Windows 11 Pro.

1. Arquitectura y Kernel

Aspecto	Windows 11 Pro	Distribuciones Linux
Kernel	Kernel NT (cerrado, basado en Windows NT)	Kernel Linux (abierto, monolítico con módulos cargables)
Arquitectura	Diseñado para x86-64 y ARM (requiere TPM 2.0 y Secure Boot)	Soporta x86-64, ARM, RISC-V, y más (sin requisitos estrictos de TPM)
Licencia	Propietario (Microsoft)	Open Source (GPL y otras licencias libres)

2. Sistema de archivos

Windows 11 Pro	Distribuciones Linux

NTFS (predeterminado), soporta exFAT y FAT32	Ext4 (predeterminado en la mayoría), Btrfs, XFS, ZFS (avanzados), soporta NTFS (lectura/escritura con drivers)
No soporta journaling en FAT32	Soporta journaling (Ext4/Btrfs) para recuperación de datos

3. Gestión de Software

Windows 11 Pro	**Distribuciones Linux**
Microsoft Store (limitada), instaladores .exe/.msi	Gestores de paquetes centralizados (APT en Debian/Ubuntu, DNF en Fedora, Pacman en Arch)
Actualizaciones forzosas (pocas opciones de control)	Actualizaciones flexibles (ej. LTS cada 2 años en Ubuntu)
Software comercial (Adobe, Office, etc.)	Alternativas libres (LibreOffice, GIMP) y soporte para Wine/Proton

4. Seguridad

Windows 11 Pro	**Distribuciones Linux**

Defender (integrado), vulnerabilidades históricas a malware	Menos afectado por malware (gracias a permisos granular y repositorios firmados)
Requiere antivirus de terceros	No necesita antivirus en la mayoría de casos
Actualizaciones obligatorias	Parches selectivos (el usuario controla cuándo actualizar)

5. Rendimiento

Windows 11 Pro	**Distribuciones Linux**
Mayor consumo de recursos (RAM/CPU en segundo plano)	Ligero (ej. Mint/Xubuntu funcionan en hardware antiguo)
Optimizado para gaming (DirectX 12)	Mejor rendimiento en servidores y tareas críticas (Kernel ajustable)
Latencia variable (por servicios en segundo plano)	Baja latencia (con kernels como XanMod o Low-Latency)

6. Personalización

Windows 11 Pro	**Distribuciones Linux**

Interfaz rígida (pocas opciones sin herramientas de terceros)	Totalmente personalizable (entornos como KDE, GNOME, i3wm)
Requiere regedit para ajustes avanzados	Control total via terminal o GUI (ej. dconf en GNOME)

7. Soporte de Hardware

Windows 11 Pro	**Distribuciones Linux**
Soporte amplio para drivers (pero cerrados)	Soporte nativo para más dispositivos (drivers en el kernel)
Problemas con hardware antiguo (sin drivers actualizados)	Mejor compatibilidad con hardware antiguo (ej. Mint)
Optimizado para periféricos gaming (RGB, etc.)	Soporte limitado para periféricos propietarios (ej. Nvidia requiere drivers privados)

8. Comunidad y Soporte

Windows 11 Pro	Distribuciones Linux
Soporte oficial (Microsoft, costoso en empresas)	Comunidad activa (foros, Stack Overflow, Arch Wiki)
Documentación cerrada	Documentación abierta y detallada (ej. Ubuntu Wiki)
Actualizaciones con ciclo de vida definido	Soporte a largo plazo (LTS) en distros como Ubuntu

9. Relación intuitiva Usuario-Equipo

Windows 11 Pro	Distribuciones Linux
Interfaz gráfica pulida (familiar para usuarios casuales)	Curva de aprendizaje en distros avanzadas (Kali, Arch)
Ideal para usuarios no técnicos	Distros como Linux Mint o Pop!_OS son amigables para principiantes
Integración con ecosystema Microsoft (Office, Azure)	Terminal necesaria para tareas avanzadas

2. Escenarios de Uso Recomendados dentro de la empresa:

1. Área de Producción (Windows 11 Pro)

- **Razón de elección:**
  - **Compatibilidad con software crítico:** SAP QM y LIMS requieren Windows para su validación GMP (Good Manufacturing Practices).
  - **Cumplimiento normativo:** Registros de eventos integrados para FDA 21 CFR Part 11 (auditoría farmacéutica).
  - **Integración con Active Directory:** Control de acceso mediante tarjetas inteligentes y políticas centralizadas.
- **Alternativas descartadas:** Linux no soporta SAP QM nativamente y carece de herramientas de auditoría específicas para GMP.

2. Investigación y Desarrollo (Windows 11 Pro)

- **Razón de elección:**
  - **Compatibilidad con herramientas científicas:** RStudio, MATLAB y SAS funcionan mejor en Windows.
  - **WSL (Windows Subsystem for Linux):** Permite ejecutar Python/R en entornos Linux sin sacrificar la usabilidad de Windows.
  - **BitLocker:** Encriptación para proteger datos sensibles de ensayos clínicos (requisito GDPR).
- **Alternativas descartadas:** Linux podría usarse, pero dificultaría la colaboración con Office 365 y herramientas clínicas validadas.

3. Técnicos Informáticos (Rocky Linux + Ubuntu LTS)

- **Razón de elección:**
  - **Cumplimiento GxP/Annex 11:** Rocky Linux (clon de RHEL) ofrece audit trails para servidores farmacéuticos.
  - **Coste reducido:** Soporte de Red Hat sin licencias costosas (ideal para Docker, OpenSSH, Wireshark).
  - **Flexibilidad:** Ubuntu LTS en workstations para desarrollo y administración de redes.
- **Alternativas descartadas:** Windows Server sería más caro y menos eficiente para herramientas CLI/networking.

4. Administración y Finanzas (Windows 11 Pro)

- **Razón de elección:**
  - **Software contable:** ContaPlus y MasterControl (validación CSV) son compatibles solo con Windows.
  - **Firma electrónica:** Integración con certificados eIDAS (requerido para documentos legales).
- **Alternativas descartadas:** Linux no soporta ContaPlus ni herramientas de firma cualificada.

5. RRHH (Windows 11 Pro)

- **Razón de elección:**
  - **Protección de datos:** Encriptación nativa (BitLocker) para cumplir con GDPR.
  - **Software de nóminas:** NominaPLUS y Meta4 son exclusivos de Windows.
- **Alternativas descartadas:** Linux carece de soporte para software de RRHH especializado.

6. Legal y Regulatorio (Windows 11 Pro)

- **Razón de elección:**
  - **Control de versiones:** Historial de cambios en Word/Adobe (auditoría legal).
  - **Certificados digitales:** Compatibilidad con herramientas de firma electrónica (acuerdos con autoridades).
- **Alternativas descartadas:** Linux no tiene equivalentes robustos para gestión documental legal.

7. Marketing (Windows 11 Pro)

- **Razón de elección:**
  - **Adobe Creative Cloud:** Photoshop, Premiere y After Effects son estándar en la industria y solo funcionan en Windows/macOS.
  - **Rendimiento gráfico:** Soporte para GPU NVIDIA/AMD con drivers optimizados.
- **Alternativas descartadas:** Linux tiene alternativas como GIMP, pero son inferiores para workflows profesionales.

