UAO - FACULTAD DE INGENIERIA - SEGURIDAD INFORMATICA
Mcs. CIRO ANTONIO DUSSAN

Ejercicio Correspondiente al Proyecto Final

Objetivo;

Analizar, Diseñar e implementar una infraestructura de red en la empresa XYZ que permita configurar el servicio de Directorio Activo (AD) y configurar las Directivas de Seguridad.

Requerimientos:

1. Software de Máquina virtual (virtual box – Vmware)
2. La .ISO de un Server 2016, 2019. La que escojan
3. Instalar un cliente Windows (7 Ultimate, 10 pro ó 11)
4. Leer la documentación sobre el DNS, DHCP, Directorio Activo TECHNET MICROSOFT
5. Observar video tutorial Instalación y configuración del Directorio Activo
6. Leer detalladamente el ejercicio propuesto
7. Diseñar la Red de datos con Packet Tracer

Entregables:

1. Diseño de la red lógica en packet tracer (Implementar los servicios de DNS, DHCP)
    a. Segmentar la red de datos según el organigrama de la empresa.
    b. Configurar los dispositivos activos (ROUTER Y SWITCH)
    c. Configurar la seguridad de la red (VLAN)
    d. Asegurar el servicio de internet (Firewall)
2. Informe sobre el diseño del DA este se debe presentar en la herramienta VISIO de Microsoft.
3. Tabla en Excel de la información de los usuarios del AD. Base de dato completa
4. Presentar las directivas de seguridad y políticas de grupo
5. Definir la Política de seguridad según la ISO 27001
6. Defenir un Plan de Recuperación de Desastres DRP

El ejercicio se prueba con otra MV cliente que puede ser un cliente Windows para hacer la autenticación al Directorio Activo y la asignación de la ip debe ser Dinámica.

Fecha de Entrega: Mayo XX (Fase de Diseño y Configuración de la MV de Windows Server. Con los servicios de DNS y DHCP) Primer Avance, corresponde al 40% parte práctica

Mayo xx entrega final con las directivas implementadas en el directorio activo. Informe final y sustentación de la calificación del III parcial. 60%

El trabajo se puede presentar máximo en grupos máximo de 4 personas.

cadussan@uao.edu.co

EJERCICIO DE DIRECTORIO ACTIVO

Objetivo

Este ejercicio tiene como objetivo la implementación del directorio activo en donde los estudiantes realicen un proceso significativo de aprendizaje mediante el proceso de investigación, reflexión y práctica.

Al final los estudiantes deberán mostrar en un escenario la red que de acuerdo con los requerimientos se les pide.

Objetivos Específicos

1. Desarrollar un proceso de planeación bien detallado donde se tenga en cuenta el escenario organizacional que se les plantea.

2. Establecer una logística de grupo, para enfrentar el problema, sobra decir que TODOS deben tener 100% de conocimientos de lo que se está haciendo, máximo deben ser 4 personas.

3. Mostrar las fases que fueron tenidas en cuenta para el proceso de implementación.

4. Diseñar una red segura con la implementación de VPN y segmentación de la red. (solo a nivel de diseño con el packet tracer)

5. Mostrar la implementación del AD. Se puede autenticar por cualquier usuario de la Base de datos, la asignación de IP debe ser por DHCP.

6. Establecer una estructura de AD que refleje la estructura organizacional y que permita una mejor administración de los recursos informáticos.

7. Mostrar el manejo de cuentas de usuario y de recursos de red (usuarios, equipos, Unidades Organizacionales, grupos, políticas de usuario).

8. Establecer las políticas de usuario (roles, privilegios, restricciones, etc. etc.) y las razones de estas, adecuadas según requerimientos funcionales de las áreas en cada organización.

9. Realizar un proceso de recuperación del AD en caso de daño.

10. Sustentar el ejercicio en una máquina virtual. Se recomienda traer su portátil para este ejercicio y no depender de otros recursos.

Caso EMPRESA "XYZ"

La compañía **XYZ (cada grupo debe tener un dominio propio que será el de sus apellidos. Ejemplo: murciayavila.com)** ubicada en Cali - Valle. Requiere de la destreza de los estudiantes de la clase de Seguridad en Redes para la implementación de su Directorio Activo Windows 200?.

