**Proyecto de Redes**

**Detalle de los equipos para los Terminales:**

- Procesador: Intel Core i5-12400 2.50GHz de 12va generacion.  
- Memoria RAM: 16GB.  
- Almacenamiento: SSD de 2TB.  
- Pantalla: Monitor Nitro X v2 series, resolución(2560x1440).  
- Conectividad: Puertos USB 3.0, HDMI y Ethernet para diversas necesidades de conexión.  
  
**Detalle del servidor para el establecimiento:**  
- Modelo: HPE ProLiant DL380 Gen10  
- Especificaciones:  
- Procesador: 2 x Intel Xeon Silver 4210  
- RAM: 64GB DDR4  
- Almacenamiento: 4 x 1TB SSD en RAID 5  
- Conectividad: 4 x 1GbE y 2 x 10GbE  
  
**Detalle y fundamentación del sistema operativo de los puestos de trabajo:**  
- Sistema Operativo: Windows 11  
- Razón: Amplio soporte de aplicaciones empresariales, seguridad robusta, y actualizaciones regulares.  
- Compatibilidad: Compatible con una amplia gama de software y hardware.  
- Seguridad: Incluye BitLocker para cifrado de disco y Windows Defender para protección antivirus.  
  
**Detalle y fundamentación del sistema operativo del servidor:**  
- Sistema Operativo: CentOS 7  
-**Razón:** CentOS 7 ofrece un entorno robusto y fiable para servidores, con un ciclo de vida prolongado que garantiza actualizaciones y soporte a largo plazo. Esto lo convierte en una opción ideal para aplicaciones empresariales y de misión crítica.

**-Compatibilidad:** CentOS 7 es altamente compatible con Apache y Nginx, bases de datos como MySQL y PostgreSQL, y herramientas de virtualización y contenedorización como Docker. Además, su compatibilidad con RHEL asegura que cualquier aplicación certificada para RHEL también funcionará en CentOS.

**Detalle del esquema lógico primario (tentativo) de interconexión del establecimiento:**  
Esquema lógico primario:  
- Topología: Estrella, con un switch central gestionado que conecta todos los terminales y servidores.  
- Segmentación de Red: VLANs para separar el tráfico de diferentes departamentos.  
- Seguridad: Firewall en el perímetro de la red y un sistema de detección de intrusos (IDS).  
- Switch central: Cisco Catalyst 9300  
- Firewalls: Fortinet FortiGate 100E

**Redes de Datos y Cumplimiento Normativo:**

Es fundamental que la infraestructura de red cumpla con las normativas vigentes para garantizar la seguridad y privacidad de los datos. Estas normativas pueden variar según la región y la industria, pero algunas de las más relevantes incluyen:

**GDPR (Reglamento General de Protección de Datos)**: Aplicable si se manejan datos de ciudadanos de la Unión Europea.

**HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud)**: Aplicable para organizaciones de atención médica en los EE. UU.

**PCI-DSS (Norma de Seguridad de Datos para la Industria de Tarjetas de Pago)**: Aplicable si se manejan pagos con tarjeta de crédito.

Para garantizar el cumplimiento, se deben implementar las siguientes medidas:

**Cifrado de Datos**: Utilizar cifrado en tránsito y en reposo para proteger la información sensible.

**Autenticación Multifactor (MFA)**: Implementar MFA para acceso a sistemas críticos.

**Monitorización y Auditoría**: Establecer sistemas de monitorización y auditoría para detectar y responder a incidentes de seguridad.

**Detalle del esquema lógico primario (tentativo) de interconexión con otros establecimientos si es que corresponde:**  
- VPN Site-to-Site: Para conectar diferentes establecimientos de manera segura a través de Internet.  
- Seguridad: Uso de IPSec para cifrar el tráfico entre establecimientos.  
- Redundancia: Conexiones redundantes en caso de fallo de la conexión principal.  
- Dispositivos de VPN: Cisco ASA 5506-X  
- Enlaces: Enlaces dedicados MPLS o conexiones de fibra óptica como respaldo.

**Glosario Técnico**  
- VLAN (Virtual Local Area Network): Técnica para segmentar una red física en redes lógicas separadas.  
- RAID (Redundant Array of Independent Disks): Sistema de almacenamiento que combina múltiples discos duros para mejorar la redundancia y/o el rendimiento.  
- IDS (Intrusion Detection System): Sistema que monitorea el tráfico de red en busca de actividades sospechosas y posibles ataques.

**Firewall**: Dispositivo de seguridad de red que monitorea y controla el tráfico de red entrante y saliente según políticas de seguridad predeterminadas.

**IPSec (Internet Protocol Security)**: Conjunto de protocolos para asegurar las comunicaciones a través de redes IP mediante la autenticación y el cifrado de cada paquete IP.

**MFA (Multifactor Authentication)**: Método de control de acceso que requiere dos o más formas de verificación para acceder a un recurso.

**GDPR (General Data Protection Regulation)**: Reglamento europeo para la protección de datos personales.

**HIPAA (Health Insurance Portability and Accountability Act)**: Ley estadounidense que establece normas de privacidad y seguridad para la información médica.

**PCI-DSS (Payment Card Industry Data Security Standard)**: Normativa de seguridad para proteger la información de las tarjetas de crédito.

**Cifrado (Encryption)**: Proceso de convertir información o datos en un código para prevenir el acceso no autorizado.

**Switch**: Dispositivo de red que conecta múltiples dispositivos en una red local (LAN) y utiliza la conmutación de paquetes para recibir y enviar datos a los dispositivos.

**VPN (Virtual Private Network)**: Red privada que se extiende a través de una red pública o compartida, permitiendo a los usuarios enviar y recibir datos como si sus dispositivos estuvieran directamente conectados a la red privada.

**MPLS (Multiprotocol Label Switching)**: Técnica de encaminamiento de datos que dirige los datos desde un nodo de red a otro basado en etiquetas de corta longitud en lugar de direcciones de red.