8. Dirección (Windows 11 Enterprise)

- **Razón de elección:**
  - **Seguridad avanzada:** Windows Defender for Endpoint protege datos sensibles de la alta dirección.
  - **Colaboración:** Integración con Teams, Slack y Google Workspace.
- **Alternativas descartadas:** Linux carece de soporte para suites de colaboración empresarial.

3. Presupuestos:

Departamento	Cantidad	Costo por equipo	Total por Departamento
Produccion	40	380.00 €	15,200.00 €
Investigación y Desarrollo	20	550.00 €	11,000.00 €
Técnicos Informáticos	10	500.00 €	5,000.00 €
Administración y Finanzas	15	380.00 €	5,700.00 €
Recursos Humanos	5	380.00 €	1,900.00 €
Legal y Regulatorio	5	550.00 €	2,750.00 €
Marketing	15	750.00 €	11,250.00 €
Dirección	10	550.00 €	5,500.00 €
Servidores	1	1000.00 €	1000.00 €
Total, de equipos:	121	Costo total	59,300.00 €

Tipo de Licencias	Cantidad	Costo Por Licencia	Total por Departamento
Windows	40	20.00 €	800.00 €
Windows	20	20.00 €	400.00 €
Linux	1	500.00 €	500.00 €
Windows	15	20.00 €	300.00 €
Windows	5	20.00 €	100.00 €
Windows	5	20.00 €	100.00 €
Windows	15	20.00 €	300.00 €
Windows	10	20.00 €	200.00 €
-	-	-	-
Total Licencias	111	Costo total	2,700.00 €

Costo del Servicio	4,840.00 €
TOTAL	66,840.00 €

Servicio de Antivirus Kaspersky Next EDR Fundations:

A partir de 193,35 €/al año

4. INSTALACIÓN DE LA MÁQUINA VIRTUAL

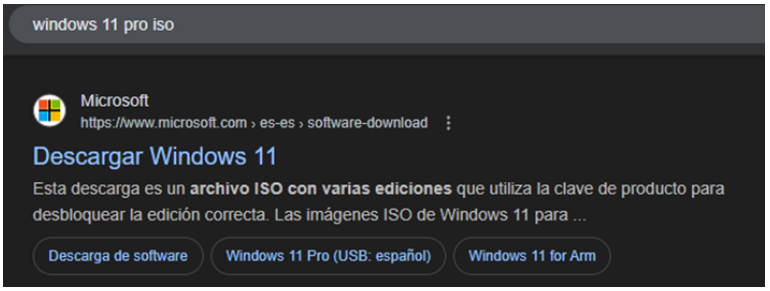
Instalación de Windows 11 Pro (Puestos administrativos)

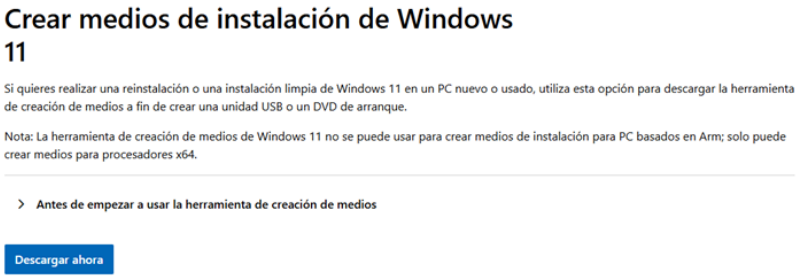
Requisitos:

- TPM 2.0 y Secure Boot (requisitos obligatorios).
- RAM: 4 GB (recomendado 8 GB).

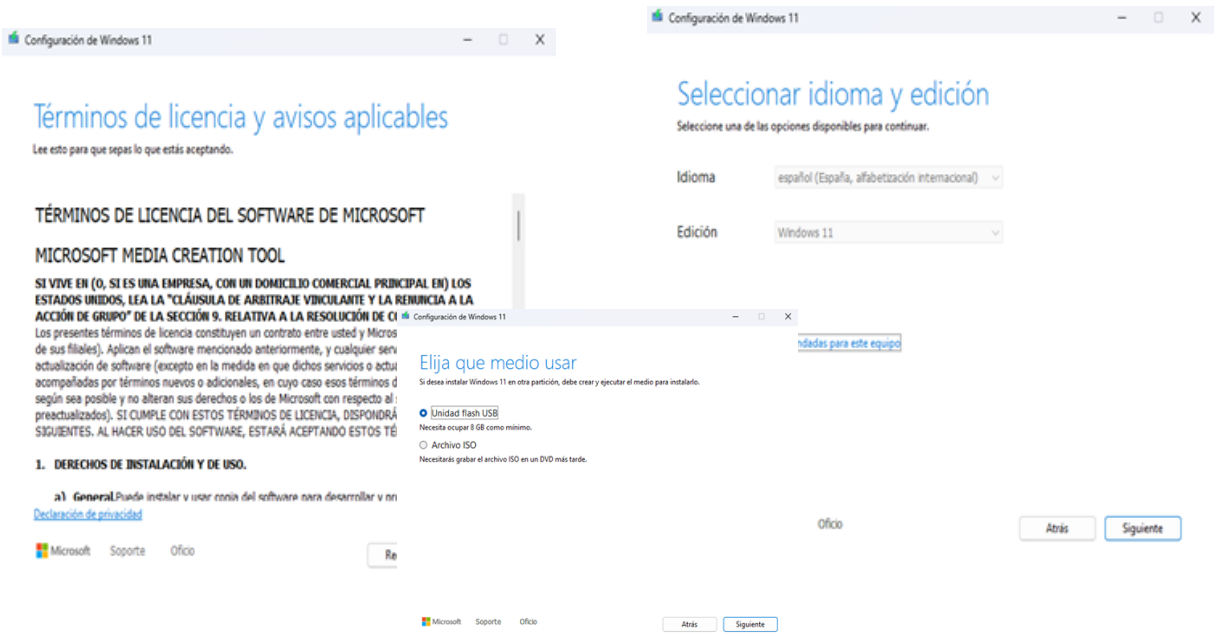
Pasos:

1. **Descargar ISO:**
   - Usar **Media Creation Tool** desde Microsoft.