XYZ es una empresa destinada al manejo de consultores de auditoria y cuenta con personal de 50 personas y 2 subcompañías, XYZ-Management y XYZ-Commercial. Tiene su dominio registrado como apellido1yapellido2**.com** que es el de la compañía como tal, posee 2 departamentos en XYZ-Management con sus respectivas sub áreas y 2 departamentos en XYZ-Commercial con sus sub-áreas:

Para el caso de **XYZ-Management** posee los siguientes departamentos:

1. Área administrativa: Cuenta con **11 personas** las cuales se especifican de la siguiente forma:

    a. Junta directiva: Integrada por 5 personas altamente importantes para la compañía ya que toman las decisiones sobre el futuro de las mismas. Son usuarios críticos que están viajando constantemente. Sus requerimientos son:

        i. Alto nivel de confidencialidad en el acceso a sus equipos.
        ii. Alto nivel de flexibilidad en sus equipos para poderse conectar desde otras redes en otros lugares sin inconvenientes.
        iii. Apoyan totalmente las políticas de seguridad que sean propuestas, pero teniendo en cuenta los requerimientos anteriores.
        iv. Se encargan de establecer la renovación del personal del área financiera cada 24 meses.

    b. Administrativo-Financiera: Son 6 personas de planta que realizan procesos administrativos de alta confidencialidad. Sus requerimientos son:

        i. Acceder a los recursos de red (impresoras, fólder compartidos, contar con los niveles de seguridad y restricción para evitar fugas de información).
        ii. Quieren ser parte de la organización y a la vez poseer independencia propia de la misma.
        iii. Brindan información financiera oportuna a la junta directiva en cualquier lugar del mundo. Esto significa que los directivos puedan conectarse desde cualquier lugar vía MODEM o vía red para acceder a Internet sin problemas.
        iv. Se encargan de Establecer el tiempo de permanencia del personal Gerentes y Auditor Técnico, ya que por políticas cada 12 meses se renueva el contrato.

2. Área de consultores: Integrada por **25 consultores** de auditoria, que se dedican a realizar proyectos relacionados con este tema a otras compañías de su sector. Se dividen en:

a. Gerentes de Proyectos: Son 5 gerentes proyectos que desempeñan labores técnico-administrativas y algunas financieras, lo cual significa que están en continúa comunicación con el área Administrativa-Financiera. Ellos tiene los siguientes requerimientos:

    i. Capacidad de ser usuarios de pruebas de nuevas configuraciones de auditoría brindadas por el personal Auditor Técnico.
    ii. Mantener los niveles de seguridad adecuados. (ellos quieren ser el modelo interno para ser mostrados a proyectos externos).

b. Auditoría Técnica: Son los auditores (20 personas) que finalmente hacen las evaluaciones técnicas en los proyectos asignados en las diferentes empresas y brindan continuamente información a los Gerentes sobre el estado del proyecto. Sus requerimientos son:

    i. Necesitan estar en capacidad de probar nuevos software en sus equipos.
    ii. Estar dentro de las políticas de seguridad, establecidas por la compañía XYZ.
    iii. Tener la flexibilidad de poderse conectar a Internet desde cualquier lugar sin inconvenientes.

Para el caso de **XYZ-Comercial** los siguientes departamentos:

3. Área comercial: Es el área que entra en contacto con los clientes (son **9 personas**) junto con los gerentes de proyectos para determinar finalmente los Auditores que entran a formar parte del equipo de trabajo. El área comercial esta integrada por:

    a. 1 Gerente comercial, encargado de las estrategias comerciales establecidas por el área y la parte financiera. Sus requerimientos son:

        i. Poder tener acceso a los recursos de área financiera y de los gerentes de proyecto.
        ii. Ser un usuario con el mayor nivel de flexibilidad para poder acceder a los estados del proyecto o fases del área de Auditoria Técnica.
        iii. Mantener total independencia del área administrativa que representa XYZ-Management.

    b. Representantes comerciales: Son los que realmente van a las reuniones para nuevos proyectos con los gerentes de proyectos de XYZ-Management, actualmente son 8 personas. Sus requerimientos son:

        i. Se encargan de tener informado al Jefe de su área y al gerente líder del proyecto sobre estado de conformidad con el cliente. No se establece comunicación directa con los técnicos ya que se quiere mantener la jerarquía y delegar opiniones en una sola persona e independizar roles.