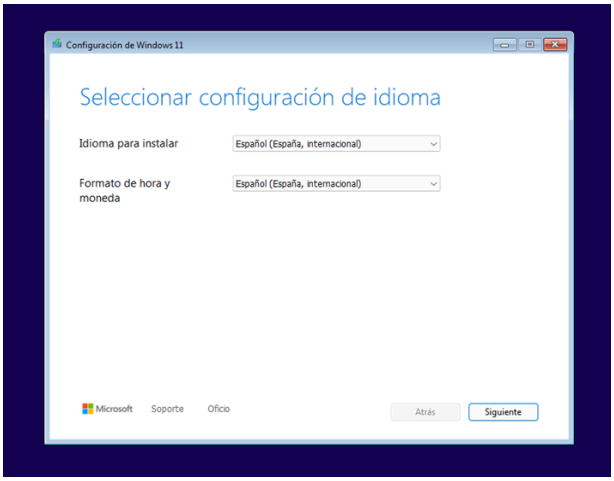


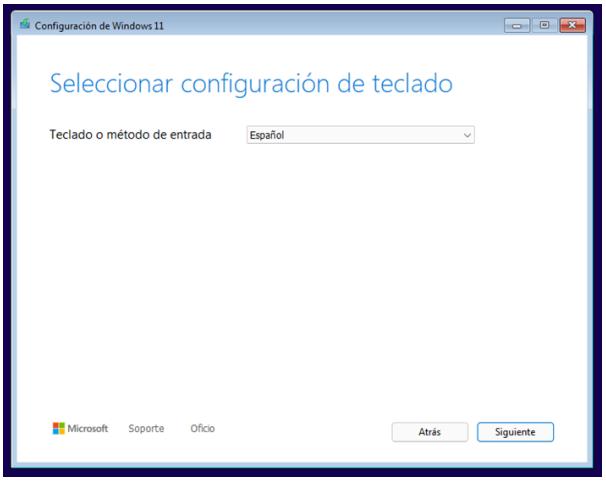


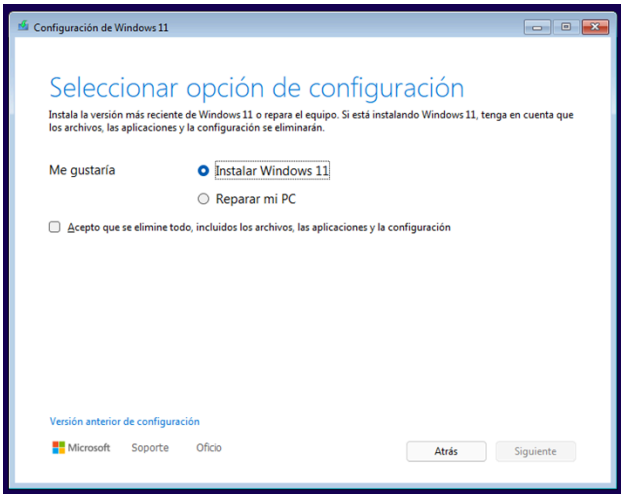
2. **USB booteable:**
   - Ejecutar la herramienta y seguir los pasos.

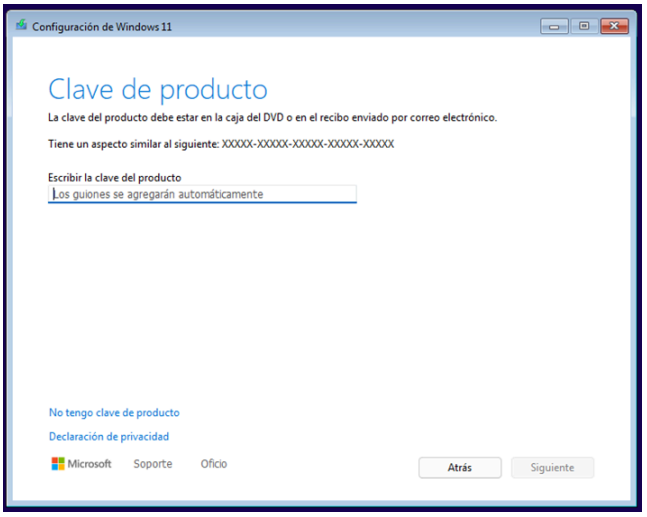


3. **Instalación:**
    - Arrancar desde USB.
    - Seleccionar idioma y distribución de teclado.
    - Introducir clave de producto (o omitir para activar luego).
    - Elegir "Instalación personalizada".
    - Particionar disco (eliminar particiones antiguas si es necesario).
    - Configurar usuario y contraseña.





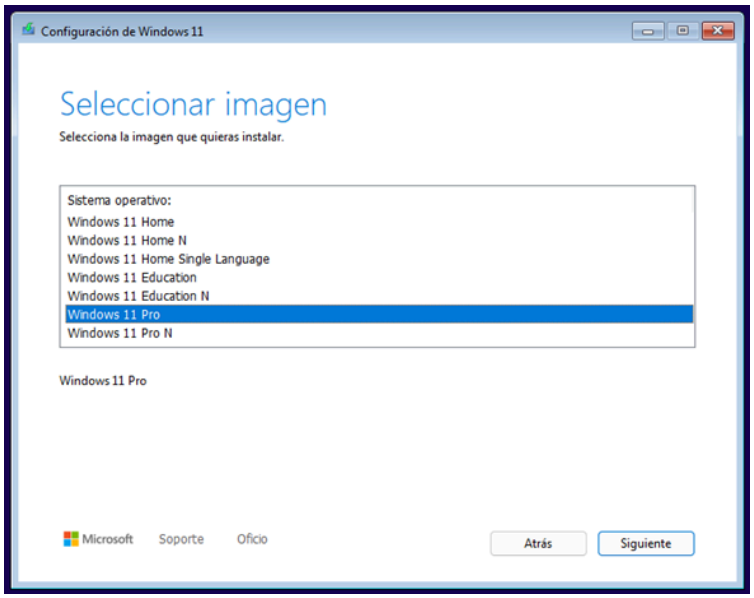


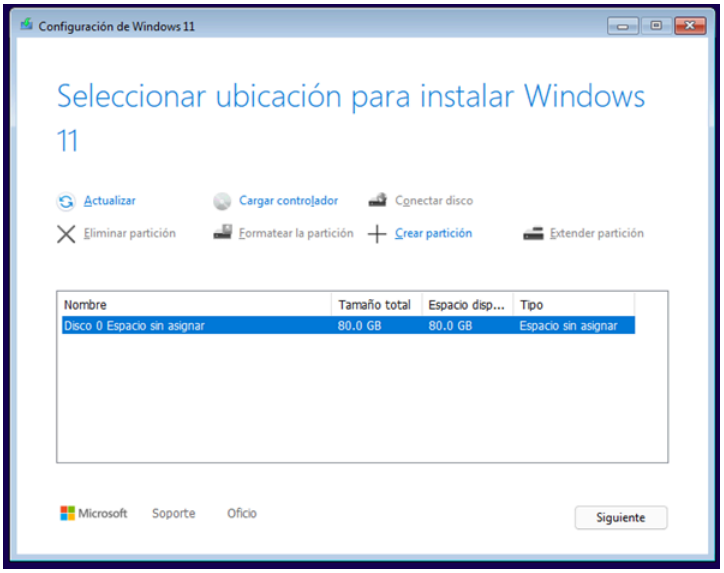


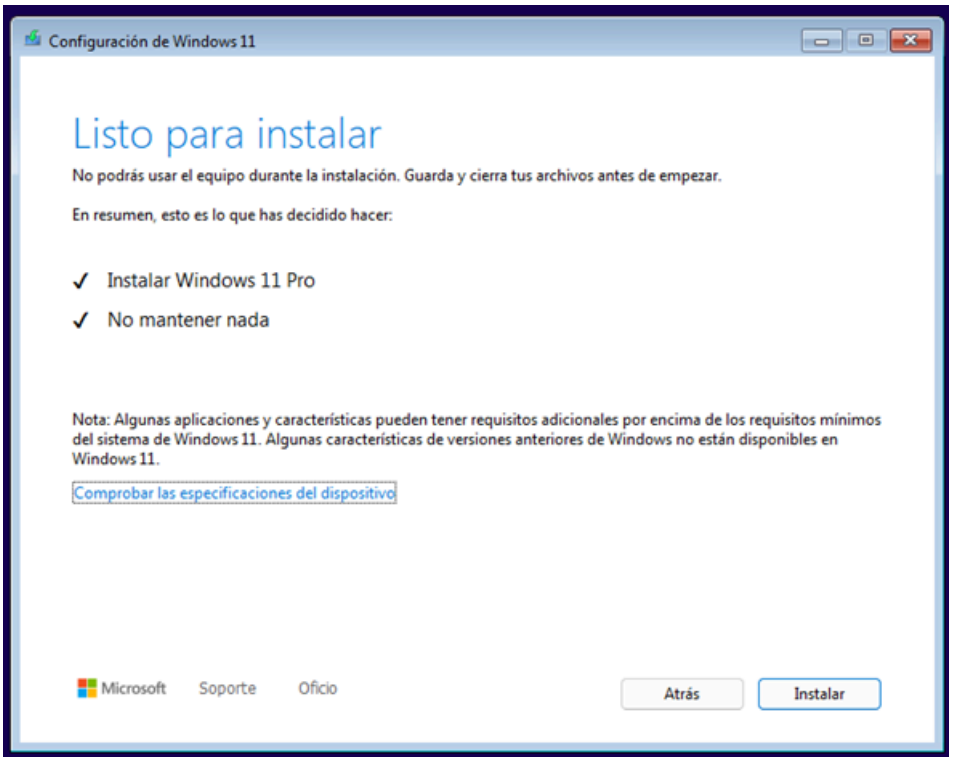
*Seleccionar “No tengo clave de producto” en caso de no tenerla. *

- Elegimos la Distribución deseada

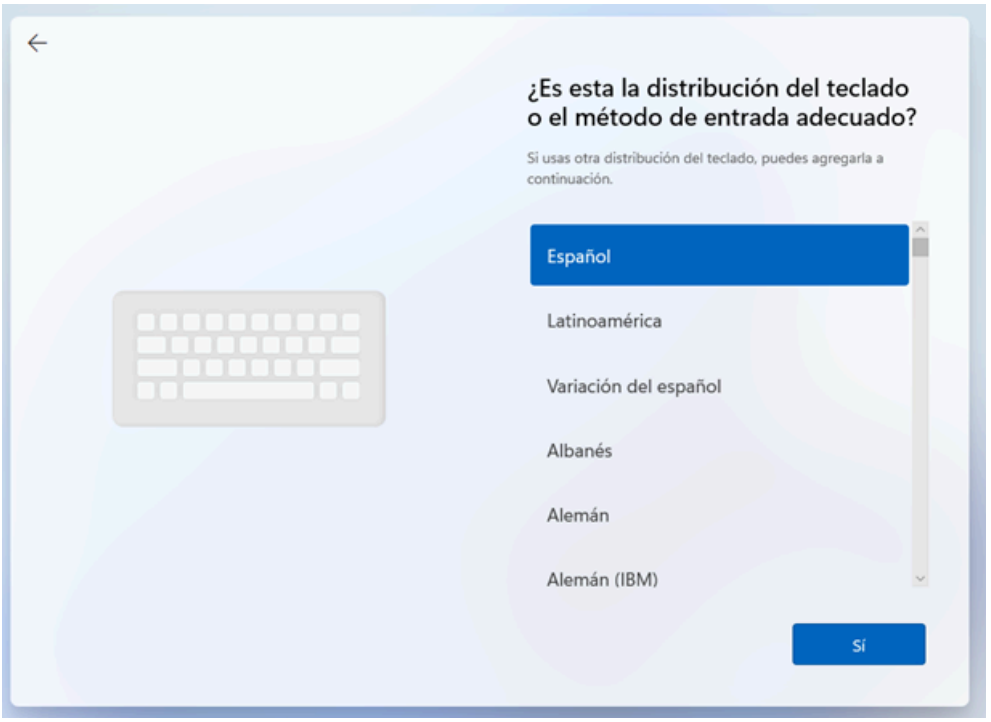
- Seleccionamos el espacio asignado al Sistema Operativo





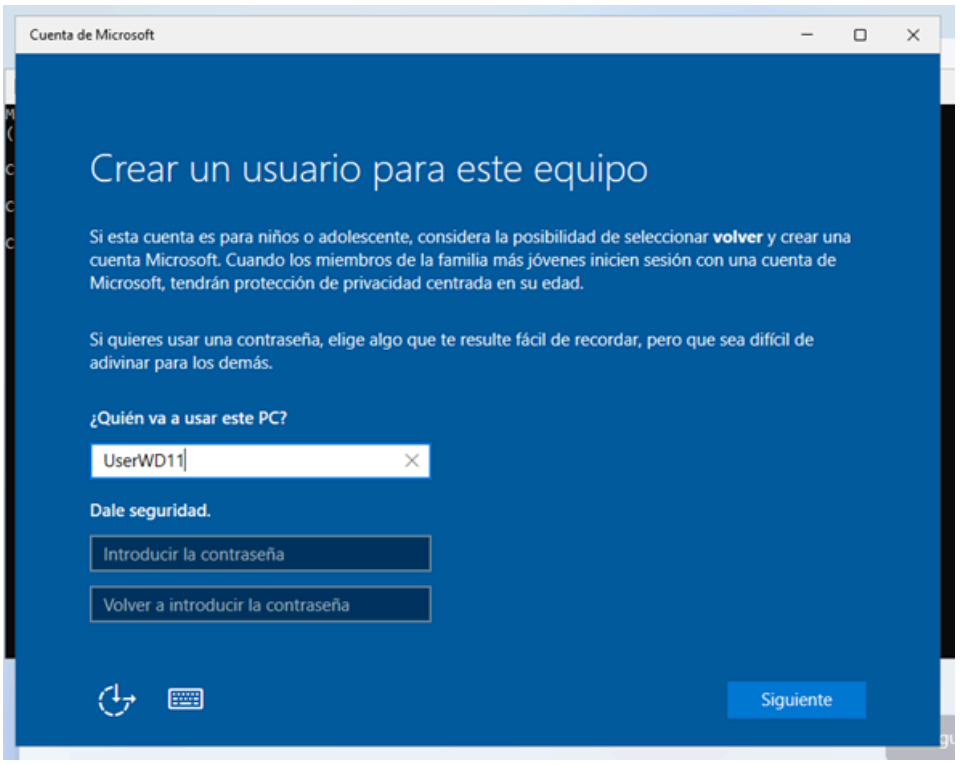


- Esperamos a que se inicie la instalación. Esto puede tomar su tiempo dependiendo de la velocidad del almacenamiento donde reside el SO. Se reiniciará automáticamente una vez terminada.