ii. En las reuniones se movilizan con Laptops cada uno de ellos de tal forma que estos equipos son solo para este fin pero deben tener la capacidad de ser configurados según las necesidades de la red donde estén, ya que un viaje puede prolongarse por varios días. Cada uno de ellos posee su propio desktop en su oficina.
iii. Quieren tener acceso directo a la información brindada por su red en general.
iv. Deben ser usuarios con controles de seguridad y dado la variabilidad en esta área sus contratos solo se renuevan cada 12 meses.
v. Es importante tener en cuenta que ellos pueden por autorización de su jefe inmediato enviar información impresa (mandar un archivo e imprimirlo en el área de Consultores) a un gerente de proyecto.

4. Área Administrativa: Son **5 personas** que cumplen la función de ver el estado de cuenta de las inversiones realizadas en los proyectos conseguidos por el área comercial y realizar respectivamente el estudio de factibilidad y nivel de riesgo que la inversión representa. Sus requerimientos son:

    a. Semanalmente todos los miércoles de 7:30 am a 4:30 pm se reúnen en las oficinas de XYZ-Management juntos con las 6 personas del área administrativa de allí y se establecen el estado financiero de los proyectos tomados y los planes a futuro.

    b. Ellos desean que en ese tiempo poder tener acceso a los recursos de XYZ-Management sin tener dificultad. Pero que ello no signifique que pierdan su independencia administrativa en XYZ-Commercial

Las políticas de XYZ-Management son:

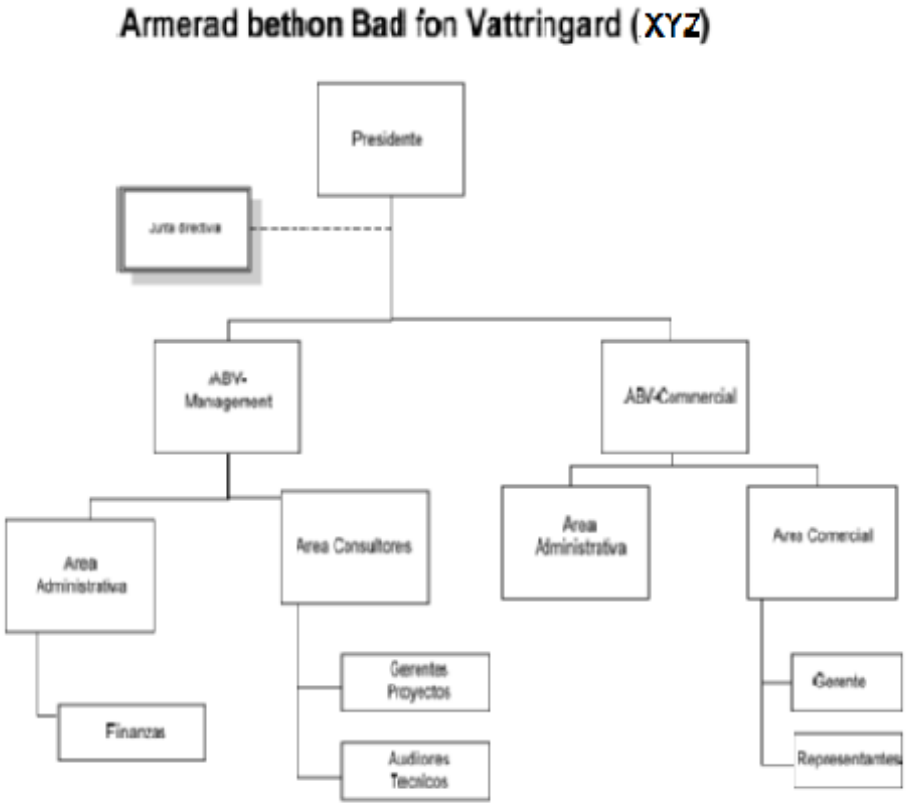
1. Mantener una unidad administrativa que refleje las funciones que este negocio muestra.
2. Toda información es confidencial.
3. Los horarios de trabajo son de 8pm a 5:30 pm
4. Cada usuario es absolutamente responsable de su información y solo debe tener acceso a su equipo.
5. En el evento que un empleado requiera permanecer más tiempo del establecido en la jornada, debe informar sobre ellos para brindarle el respectivo permiso, el cual solo aplica para el día solicitado.
6. Cada departamento es totalmente autónomo en la toma de decisiones, pero a nivel de informático debe estar acorde a las políticas establecidas por los consultores informáticos externos.
7. Cualquier mejora que no vaya en contra de los requerimientos y/o exigencias es bienvenida.
8. La junta directiva quiere full acceso a cualquier recurso en cualquiera de sus 2 compañías.