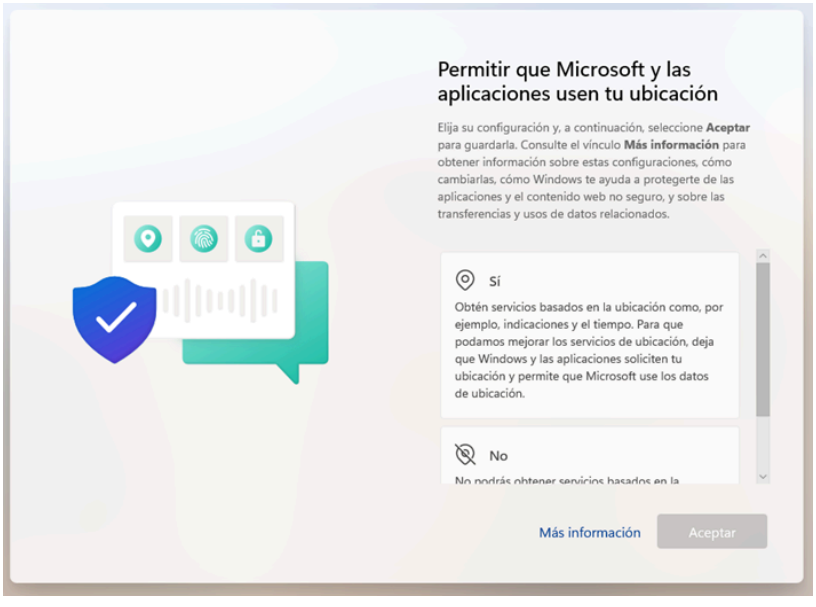
- Seleccionamos el idioma y una distribución de teclado.

-



Windows 11 Pro solo permite el acceso a cuentas de Microsoft. Sin embargo, se puede acceder a colocar una cuenta nativa por medio de comandos CMD:

- Shift + 10 à start ms-cxh:localonly



- Este apartado dependerá del cliente sobre si desea colaborar con aditivos servicios opcionales de Windows para facilitar el despliegue de anuncios,

datos de diagnóstico de Windows, acceso a la ubicación y demás.

5. SERVIDOR

El servidor será el centro de toda la infraestructura tecnológica de la empresa. Se encargará de gestionar usuarios, compartir archivos, proteger la información y automatizar tareas importantes.

Usaremos Rocky Linux como sistema operativo por ser seguro, gratuito y muy estable. El servidor ofrecerá los siguientes servicios:

-Control de usuarios y accesos.

-Carpetas compartidas entre departamentos.

-Servidor DNS y DHCP: para asignar direcciones IP automáticamente y facilitar la comunicación entre los equipos.

-Copias de seguridad automáticas (backups).

-Firewall y otras medidas de seguridad para evitar accesos no autorizados.

-VPN para conexión segura desde fuera de la empresa.

Este servidor es esencial para que la empresa funcione de forma digital, segura y organizada.

1. POLÍTICAS GENERALES DE SEGURIDAD

1.1. Justificación de la seguridad como parte integral del proyecto

La seguridad informática es un componente importante e inseparable en el diseño, implementación y operación de cualquier infraestructura tecnológica moderna. En relación con este proyecto basado en Windows y Linux, la seguridad cibernética después de la implementación no debe considerarse una fase, sino como una necesidad estructural porque el sistema está establecido. Esta integración temprana es particularmente crítica para las PYME, donde los recursos son limitados y la exposición al riesgo puede poner en peligro la continuidad del negocio. La introducción de medidas de seguridad desde el principio permite una reducción significativa en el riesgo operativo al prevenir los ataques, el acceso no autorizado o la pérdida de información, situaciones que pueden tener reputación financiera y reputación significativa. También facilita la adherencia a la legislación, ya que garantiza un marco legal, como GDPR, que proporciona trazabilidad, acceso adecuado y protección contra datos personales.

Además, en realidad brinda la oportunidad de proteger los activos más críticos de la empresa, como bases de datos de clientes, documentos internos o de identificación a través de herramientas de cifrado, políticas de usuario y planes de reemplazo apropiados. La infraestructura creada con criterios de seguridad también promueve eventos de resistencia incluso desde el comienzo del diseño, como robusta, segmentación de red, control de tráfico e informes o ataques incorrectos. Desde un punto de vista práctico, se utiliza en la evaluación inicial de riesgos, definiendo los requisitos de seguridad no funcionales, incluidas las tareas relacionadas y la suposición de responsabilidad compartida entre todos los miembros del equipo. Esta visión transversal proporciona protección continua, mejora la calidad general del sistema y promueve el éxito del proyecto no solo desde un punto de vista técnico, sino también de las actividades y las perspectivas estratégicas de la organización.

1.2. Comparativa del enfoque de seguridad en Windows y Linux

Windows 11 ofrece un método de seguridad mejorado desde el principio. TPM 2.0 requiere un inicio obligatorio y seguro (troncal seguro) y una compañía UEFI que garantiza un entorno más protegido del software malicioso que opera antes de que se cargue el sistema. Para Linux, la seguridad se basa en un modelo de control más detallado. Aunque esto no incluye VBS o HVCI, distribuciones como los sistemas de control de acceso de Ubuntu o Fedor como Apparmor y Selinux, que limitan el comportamiento de los procesos sensibles. Además, Linux es compatible con TPM y Secure Boot y permite controlar los servicios, permisos y actualizaciones de control manual, dando al administrador un mayor control sobre el entorno.

1.3. Establecimiento de políticas de seguridad según perfil de usuario

Introducción

Las políticas de seguridad sirven para limitar el riesgo operativo y aplicar el principio de mínimo privilegio. Nos hemos basado en las políticas como base de las plantillas y directrices del INCIBE (Instituto Nacional de Ciberseguridad)

Administrador de sistemas

- Uso de credenciales personales con autenticación segura; recomendación de doble factor (2FA) en accesos críticos.
- Cuentas separadas para tareas administrativas y uso diario.
- Registro de logs de actividad administrativa y revisión periódica.
- Acceso remoto restringido mediante VPN o redes autorizadas.
- Documentación obligatoria de cambios críticos en la infraestructura.
- Prohibición de utilizar dispositivos personales para acceder al sistema.

Usuario estándar

- Acceso limitado exclusivamente a los recursos necesarios para su función.
- Prohibición de instalación o modificación de software no autorizado.
- Uso obligatorio de contraseñas seguras (mínimo 10 caracteres, alfanuméricas), con renovación cada 90 días.
- Bloqueo automático de sesión tras un máximo de 10 minutos de inactividad.
- Antivirus activo y actualizado permanentemente.
- Uso restringido de dispositivos externos (USB, discos portátiles) no autorizados.
- Prohibición de almacenar datos en el escritorio local o dispositivos externos.

Técnico o desarrollador

- Acceso autorizado a terminales, entornos de desarrollo, compiladores, contenedores y máquinas virtuales.
- Prohibición de privilegios administrativos en sistemas de producción sin autorización expresa.
- Uso de control de versiones obligatorio para scripts y automatizaciones.
- Revisión y documentación de toda actividad técnica realizada.
- Uso exclusivo de herramientas validadas por la organización.

Usuario temporal o invitado

- Cuentas temporales con fecha de caducidad predefinida.
- Acceso restringido a funciones básicas y no persistentes (sin almacenamiento local).
- Prohibición de acceso a carpetas compartidas internas o documentación sensible.
- Eliminación automática de la cuenta una vez concluida la actividad prevista.

Políticas comunes a todos los usuarios

- Uso obligatorio de contraseñas robustas y personales.
- Prohibido compartir credenciales de acceso.
- Eliminación de cuentas inactivas tras 30 días sin uso.
- Revisión periódica de los permisos asignados en función del rol.
- Uso exclusivo de software autorizado y actualizado.
- Almacenamiento de archivos únicamente en ubicaciones seguras designadas por el administrador.
- Bloqueo manual de sesión al ausentarse del puesto.
- Custodia física adecuada de dispositivos móviles o portátiles.
- Participación en formación básica en ciberseguridad (navegación, correo, identificación de amenazas).

Medidas adicionales complementarias

- Solo se permite el uso de dispositivos USB previamente autorizados por el administrador.
- Cualquier unidad externa deberá ser escaneada antes de su utilización.
- El uso de impresoras compartidas estará sujeto a control de acceso y podrá ser auditado si la infraestructura lo permite.

- Se realizará una auditoría mensual del inventario de cuentas. Las cuentas de usuarios dados de baja serán eliminadas de inmediato.
- En caso de detección de accesos no autorizados o comportamiento anómalo, se notificará de inmediato al administrador, quien registrará el incidente conforme al protocolo interno.

2. ENDURECIMIENTO (HARDENING) DEL SISTEMA

El endurecimiento del sistema consiste en el uso de varias medidas técnicas y organizativas que reducen la superficie de exposición a los posibles ataques, no eliminen y limiten las funciones a tomar y usar configuraciones seguras, reduciendo las vulnerabilidades para aumentar el control del sistema y proteger la información confidencial.

2.1. Desactivación de servicios innecesarios

Una de las primeras actividades de la cura del sistema es la identificación y desactivación de servicios y procesos que no son necesarios para la actividad planificada del equipo. Esto reduce el consumo de recursos y previene los posibles vectores de ataque, especialmente si los servicios están sujetos a la red.

2.1.1. Windows

En Windows Systems, es aconsejable revisar una lista de servicios de la consola de servicios (Services.MSC) o utilizar herramientas de gestión de políticas grupales. Algunos servicios innecesarios en el entorno corporativo pueden ser:

- **Fax**: en desuso en muchas oficinas.
- **Bluetooth**: si el equipo no requiere conectividad inalámbrica de corto alcance.
- **Windows Remote Registry**: innecesario salvo en entornos de administración centralizada.
- **XPS Services**: funcionalidad de impresión que puede ser sustituida por PDF.
- **Servidores multimedia o servicios de juegos**.

La discapacidad debe llevarse a cabo de manera controlada, confirmando que no afecta la funcionalidad general o los procesos críticos. Es aconsejable establecer una política de discapacidad grupal o estándar.

2.1.2. Linux

En entornos Linux, la gestión de servicios se realiza mediante systemctl, service o herramientas específicas de cada distribución. Algunos servicios que pueden desactivarse si no se utilizan son:

- **Avahi-daemon** (descubrimiento de red).
- **rpcbind** (llamadas a procedimientos remotos).
- **telnet**, **ftp**: protocolos obsoletos y no cifrados.

Se puede utilizar el comando systemctl list-unit-files --type=service para listar todos los servicios y su estado, y desactivar aquellos innecesarios con systemctl disable nombre-del-servicio.

2.2. Configuración segura del arranque y la BIOS/UEFI

La protección del proceso de arranque es crítica para evitar la manipulación del sistema antes de que el control pase al sistema operativo. Las siguientes recomendaciones son aplicables a sistemas modernos:

- **Activar Secure Boot** desde la BIOS/UEFI para impedir el arranque de sistemas no firmados.
- **Establecer una contraseña de acceso a la BIOS/UEFI** para evitar modificaciones no autorizadas.
- **Desactivar el arranque desde dispositivos externos** (USB, DVD) si no son necesarios, reduciendo el riesgo de bootkits o cargas no autorizadas.
- **Activar el arranque desde disco interno en primer lugar** y bloquear cambios sin autenticación.
- En entornos Windows 11, **la presencia de TPM 2.0 y UEFI** fortalece el entorno de arranque frente a amenazas de bajo nivel.

Estas medidas refuerzan la integridad del sistema desde el encendido hasta la carga completa del sistema operativo.

2.3. Aplicación de recomendaciones de buenas prácticas (CIS Benchmarks, Lynis)

Para complementar las medidas anteriores, se recomienda aplicar guías de buenas prácticas y realizar auditorías automatizadas de seguridad. Dos herramientas destacadas en este ámbito son:

- **CIS Benchmarks (Center for Internet Security)**: proporciona guías detalladas y actualizadas con configuraciones recomendadas para múltiples sistemas (Windows, Linux, dispositivos de red, etc.). Estas guías permiten asegurar parámetros como:
    - Políticas de contraseñas.
    - Configuración de auditoría de eventos.
    - Restricciones en servicios y puertos.
    - Permisos de archivos y registros.
    - Seguridad en el navegador y actualizaciones automáticas.

- **Lynis (Linux Audit Tool)**: herramienta de auditoría de seguridad automatizada para sistemas Linux y Unix. Permite identificar configuraciones inseguras, servicios activos innecesarios, permisos incorrectos, entre otros. Proporciona un informe con puntuación de seguridad y recomendaciones prácticas para su mejora.

Ambas herramientas permiten estandarizar y verificar el cumplimiento de políticas de seguridad en los sistemas, facilitando la gestión continua del hardening.

4. FIREWALL Y CONTROL DE TRÁFICO

4.1. Configuración del cortafuegos en Windows (Defender Firewall)

Windows Defender Firewall es la solución integrada en los sistemas Windows para la gestión del tráfico de red. Permite aplicar reglas específicas por tipo de red (pública, privada o de dominio) y controlar el acceso por aplicación o puerto.

Pasos recomendados:

- Activar el firewall en los tres perfiles (privado, público y de dominio).
- Bloquear todas las conexiones entrantes por defecto y permitir solo las necesarias.
- Crear reglas explícitas para permitir servicios esenciales (ej. Escritorio remoto, SMB compartido con seguridad, etc.).
- Restringir las aplicaciones que pueden comunicarse con el exterior.
- Revisar las reglas preconfiguradas y desactivar aquellas que no sean necesarias

4.2. Configuración del cortafuegos en Linux (UFW o firewalld)

En sistemas Linux, el cortafuegos por excelencia es **iptables**, pero por simplicidad de uso se emplean interfaces como **UFW** (Ubuntu/Debian) o **firewalld** (Fedora/CentOS/RHEL).