Las políticas de XYZ-Comercial:

1. Los horarios de trabajo son 24 horas al día. Es decir, no hay restricciones de horario de trabajo. Normalmente la jornada dura de 7:30 pm a 4:30 pm, pero si alguien desea trabajar más lo puede hacer.
2. Todos los usuarios son usuarios móviles para esta red, cualquiera de ellos puede viajar y eso conlleva que hay que tener en cuenta que debe poder tener total autonomía de sus equipos durante el viaje.
3. El Gerente rinde cuentas directamente a la junta directiva todos los viernes de 2 pm a 6 pm y requiere tener el acceso a los recursos de esa red.

El presidente de la compañía está convencido que esta nueva infraestructura operativa no debe ocasionar ningún tipo de trauma a los jefes de departamento quienes son sus guías en la toma de decisiones. Quiere que su tecnología sea un fiel reflejo en esta nueva organización o si hay recomendaciones son bienvenidas. El suministra el Organigrama:

NOTA: PUEDE IMPLEMENTAR LAS DIRECTIVAS QUE SUGIERAN QUE REFUERCEN LA SEGURIDAD DE LA INFRAESTRUCTURA DE LA RED.



Entrega: Mayo 09. Toda la Fase de Diseño, Packetracer (funcionando segmentando, con direccionamiento, con VLAN), Diseño del AD, Lista de Empleados en Excel. Instalado el Windows Server y Promover a Controlador de Dominio. Servicios DNS, Esto se calificará.

Entrega: Mayo 23 mayo Instalada la máquina cliente, configurado el DHCP, subido los empleados automáticamente creados en el AD, Implementar Directivas de Grupo en el AD. Segunda parte final del Proyecto

Archivos en la plataforma de Google en espacio de tareas indicando los nombres de los integrantes.

MG. ING. CIRO ANTONIO DUSSAN C.

BIBLIOGRAFIA

https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

https://www.youtube.com/watch?v=a7lguPUW6k0

https://social.technet.microsoft.com/wiki/contents/articles/19495.guia-paso-a-paso-para-configurar-el-controlador-de-dominio-de-windows-server-2012-es-es.aspx

https://learn.microsoft.com/es-es/windows-server/identity/ad-fs/operations/set-up-an-ad-fs-lab-environment

https://blogdesistemas.com/crear-dominio-windows-server-2019/

https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/install-configure-dhcp-server-workgroup

https://social.technet.microsoft.com/wiki/contents/articles/24914.instalacion-y-configuracion-basica-de-un-servidor-dhcp-en-windows-server-2012-desde-powershell-es-es.aspx

https://learn.microsoft.com/es-es/windows-server/networking/dns/quickstart-install-configure-dns-server?tabs=powershell

https://social.technet.microsoft.com/Forums/es-ES/e4f54e7d-761b-4c6a-88a8-8a9ca2e2210e/creacion-de-usuarios-en-directorio-activo?forum=scriptgenerales

https://techexpert.tips/es/windows-es/instalacion-de-active-directory-en-windows-server/

Plantilla Visio Microsoft AD

https://support.microsoft.com/es-es/office/diagramas-y-plantillas-destacados-de-visio-27d4274b-5fc2-4f5c-8190-35ff1db34aa5

Directivas de Seguridad

https://learn.microsoft.com/es-es/troubleshoot/windows-server/group-policy/configure-group-policies-set-security

CISCO

https://learningnetwork.cisco.com/s/all-media?ccid=sem&dtid=mediabuy&oid=sem&gclid=CjwKCAjw586hBhBrEiwAQYEnHdjxbIlotcX87bO_Np6Bv0IZV2p2J8dSSQlzqiKVvVuvY3Ibp8ftEhoC_G8QAvD_BwE