UFW (Uncomplicated Firewall)

- Se activa con: sudo ufw enable
- Reglas básicas:

  sudo ufw default deny incoming
  sudo ufw default allow outgoing

  sudo ufw allow ssh

  sudo ufw allow 80/tcp

  Ver estado y reglas:

  sudo ufw status verbose

firewalld

- Utiliza zonas de red y es más dinámico.
- Activación: sudo systemctl enable --now firewalld
- Configurar zonas:

  sudo firewall-cmd --zone=public --add-port=22/tcp --permanent
  sudo firewall-cmd --reload

4.3. Aplicación de reglas según zonas de red y roles

Es recomendable definir reglas de firewall **según el contexto de red** y **los roles de los dispositivos**:

- **Zona interna (LAN):** permitir puertos específicos como SMB, RDP o SSH si son necesarios, con control de IP origen.
- **Zona pública (Internet):** bloquear todo por defecto y permitir solo servicios estrictamente necesarios (ej. HTTP/HTTPS en servidores web).
- **Zona de gestión:** red interna protegida donde solo accede el equipo de administración (IP restringidas).

Por roles:

- **Servidores:** abrir solo los puertos del servicio que ofrecen (ej. 80/443 para web, 22 para SSH).

- **Clientes/Usuarios:** bloquear puertos innecesarios de entrada y salida (ej. puertos de juegos, P2P, etc.).
- **Equipos administrativos:** permitir acceso solo a servicios de gestión seguros, y registrar el tráfico de administración.

Estas reglas deben estar documentadas y ser coherentes con la arquitectura de red definida.

5. ANTIVIRUS Y PROTECCIÓN ANTIMALWARE

5.1. Soluciones integradas en Windows (Windows Defender)

Microsoft Defender Antivirus (anteriormente Windows Defender) es la solución nativa de Windows 10 y 11, incluida sin coste adicional. Su integración con el sistema operativo permite una protección en tiempo real eficaz y sin interferencias significativas en el rendimiento.

Características destacadas:

- Protección en tiempo real y análisis bajo demanda.
- Monitorización de comportamiento con protección contra ransomware (mediante "Acceso controlado a carpetas").
- Integración con el **Centro de Seguridad de Windows**.
- Actualizaciones automáticas a través de Windows Update.
- Compatible con políticas de grupo y administración remota mediante PowerShell o Intune.

Para entornos corporativos pequeños, Defender es una solución más que suficiente si se complementa con buenas prácticas y políticas de restricción de ejecución

5.2. Implementación de antivirus en Linux (ClamAV u otros)

Aunque los sistemas Linux son menos propensos a malware convencional, pueden actuar como **puentes de infección** en redes mixtas o estar expuestos a amenazas específicas (scripts maliciosos, exploits, troyanos).

ClamAV es el antivirus de código abierto más común para entornos Linux:

- Permite escaneo bajo demanda y programación de análisis periódicos.

- Se actualiza regularmente mediante freshclam.
- Compatible con la exploración de directorios compartidos, servidores de correo, y servidores web.

5.3. Análisis periódicos y gestión de amenazas

Los análisis programados son clave para detectar amenazas latentes o archivos sospechosos que hayan eludido la protección en tiempo real. En ambos sistemas (Windows y Linux), se recomienda:

- Programar escaneos completos **semanales** y rápidos **diarios** fuera del horario laboral.
- Excluir carpetas críticas del sistema para evitar conflictos o lentitud (por ejemplo: /proc, /sys en Linux).
- Configurar alertas o informes automáticos en caso de detección.
- Mantener un log de amenazas detectadas y acciones tomadas (aislamiento, eliminación, cuarentena).
- Analizar con herramientas como **VirusTotal** archivos sospechosos antes de ejecutarlos.

8. CIFRADO Y PROTECCIÓN DE DATOS

El cifrado es una de las medidas más eficaces para proteger la confidencialidad y la integridad de la información, especialmente en caso de pérdida, robo o acceso no autorizado a dispositivos o archivos. La implementación de políticas de cifrado, junto con la gestión segura de contraseñas y verificación de integridad, permite cumplir con los principios fundamentales de la seguridad de la información (confidencialidad, integridad, disponibilidad).

8.1. Cifrado de unidades (BitLocker en Windows, LUKS en Linux)

Windows: BitLocker

- BitLocker es la solución de cifrado de disco completo integrada en las ediciones profesionales y empresariales de Windows.
- Permite cifrar unidades del sistema y secundarias con autenticación transparente (TPM) o mediante PIN/contraseña.

- Se configura desde el Panel de Control o mediante manage-bde y PowerShell.
- Es recomendable activarlo en equipos portátiles, dispositivos que contengan datos sensibles o en entornos de movilidad.

Linux: LUKS (Linux Unified Key Setup)

- LUKS es el estándar de cifrado de disco en Linux, utilizado principalmente junto a cryptsetup.
- Puede cifrar particiones completas (como /home) durante la instalación o post-instalación.
- Soporta múltiples claves de acceso y autenticación mediante contraseña o archivo de clave.
- Se activa al inicio del sistema, solicitando la contraseña para el desbloqueo.

8.2. Cifrado de archivos sensibles y backups

Además del cifrado de disco completo, es recomendable cifrar documentos críticos y copias de seguridad, especialmente si se almacenan en ubicaciones compartidas, en la nube o en medios extraíbles.

Backups cifrados:

- Las copias de seguridad externas deben cifrarse antes de su envío a la nube o almacenamiento externo.
- Algunos sistemas de backup permiten cifrado nativo (ej. duplicity, restic, Veeam con cifrado AES).

8.3. Gestión de claves y contraseñas seguras

La protección del acceso a los sistemas depende de la calidad de las contraseñas y de la gestión segura de las claves de cifrado. Algunas recomendaciones esenciales:

- Contraseñas con al menos 10-12 caracteres, alfanuméricas y con símbolos.
- Evitar reutilizar contraseñas entre servicios.
- Uso de **gestores de contraseñas seguros** (KeePassXC, Bitwarden, 1Password).
- Implementar **autenticación multifactor (2FA)** cuando sea posible.
- Almacenar claves privadas o ficheros .gpg, .pem en ubicaciones protegidas con permisos estrictos.

La pérdida o filtración de claves de cifrado compromete completamente la seguridad del sistema, por lo que su protección debe ser prioritaria.

8.4. Verificación de integridad de datos críticos

El cifrado no garantiza por sí solo que la información no haya sido modificada. Por ello, debe complementarse con mecanismos de **verificación de integridad**:

- Utilización de **hashes** (SHA-256, SHA-512) para comprobar que archivos no han sido alterados.
- Almacenamiento de los hashes en un repositorio seguro para comparación posterior.
- Comprobación de integridad en backups antes y después de la restauración.
- En entornos más avanzados, se pueden usar firmas digitales con GPG para validar tanto la autoría como la integridad de archivos distribuidos.

9. BACKUPS Y RECUPERACIÓN

Las copias de seguridad son la última línea de defensa frente a incidentes como fallos del sistema, errores humanos, ransomware o pérdidas físicas. Una estrategia de backup eficaz debe combinar redundancia, cifrado, automatización y verificación de recuperación

9.1. Política de copias de seguridad (locales y externas)

Una política de respaldo debe definir:

- **Periodicidad**: diaria, semanal o mensual, según criticidad de los datos.
- **Ubicación**: combinación de copias **locales** (discos externos, NAS) y **externas** (nube, datacenter).
- **Tipo de backup**:
    - Completo: copia de todo el sistema o directorios clave.
    - Incremental: solo archivos modificados desde el último backup.
    - Diferencial: cambios desde el último completo.

Recomendación práctica: estrategia 3-2-1

- 3 copias en total
- 2 en distintos soportes
- 1 en una ubicación externa (offline o en la nube)

9.3. Encriptación y control de acceso a copias de seguridad

Dado que los backups pueden contener información sensible:

- **Cifrado obligatorio** en backups externos (USB, nube, discos portátiles).
- Herramientas como **VeraCrypt**, gpg, openssl o backup tools con cifrado nativo.
- **Restricción de acceso** al personal autorizado mediante permisos del sistema de archivos.
- En entornos Windows, establecer permisos NTFS y cifrado EFS si no se usa software externo.

9.4. Pruebas de restauración y documentación del procedimiento

No basta con hacer copias, hay que comprobar que se pueden recuperar:

- **Pruebas periódicas de restauración**, tanto parciales como completas.

- Validación de la integridad de los archivos restaurados.
- Documentación paso a paso del procedimiento de restauración, incluyendo:
    - Tiempo estimado de recuperación (RTO).
    - Datos críticos a restaurar con prioridad (RPO).
    - Responsable del proceso y ubicaciones de respaldo.

10. SEGURIDAD EN REDES

La protección de la red es esencial para evitar accesos no autorizados, ataques de denegación de servicio, escaneos o infecciones desde dispositivos internos o externos. Una red bien segmentada, controlada y monitorizada reduce significativamente los riesgos.

10.1. Configuración segura de interfaces de red y DNS

- Asignar interfaces a zonas según el firewall (privada, pública).
- Desactivar interfaces no utilizadas o inalámbricas si no son necesarias.
- Usar **servidores DNS confiables y seguros** (Cloudflare, Quad9, Google DNS), y desactivar la resolución recursiva en servidores internos.
- Restringir el tráfico DNS mediante firewall (puerto 53 solo hacia servidores permitidos).

10.2. Limitación de servicios expuestos

- Solo deben estar accesibles desde la red externa los servicios estrictamente necesarios (web, correo, VPN).
- Utilizar escáneres de puertos como nmap o netstat para auditar servicios activos.
- Activar cortafuegos para bloquear puertos no utilizados.
- Para servicios internos, establecer redes separadas (VLANs o subredes) o usar túneles VPN.

10.3. Control de accesos remotos con autenticación fuerte

- Proteger servicios como SSH, RDP o VPN con:
    - Contraseñas robustas y autenticación de doble factor (2FA).

    - Limitación de IPs permitidas.
    - Deshabilitación del acceso remoto a cuentas administrativas, salvo excepciones justificadas.
    - En SSH: desactivar login por contraseña (PasswordAuthentication no) y usar claves públicas.
- Monitorizar y registrar todos los accesos remotos.

10.4. Prevención de escaneos y ataques comunes (fail2ban, configuración de firewall)

- **Fail2ban**: herramienta que analiza logs y bloquea IPs tras intentos de acceso fallidos.
    - Protege servicios como SSH, FTP, Apache.
    - Configurable en /etc/fail2ban/jail.conf.
- **Configuración del firewall**:
    - Rechazar paquetes ICMP o SYN a puertos cerrados para evitar fingerprinting.
    - Aplicar políticas restrictivas por defecto y listas blancas de IP confiables.
    - Monitorizar tráfico sospechoso (por ejemplo, mediante iptables, firewalld, Wireshark o Suricata).

6. LÍNEAS DE INVESTIGACIÓN FUTURAS

Integración de tecnologías de Industria 4.0 en procesos farmacéuticos

Explorar la implementación de tecnologías avanzadas como IoT (Internet de las Cosas), sensores inteligentes y automatización robótica para optimizar la producción, control de calidad y trazabilidad en la planta farmacéutica.

Desarrollo de sistemas de inteligencia artificial para análisis predictivo

Investigar el uso de algoritmos de machine learning y análisis de big data para predecir fallas en maquinaria, optimizar inventarios y mejorar la toma de decisiones en la gestión de recursos y producción.

Implementación de blockchain para trazabilidad y seguridad documental

Analizar la viabilidad de aplicar blockchain para asegurar la trazabilidad de medicamentos desde la fabricación hasta la distribución, garantizando la autenticidad y seguridad de los registros digitales.

Evaluación del impacto de la transformación digital en la cultura organizacional

Estudiar cómo los cambios tecnológicos afectan la dinámica laboral, la motivación y la capacitación continua del personal, con el objetivo de diseñar estrategias que faciliten la adaptación y el desarrollo profesional.

Ciberseguridad avanzada y resiliencia ante ciberataques

Investigar nuevas técnicas y protocolos de ciberseguridad específicos para el sector farmacéutico, enfocándose en la prevención de ataques sofisticados y en la recuperación rápida ante incidentes.

Explorar la incorporación de tecnologías digitales que permitan monitorizar y reducir el impacto ambiental de la producción farmacéutica, alineándose con políticas de sostenibilidad y responsabilidad social corporativa.

7. BIBLIOGRAFÍA

1. Documentación oficial de Microsoft – Para saber cómo instalar y configurar Windows 11 Pro. Enlace: **https://support.microsoft.com**

2. Guías de Linux (Ubuntu y Rocky Linux) – Enlace: **https://ubuntu.com**

3. Seguridad informática – Apuntes y conocimientos de Víctor de la carrera

4. Tutoriales en YouTube – Algunos vídeos nos ayudaron a ver cómo se hacía la instalación paso a paso, sobre todo para la máquina virtual y la partición de discos.

8. OTROS PUNTOS

Aportaciones personales: Este proyecto nos ha servido un montón para entender lo importante que es la tecnología hoy en día, especialmente en empresas como esta que todavía trabajan todo a mano. Me ha ayudado a aplicar lo que veo en clase a algo real, y también a mejorar en plan organizarse y pensar soluciones prácticas que de verdad funcionen para ellos.

Retos profesionales: Lo más difícil ha sido ver cómo a veces la gente no está tan abierta al cambio, porque ya están acostumbrados a hacer las cosas de una manera. También nos costó un poco pensar en una solución que no fuera muy cara ni complicada, pero que de verdad pueda funcionar con lo que tienen ahora y con lo que pueden manejar.

Restos personales: Por parte del grupo, la verdad es que no ha sido fácil compaginar todos los proyectos y la vida diaria. Nos ha tocado aprender a organizar mejor el tiempo para poder avanzar sin agobiarnos ya que era un proyecto que no tuvimos en cuenta en un principio.

Agradecimientos: Quiero dar las gracias a toda la gente de la empresa que nos ayudó, que nos contó cómo hacen las cosas y me dio su tiempo sin problemas para desarrollar una solución.